Gerenciamento de storage nas

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciamento de storage nas . . . 1
Gerenciar protocolos nas com o System Manager . . . 1
Configurar o NFS com a CLI . . . 23
Gerencie o NFS com a CLI . . . 97
Gerenciar trunking NFS . . . 220
Gerenciar NFS em RDMA . . . 230
Configure o SMB com a CLI . . . 236
Gerencie SMB com a CLI . . . 279
Fornecer acesso de cliente S3 aos dados nas . . . 639
Configuração SMB para Microsoft Hyper-V e SQL Server . . . 649

Gerenciamento de storage nas

Gerenciar protocolos nas com o System Manager

Visão geral do gerenciamento nas com o System Manager

Os tópicos nesta seção mostram como configurar e gerenciar ambientes nas com o System Manager no ONTAP 9.7 e versões posteriores.

Se você estiver usando o gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e versões anteriores), consulte estes tópicos:

- "Visão geral da configuração NFS"
- "Visão geral da configuração SMB"

O System Manager é compatível com fluxos de trabalho para:

- Configuração inicial de clusters que você pretende usar para serviços de arquivos nas.
- Provisionamento de volume adicional para necessidades dinâmicas de storage.
- Configuração e manutenção para instalações de autenticação e segurança padrão do setor.

Com o System Manager, você pode gerenciar serviços nas no nível de componente:

- Protocolos - NFS, SMB ou ambos (multiprotocolo nas)
- Serviços de nomes - DNS, LDAP e NIS
- Switch do serviço de nomes
- Segurança Kerberos e TLS
- Exportações e ações
- Qtrees
- Mapeamento de nomes de usuários e grupos

Provisione storage NFS para datastores VMware

Antes de usar o console de storage virtual para VMware vSphere (VSC) para provisionar volumes NFS em um sistema de storage baseado em ONTAP para hosts ESXi, ative o NFS usando o System Manager para ONTAP 9.7 ou posterior.

Depois de criar um "VM de storage habilitada por NFS" no System Manager, você provisiona volumes NFS e gerencia armazenamentos de dados usando o VSC.

A partir do VSC 7,0, o VSC faz parte "Ferramentas do ONTAP para o dispositivo virtual VMware vSphere" do , que inclui o VSC, o provedor vStorage APIs for Storage Awareness (VASA) e o Storage Replication Adapter (SRA) para os recursos do VMware vSphere.

Certifique-se de que verifica o "Matriz de interoperabilidade do NetApp" para confirmar a compatibilidade entre as versões atuais do ONTAP e do VSC.

Para configurar o acesso NFS para hosts ESXi em armazenamentos de dados usando o System Manager

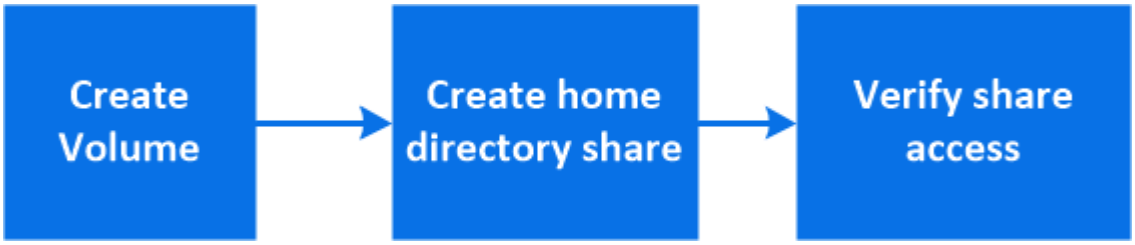
Classic (para ONTAP 9.7 e versões anteriores), consulte "Configuração NFS para ESXi usando visão geral do VSC"

Para obter mais informações, consulte "TR-4597: VMware vSphere for ONTAP" e a documentação da versão do VSC.

Provisione storage nas para diretórios base

Crie volumes para fornecer armazenamento para diretórios base usando o protocolo SMB.

Este procedimento cria novos volumes para diretórios base em um "VM de storage habilitada para SMB existente". Você pode aceitar padrões de sistemas ao configurar volumes ou especificar configurações personalizadas.



Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para SMB.
   a. Selecione **armazenamento > volumes** e clique em **Adicionar**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Apenas as VMs de armazenamento configuradas com o protocolo SMB são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.
      - Você pode clicar em **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. clique em **armazenamento > compartilhamentos**, clique em **Adicionar** e selecione **Home Directory**.
3. Em um cliente Windows, faça o seguinte para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\<SMB_Server_Name>\<Share_Name>`

      Se o nome do compartilhamento foi criado com variáveis (%W, %d ou %u), certifique-se de testar o acesso com um nome resolvido.

b. Na unidade recém-criada, crie um arquivo de teste e exclua o arquivo.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

    Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.
- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.
- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento completo para diretórios base.

Provisione storage nas para servidores Linux usando NFS

Crie volumes para fornecer storage para servidores Linux usando o protocolo NFS com o ONTAP System Manager (9,7 e posterior).

Este procedimento cria novos volumes em um "VM de storage habilitada por NFS existente". Você pode aceitar padrões do sistema ao configurar volumes ou especificar configurações personalizadas.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Se quiser obter detalhes sobre a gama de capacidades do protocolo NFS da ONTAP, consulte o "Visão geral de referência de NFS".

Passos

1. Adicionar um novo volume em uma VM de storage habilitada por NFS.
   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Somente as VMs de storage configuradas com o protocolo NFS são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.

        A política de exportação padrão concede acesso total a todos os usuários.

      - Você pode clicar em **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. em um cliente Linux, faça o seguinte para verificar o acesso.
   a. Crie e monte o volume usando a interface de rede da VM de armazenamento.
   b. No volume recém-montado, crie um arquivo de teste, escreva texto nele e exclua o arquivo.

   Depois de verificar o acesso, você pode "restringir o acesso do cliente com a política de exportação do volume" e definir qualquer propriedade e permissões UNIX desejadas no volume montado.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**)

no qual deseja colocar o volume que está criando.

Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne ao Etapa 2 no fluxo de trabalhoprovisionamento completo para servidores Linux usando NFS.

Outras maneiras de fazer isso em ONTAP

Para executar esta tarefa com…	Consulte…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração NFS"
A interface de linha de comando (CLI) do ONTAP	"Visão geral da configuração de NFS com a CLI"

Gerenciar o acesso usando políticas de exportação

Habilite o acesso de cliente Linux a servidores NFS usando políticas de exportação.

Este procedimento cria ou modifica políticas de exportação para um "VM de storage habilitada por NFS existente".

Passos

1. No System Manager, clique em **Storage** > **volumes**.
2. Clique em um volume habilitado para NFS e clique em **More**.
3. Clique em **Editar política de exportação** e, em seguida, clique em **Selecionar uma política existente** ou em **Adicionar uma nova política**.

Provisione storage nas para servidores Windows usando SMB

Crie volumes para fornecer storage para servidores Windows usando o protocolo SMB usando o Gerenciador de sistemas, que está disponível com o ONTAP 9.7 e posterior.

Esse procedimento cria novos volumes em um "VM de storage habilitada para SMB existente" e cria um compartilhamento para o diretório raiz de volume (/). Você pode aceitar padrões de sistemas ao configurar volumes ou especificar configurações personalizadas. Após a configuração inicial do SMB, você também pode criar compartilhamentos adicionais e modificar suas propriedades.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance,

criar o FlexGroup volumes. Consulte também "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup".

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Se pretender obter detalhes sobre a gama de capacidades do protocolo SMB do ONTAP, consulte o "Visão geral de referência SMB".

Antes de começar

- A partir do ONTAP 9.13,1, você pode habilitar a análise de capacidade e o acompanhamento de atividades por padrão em novos volumes. No System Manager, você pode gerenciar as configurações padrão no nível de cluster ou VM de armazenamento. Para obter mais informações, "Ative a análise do sistema de ficheiros"consulte .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para SMB.
   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Apenas as VMs de armazenamento configuradas com o protocolo SMB são listadas. Se apenas uma VM de armazenamento configurada com o protocolo SMB estiver disponível, o campo **Storage VM** não será exibido.

      - Se você selecionar **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.
      - Você pode selecionar **mais opções** para personalizar a configuração do volume para ativar serviços como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.
2. mude para um cliente Windows para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\_SMB_Server_Name__Share_Name_`
   b. Na unidade recém-criada, crie um arquivo de teste, escreva texto para ele e exclua o arquivo.

Depois de verificar o acesso, você pode restringir o acesso do cliente com a ACL de compartilhamento e definir as propriedades de segurança desejadas na unidade mapeada. Consulte "Crie um compartilhamento SMB" para obter mais informações.

Adicionar ou modificar compartilhamentos

Você pode adicionar compartilhamentos adicionais após a configuração inicial do SMB. Os compartilhamentos são criados com valores e propriedades padrão que você selecionar. Estes podem ser modificados mais tarde.

Você pode definir as seguintes propriedades de compartilhamento ao configurar um compartilhamento:

- Permissões de acesso
- Compartilhar propriedades
  - Ative a disponibilidade contínua para compartilhamentos que contêm dados Hyper-V e SQL Server sobre SMB (começando com ONTAP 9.10,1). Veja também:

        - "Requisitos de compartilhamento continuamente disponíveis para Hyper-V sobre SMB"
        - "Requisitos de compartilhamento continuamente disponíveis para SQL Server sobre SMB"
    - Criptografe dados com SMB 3,0 enquanto acessa esse compartilhamento.

Após a configuração inicial, você também pode modificar estas propriedades:

- Links simbólicos
    - Ative ou desative links simbólicos e widelinks
- Compartilhar propriedades
    - Permitir que os clientes acessem o diretório cópias Snapshot.
    - Ative os oplocks, permitindo que os clientes bloqueiem arquivos e armazenem conteúdo em cache localmente (padrão).
    - Ative a enumeração baseada em acesso (ABE) para exibir recursos compartilhados com base nas permissões de acesso do usuário.

Procedimentos

Para adicionar um novo compartilhamento em um volume habilitado para SMB, clique em **armazenamento > compartilhamentos**, clique em **Adicionar** e selecione **compartilhar**.

Para modificar um compartilhamento existente, clique em **armazenamento > compartilhamentos** e, em seguida, clique em ⋮ e selecione **Editar**.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

    - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
    - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
    - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado, poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

      Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento completo para servidores Windows usando SMB.

Outras maneiras de fazer isso em ONTAP

Para executar esta tarefa com…	Consulte…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração SMB"
A interface da linha de comando ONTAP	"Visão geral da configuração SMB com a CLI"

Provisionar storage nas para Windows e Linux usando NFS e SMB

Crie volumes para fornecer storage para clientes usando o protocolo NFS ou SMB.

Este procedimento cria novos volumes em um "VM de storage existente habilitada para protocolos NFS e SMB".

O protocolo NFS geralmente é usado em ambientes Linux. O protocolo SMB é geralmente usado em ambientes Windows. No entanto, tanto o NFS como o SMB podem ser usados com Linux ou Windows.

Você pode criar o FlexVol volumes ou, para sistemas de arquivos grandes com requisitos de alta performance, criar o FlexGroup volumes. "Provisionar storage nas para sistemas de arquivos grandes usando volumes FlexGroup"Consulte .

Você também pode salvar as especificações desse volume em um Playbook do Ansible. Para obter mais detalhes, "Use os Playbooks do Ansible para adicionar ou editar volumes ou LUNs"visite .

Passos

1. Adicione um novo volume em uma VM de storage habilitada para NFS e SMB.
   a. Clique em **Storage > volumes** e, em seguida, clique em **Add**.
   b. Insira um nome, selecione a VM de armazenamento e insira um tamanho.

      Somente as VMs de storage configuradas com os protocolos NFS e SMB são listadas. Se apenas uma

VM de storage configurada com os protocolos NFS e SMB estiver disponível, o campo **Storage VM** não será exibido.

c. Clique em **mais Opções** e selecione **Exportar via NFS**.

A configuração padrão concede acesso total a todos os usuários. Você pode adicionar regras mais restritivas à política de exportação mais tarde.

d. Selecione **compartilhar via SMB/CIFS**.

O compartilhamento é criado com uma lista de controle de acesso (ACL) padrão definida como "Controle total" para o grupo **todos**. Você pode adicionar restrições à ACL mais tarde.

e. Se você clicar em **Salvar** neste ponto, o Gerenciador do sistema usará os padrões do sistema para criar e adicionar um FlexVol volume.

Como alternativa, você pode continuar a ativar quaisquer serviços adicionais necessários, como autorização, qualidade do serviço e proteção de dados. Personalizar a configuração do volumeConsulte a e, em seguida, volte aqui para concluir os passos seguintes.

2. em um cliente Linux, verifique se a exportação está acessível.
   a. Crie e monte o volume usando a interface de rede da VM de armazenamento.
   b. No volume recém-montado, crie um arquivo de teste, escreva texto nele e exclua o arquivo.
3. Em um cliente Windows, faça o seguinte para verificar se o compartilhamento está acessível.
   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\_SMB_Server_Name__Share_Name_`
   b. Na unidade recém-criada, crie um arquivo de teste, escreva texto para ele e exclua o arquivo.

Depois de verificar o acesso, você pode "Restrinja o acesso do cliente com a política de exportação do volume, restrinja o acesso do cliente com a ACL de compartilhamento"e definir qualquer propriedade e permissões desejadas no volume exportado e compartilhado.

Personalizar a configuração do volume

Você pode personalizar a configuração de volume quando adicionar volumes em vez de aceitar os padrões do sistema.

Procedimento

Depois de clicar em **mais opções**, selecione a funcionalidade de que necessita e introduza os valores necessários.

- Cache para volume remoto.
- Nível de serviço de performance (qualidade do serviço, QoS).

  A partir do ONTAP 9.8, você pode especificar uma política de QoS personalizada ou desativar QoS, além da seleção de valor padrão.

  - Para desativar a QoS, selecione **Custom**, **existing** e, em seguida, **none**.
  - Se você selecionar **Custom** e especificar um nível de serviço existente, um nível local será escolhido automaticamente.
  - A partir do ONTAP 9.9,1, se você optar por criar um nível de serviço de desempenho personalizado,

poderá usar o Gerenciador do sistema para selecionar manualmente o nível local (**colocação manual**) no qual deseja colocar o volume que está criando.

Esta opção não estará disponível se selecionar as opções de cache remoto ou volume FlexGroup.

- FlexGroup volumes (selecione **distribuir dados de volume pelo cluster**).

  Esta opção não está disponível se tiver selecionado anteriormente **colocação manual** em **nível de serviço de desempenho**. Caso contrário, o volume que você está adicionando se torna um FlexVol volume por padrão.

- Permissões de acesso para os protocolos para os quais o volume está configurado.
- Proteção de dados com SnapMirror (local ou remoto) e especifique a política de proteção e as configurações do cluster de destino nas listas suspensas.
- Selecione **Salvar** para criar o volume e adicioná-lo ao cluster e à VM de armazenamento.

Depois de salvar o volume, retorne Etapa 2 no fluxo de trabalhoao provisionamento multiprotocolo completo para servidores Windows e Linux.

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Veja este conteúdo…
Gerenciador de sistema Clássico (ONTAP 9 .7 e anteriores)	"Visão geral da configuração multiprotocolo SMB e NFS"
A interface da linha de comando ONTAP	• "Visão geral da configuração SMB com a CLI" • "Visão geral da configuração de NFS com a CLI" • "Quais são os estilos de segurança e seus efeitos" • "Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo"

Acesso de cliente seguro com Kerberos

Ative o Kerberos para proteger o acesso ao armazenamento para clientes nas.

Este procedimento configura o Kerberos em uma VM de armazenamento existente habilitada "NFS"para ou "SMB".

Antes de começar, você deve ter configurado DNS, NTP e "LDAP"no sistema de armazenamento.

Passos

1. Na linha de comando ONTAP, defina permissões UNIX para o volume raiz da VM de armazenamento.

   a. Exiba as permissões relevantes no volume raiz da VM de armazenamento: `volume show -volume root_vol_name-fields user,group,unix-permissions`

O volume raiz da VM de storage deve ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

a. Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Definir permissões de usuário para o volume raiz da VM de armazenamento.

a. Exibir os usuários locais do UNIX: `vserver services name-service unix-user show -vserver vserver_name`

A VM de storage deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal
nfs	500	0
raiz	0	0

+
Nota: o usuário NFS não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS; consulte a etapa 5.

a. Se esses valores não forem exibidos, use o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Definir permissões de grupo para o volume raiz da VM de armazenamento.

a. Exibir os grupos UNIX locais: `vserver services name-service unix-group show -vserver vserver_name`

A VM de armazenamento deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

a. Se esses valores não forem exibidos, use o `vserver services name-service unix-group modify` comando para atualizá-los.

4. Mude para o System Manager para configurar o Kerberos
5. No System Manager, clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
6. Clique em **Configurações**.
7. Clique → em Kerberos.
8. Clique em **Add** em Kerberos Realm e complete as seguintes seções:
   - Adicione o realm Kerberos

Insira os detalhes de configuração dependendo do fornecedor do KDC.

- Adicionar interface de rede ao realm

  Clique em **Add** e selecione uma interface de rede.

9. Se desejado, adicione mapeamentos de nomes principais do Kerberos aos nomes de usuário locais.
   a. Clique em **Storage > Storage VMs** e selecione a VM de armazenamento.
   b. Clique em **Configurações** e, em seguida, clique em **Mapeamento de nomes**.
   c. Em **Kerberos para UNIX**, adicione padrões e substituições usando expressões regulares.

Ative ou desative o acesso seguro do cliente NFS com TLS

Você pode melhorar a segurança das conexões NFS configurando o NFS em TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS. Você pode configurá-lo em uma VM de armazenamento existente habilitada para "NFS"o .

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

"requisitos"Consulte o para NFS sobre TLS.

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. No bloco **NFS**, clique em **NFS over TLS settings**.
3. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
4. Clique em ⋮ para essa interface.
5. Clique em **Ativar**.
6. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
7. Clique em **Salvar**.

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

Passos

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. No bloco **NFS**, clique em **NFS over TLS settings**.
3. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja desativar TLS.
4. Clique em ⋮ para essa interface.
5. Clique em **Desativar**.
6. Na caixa de diálogo de confirmação resultante, selecione **Disable**.

Fornecer acesso ao cliente com serviços de nome

Ative o ONTAP para procurar informações de host, usuário, grupo ou netgroup usando LDAP ou NIS para autenticar clientes nas.

Este procedimento cria ou modifica configurações LDAP ou NIS em uma VM de armazenamento existente habilitada para "NFS" ou "SMB".

Para configurações LDAP, você deve ter os detalhes de configuração LDAP necessários em seu ambiente e você deve usar um esquema LDAP padrão do ONTAP.

Passos

1. Configure o serviço necessário: Clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento, clique em **Definições** e, em seguida, clique ⚙ em para LDAP ou NIS.
3. Inclua quaisquer alterações no switch de serviços de nome: Clique ✎ em Name Services Switch.

Gerencie diretórios e arquivos

Expanda a exibição do volume do System Manager para exibir e excluir diretórios e arquivos.

A partir do ONTAP 9.9,1, os diretórios são excluídos com a funcionalidade de exclusão assíncrona de diretório de baixa latência.

Para obter mais informações sobre como visualizar sistemas de arquivos no ONTAP 9.9,1 e posterior, "Visão geral do File System Analytics"consulte .

Passo

1. Selecione **armazenamento > volumes**. Expanda um volume para ver o seu conteúdo.

Gerencie usuários e grupos específicos do host com o System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para gerenciar usuários e grupos específicos de um host UNIX ou Windows.

Você pode executar os seguintes procedimentos:

Windows	UNIX

• Exibir usuários e grupos do Windows • [add-edit-delete-Windows] • [manage-windows-users]	• Exibir usuários e grupos UNIX • [add-edit-delete-UNIX] • [manage-unix-users]

Exibir usuários e grupos do Windows

No System Manager, você pode exibir uma lista de usuários e grupos do Windows.

Passos

1. No System Manager, clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento e, em seguida, selecione a guia **Configurações**.
3. Role até a área **Host Users and Groups**.

   A seção **Windows** exibe um resumo do número de usuários em cada grupo associado à VM de armazenamento selecionada.

4. Clique → na seção **Windows**.
5. Clique na guia **Groups** e, em seguida, clique ⌄ ao lado de um nome de grupo para exibir detalhes sobre esse grupo.
6. Para exibir os usuários em um grupo, selecione o grupo e clique na guia **usuários**.

Adicione, edite ou exclua um grupo do Windows

No System Manager, você pode gerenciar grupos do Windows adicionando, editando ou excluindo-os.

Passos

1. No System Manager, veja a lista de grupos do Windows. Exibir usuários e grupos do WindowsConsulte a .
2. Na guia **Groups**, você pode gerenciar grupos com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um grupo	1. Clique + Add em . 2. Introduza as informações do grupo. 3. Especifique Privileges. 4. Especifique membros do grupo (adicione usuários locais, usuários de domínio ou grupos de domínio).
Edite um grupo	1. Ao lado do nome do grupo, clique ⋮ em e, em seguida, clique em **Editar**. 2. Modifique as informações do grupo.

Eliminar um grupo	1. Marque a caixa ao lado do grupo ou grupos que deseja excluir. 2. Clique Delete em . **Observação:** você também pode excluir um único grupo clicando ⋮ ao lado do nome do grupo e clicando em **Excluir**.

Gerenciar usuários do Windows

No System Manager, você pode gerenciar usuários do Windows adicionando, editando, excluindo, habilitando ou desativando-os. Você também pode alterar a senha de um usuário do Windows.

Passos

1. No System Manager, visualize a lista de utilizadores do grupo. Exibir usuários e grupos do WindowsConsulte a .
2. Na guia **usuários**, você pode gerenciar usuários com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um utilizador	1. Clique + Add em . 2. Introduza as informações do utilizador.
Editar um utilizador	1. Ao lado do nome de usuário, clique ⋮ em e, em seguida, clique em **Editar**. 2. Modifique as informações do usuário.
Eliminar um utilizador	1. Marque a caixa ao lado do usuário ou usuários que você deseja excluir. 2. Clique Delete em . **Observação:** você também pode excluir um único usuário clicando ⋮ ao lado do nome de usuário e clicando em **Excluir**.
Alterar a palavra-passe do utilizador	1. Ao lado do nome de usuário, clique ⋮ em e, em seguida, clique em **alterar senha**. 2. Introduza a nova palavra-passe e confirme-a.
Ativar um utilizador	1. Marque a caixa ao lado de cada usuário desativado que você deseja habilitar. 2. Clique Enable em .

Desative um usuário	1. Marque a caixa ao lado de cada usuário habilitado que você deseja desativar. 2. Clique Disable em .

Exibir usuários e grupos UNIX

No System Manager, você pode exibir uma lista de usuários e grupos UNIX.

Passos

1. No System Manager, clique em **Storage > Storage VMs**.
2. Selecione a VM de armazenamento e, em seguida, selecione a guia **Configurações**.
3. Role até a área **Host Users and Groups**.

   A seção **UNIX** exibe um resumo do número de usuários em cada grupo associado à VM de armazenamento selecionada.

4. Clique → na seção **UNIX**.
5. Clique na guia **Groups** para exibir detalhes sobre esse grupo.
6. Para exibir os usuários em um grupo, selecione o grupo e clique na guia **usuários**.

Adicione, edite ou exclua um grupo UNIX

No System Manager, você pode gerenciar grupos UNIX adicionando, editando ou excluindo-os.

Passos

1. No System Manager, veja a lista de grupos UNIX. Exibir usuários e grupos UNIXConsulte a .
2. Na guia **Groups**, você pode gerenciar grupos com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um grupo	1. Clique + Add em . 2. Introduza as informações do grupo. 3. (Opcional) Especifique usuários associados.
Edite um grupo	1. Selecione o grupo. 2. Clique Edit em . 3. Modifique as informações do grupo. 4. (Opcional) Adicionar ou remover usuários.
Eliminar um grupo	1. Selecione o grupo ou grupos que deseja excluir. 2. Clique Delete em .

Gerenciar usuários UNIX

No System Manager, você pode gerenciar usuários do Windows adicionando, editando ou excluindo-os.

Passos

1. No System Manager, visualize a lista de utilizadores do grupo. Exibir usuários e grupos UNIXConsulte a .
2. Na guia **usuários**, você pode gerenciar usuários com as seguintes tarefas:

Para executar esta ação…	Execute estas etapas…
Adicionar um utilizador	1. Clique + Add em . 2. Introduza as informações do utilizador.
Editar um utilizador	1. Selecione o utilizador que pretende editar. 2. Clique Edit em . 3. Modifique as informações do usuário.
Eliminar um utilizador	1. Selecione o utilizador ou utilizadores que pretende eliminar. 2. Clique Delete em .

Monitorar clientes ativos NFS

A partir do ONTAP 9.8, o Gerenciador de sistema mostra quais conexões de cliente NFS estão ativas quando o NFS é licenciado em um cluster.

Isso permite verificar rapidamente quais clientes NFS estão ativamente conetados a uma VM de storage, que estão conetados, mas ociosos, e quais são desconetados.

Para cada endereço IP do cliente NFS, o visor **Clientes NFS** mostra: * Hora do último acesso * Endereço IP da interface de rede * versão da conexão NFS * Nome da VM de armazenamento

Além disso, uma lista de clientes NFS ativos nas últimas 48 horas também é mostrada na exibição **Storage>volumes** e uma contagem de clientes NFS é incluída na exibição **Dashboard**.

Passo

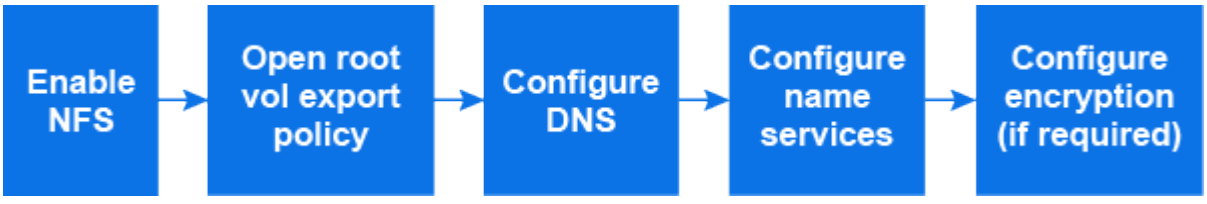
1. Exibir atividade do cliente NFS: Clique em **hosts > clientes NFS**.

Ative o armazenamento nas

Ative o storage nas para servidores Linux usando NFS

Crie ou modifique VMs de storage para habilitar servidores NFS para fornecer dados a clientes Linux.

Ative uma VM de storage nova ou existente para o protocolo NFS usando este procedimento.



Antes de começar

Certifique-se de que anotou os detalhes de configuração de qualquer rede, autenticação ou serviços de segurança necessários no seu ambiente.

Passos

1. Habilite o NFS em uma VM de storage.
   - Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable NFS**.
     i. Confirme o idioma predefinido.
     ii. Adicione interfaces de rede.
     iii. Atualizar as informações da conta do administrador da VM de armazenamento (opcional).
   - Para VMs de armazenamento existentes: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento, clique em **Settings** e, em seguida, clique em **NFS**.
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name* _root) e, em seguida, clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: NFS
      - Detalhes de acesso: UNIX Read-only
3. Configurar DNS para resolução de nome de host: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento, clique em **Configurações** e, em seguida, clique em **DNS**.
4. Configure os serviços de nomes conforme necessário.
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em for LDAP ou NIS.
   b. Clique no mosaico Name Services Switch para incluir quaisquer alterações.
5. Configure a encriptação, se necessário:

Configurar TLS para clientes NFS

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Passos

1. Consulte "requisitos"o para NFS sobre TLS antes de começar.
2. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
3. No bloco **NFS**, clique em **NFS over TLS settings**.
4. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
5. Clique em ⋮ para essa interface.
6. Clique em **Ativar**.
7. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
8. Clique em **Salvar**.

Configurar Kerberos

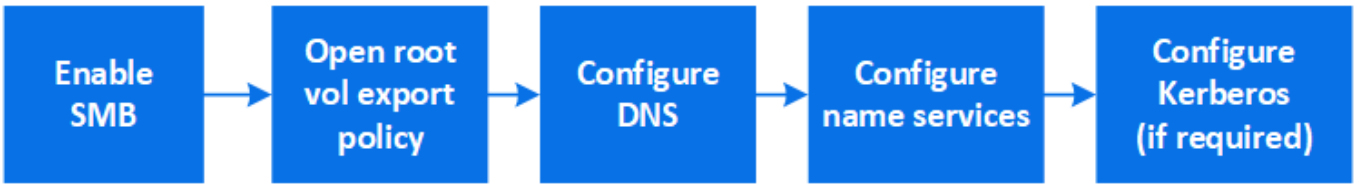
Passos

1. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
2. Clique →no mosaico Kerberos e, em seguida, clique em **Add**.

Ative o armazenamento nas para servidores Windows usando SMB

Crie ou modifique VMs de storage para habilitar servidores SMB para fornecer dados aos clientes Windows.

Este procedimento permite uma VM de storage nova ou existente para o protocolo SMB. Supõe-se que os detalhes de configuração estejam disponíveis para qualquer rede, autenticação ou serviços de segurança necessários em seu ambiente.



Passos

1. Habilite o SMB em uma VM de storage.
   a. Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable SMB/CIFS**.

- Introduza as seguintes informações:
  - Nome e senha do administrador
  - Nome do servidor
  - Domínio do diretório ativo
- Confirme a unidade organizacional.
- Confirme os valores DNS.
- Confirme o idioma predefinido.
- Adicione interfaces de rede.
- Atualizar as informações da conta do administrador da VM de armazenamento (opcional).

b. Para VMs de armazenamento existentes:: Clique em **armazenamento > armazenamento de VMs**, selecione uma VM de armazenamento, clique em **Configurações** e, em seguida, clique em **SMB**.

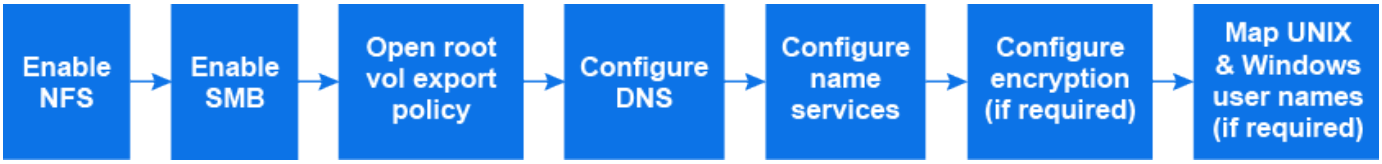
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name_root*) e clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: SMB
      - Detalhes de acesso: NTFS somente leitura
3. Configurar DNS para resolução de nome de host:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e, em seguida, clique em **DNS**.
   b. Mude para o servidor DNS e mapeie o servidor SMB.
      - Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP da interface de rede de dados.
      - Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico de alias (CNAME resource record) para mapear cada alias para o endereço IP da interface de rede de dados do servidor SMB.
4. Configure os serviços de nomes conforme necessário
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em **LDAP** ou **NIS**.
   b. Inclua quaisquer alterações no arquivo de switch de serviços de nome: Clique em **Name Services Switch**.
5. Configure Kerberos se necessário:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
   b. Clique em **Kerberos** e, em seguida, clique em **Add**.

Habilite o storage nas para Windows e Linux usando NFS e SMB

Crie ou modifique VMs de storage para permitir que os servidores NFS e SMB forneçam dados a clientes Linux e Windows.

Habilite uma VM de storage nova ou existente para atender aos protocolos NFS e SMB usando este

procedimento.



Antes de começar

Certifique-se de que anotou os detalhes de configuração de qualquer rede, autenticação ou serviços de segurança necessários no seu ambiente.

Passos

1. Habilite NFS e SMB em uma VM de storage.
   a. Para novas VMs de armazenamento: Clique em **Storage > Storage VMs**, clique em **Add**, insira um nome de VM de armazenamento e, na guia **SMB/CIFS, NFS, S3**, selecione **Enable SMB/CIFS** e **Enable NFS**.
   b. Introduza as seguintes informações:
      - Nome e senha do administrador
      - Nome do servidor
      - Domínio do diretório ativo
   c. Confirme a unidade organizacional.
   d. Confirme os valores DNS.
   e. Confirme o idioma predefinido.
   f. Adicione interfaces de rede.
   g. Atualizar as informações da conta do administrador da VM de armazenamento (opcional).
   h. Para VMs de armazenamento existentes: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento e clique em **Settings**. Conclua as subetapas a seguir se NFS ou SMB ainda não estiver habilitado.
      - Clique em **NFS**.
      - Clique em **SMB**.
2. Abra a política de exportação do volume raiz da VM de storage:
   a. Clique em **Storage > volumes**, selecione o volume raiz da VM de armazenamento (que por padrão é *volume-name_root*) e clique na política exibida em **Export Policy**.
   b. Clique em **Add** para adicionar uma regra.
      - Especificação do cliente `0.0.0.0/0`
      - Protocolos de acesso: NFS
      - Detalhes de acesso: Somente leitura NFS
3. Configurar DNS para resolução de nome de host:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e, em seguida, clique em **DNS**.
   b. Quando a configuração DNS estiver concluída, mude para o servidor DNS e mapeie o servidor SMB.
      - Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP da interface de rede de dados.

- Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico de alias (CNAME resource record) para mapear cada alias para o endereço IP da interface de rede de dados do servidor SMB.

4. Configure os serviços de nomes conforme necessário:
   a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento, clique em **Settings** e clique em for LDAP ou NIS.
   b. Inclua quaisquer alterações no arquivo de switch de serviços de nome: Clique em **Name Services Switch**.
5. Configure a autenticação e a criptografia, se necessário:

Configurar TLS para clientes NFS

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Passos

a. Consulte "requisitos"o para NFS sobre TLS antes de começar.
b. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
c. No bloco **NFS**, clique em **NFS over TLS settings**.
d. Na área **NFS over TLS settings**, selecione uma interface de rede NFS para a qual deseja ativar o TLS.
e. Clique em para essa interface.
f. Clique em **Ativar**.
g. Na caixa de diálogo **Configuração TLS da interface de rede**, inclua um certificado para uso com TLS selecionando uma das seguintes opções:
   - **Certificado instalado**: Escolha um certificado previamente instalado na lista suspensa.
   - **Novo certificado**: Escolha um nome comum para o certificado.
   - **Certificado assinado por CA externo**: Siga as instruções para colar o conteúdo do seu certificado e chave privada nas caixas.
h. Clique em **Salvar**.

Configurar Kerberos

Passos

a. Clique em **Storage > Storage VMs**, selecione a VM de armazenamento e clique em **Settings**.
b. Clique no mosaico Kerberos e, em seguida, clique em **Add**.

6. Mapeie nomes de usuário UNIX e Windows, se necessário: Clique em **Mapeamento de nomes** e clique em **Adicionar**.

   Você deve fazer isso somente se o seu site tiver contas de usuário do Windows e UNIX que não mapeem implicitamente, ou seja, quando a versão minúscula de cada nome de usuário do Windows corresponder ao nome de usuário do UNIX. Você pode mapear nomes de usuários usando LDAP, NIS ou usuários locais. Se você tiver dois conjuntos de usuários que não correspondem, você deve configurar o mapeamento de nomes.

Configurar o NFS com a CLI

Visão geral da configuração de NFS com a CLI

Você pode usar os comandos de CLI do ONTAP 9 para configurar o acesso de cliente NFS a arquivos contidos em um novo volume ou qtree em uma máquina virtual de storage (SVM) nova ou existente.

Utilize estes procedimentos se pretender configurar o acesso a um volume ou qtree da seguinte forma:

- Você deseja usar qualquer versão do NFS atualmente compatível com ONTAP: NFSv3, NFSv4, NFSv4,1, NFSv4,2 ou NFSv4,1 com pNFS.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

  Para usar o System Manager para configurar o acesso multiprotocolo nas, "Provisionar storage nas para Windows e Linux usando NFS e SMB"consulte .

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.

  Detalhes sobre a sintaxe de comando estão disponíveis nas páginas de ajuda CLI e man do ONTAP.

- As permissões de arquivo UNIX serão usadas para proteger o novo volume.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

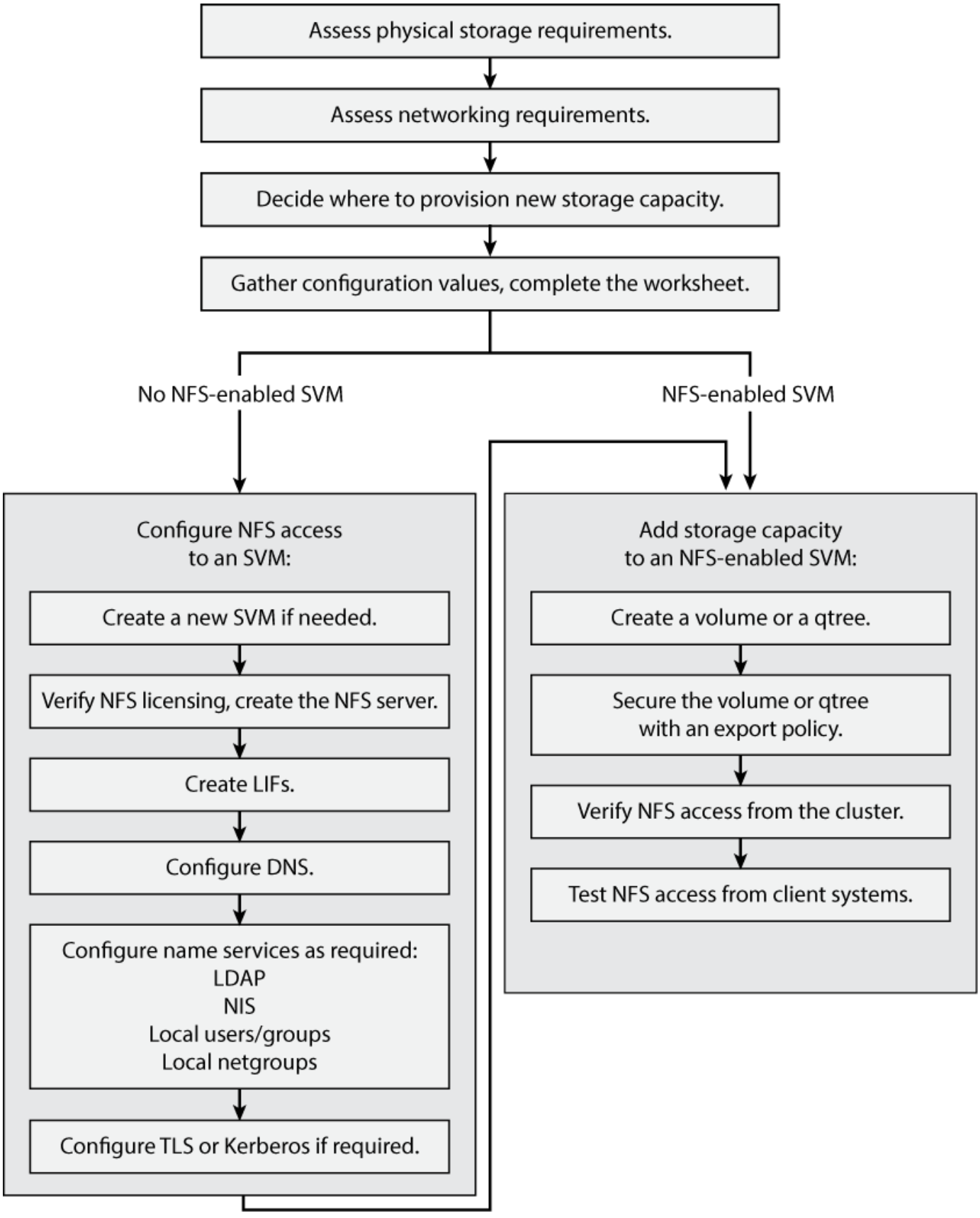
Se quiser obter detalhes sobre a gama de capacidades do protocolo NFS da ONTAP, consulte o "Visão geral de referência de NFS".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Consulte…
O Gerenciador de sistema redesenhado (disponível com o ONTAP 9.7 e posterior)	"Provisione storage nas para servidores Linux usando NFS"
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores	"Visão geral da configuração NFS"

Fluxo de trabalho de configuração NFS

A configuração do NFS envolve a avaliação dos requisitos de rede e storage físico e, depois, a escolha de um fluxo de trabalho específico para sua meta: Configurar o acesso NFS a uma nova SVM ou existente, ou adicionar um volume ou qtree a uma SVM existente que já esteja totalmente configurada para acesso ao NFS.


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

Preparação

Avaliar os requisitos de armazenamento físico

Antes de provisionar o storage NFS para clientes, você deve garantir que haja espaço suficiente em um agregado existente para o novo volume. Se não houver, você poderá adicionar discos a um agregado existente ou criar um novo agregado do tipo desejado.

Passos

1. Exibir espaço disponível em agregados existentes:

   ```
   storage aggregate show
   ```

   Se houver um agregado com espaço suficiente, Registre seu nome na Planilha.

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Se não houver agregados com espaço suficiente, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede

Antes de fornecer storage NFS aos clientes, verifique se a rede está configurada corretamente para atender aos requisitos de provisionamento de NFS.

O que você vai precisar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)

- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Passos

1. Exiba as portas físicas e virtuais disponíveis:

   `network port show`

   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis

   `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis:

   `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster:

   `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decidir onde provisionar nova capacidade de storage NFS

Antes de criar um novo volume ou qtree NFS, você precisa decidir se deseja colocá-lo em uma SVM nova ou existente e quanto de configuração o SVM precisa. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um volume ou qtree em um novo SVM ou em um SVM existente que tenha o NFS habilitado, mas não configurado, siga as etapas em "Configurar acesso NFS a um SVM" e "Adicionar storage NFS a um SVM habilitado para NFS".

  Configurar o acesso NFS a uma SVM

  Adicionar storage NFS a uma SVM habilitada para NFS

  Você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando o NFS em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja habilitar o suporte a NFS.

◦ Você tem um ou mais SVMs habilitados para NFS em um cluster e deseja outro servidor NFS em um namespace isolado (cenário de alocação a vários clientes). Você também deve escolher essa opção para provisionar storage em uma SVM existente que tenha o NFS habilitado, mas não configurado. Esse pode ser o caso se você criou o SVM para acesso à SAN ou se nenhum protocolo foi habilitado quando o SVM foi criado.

Depois de ativar o NFS no SVM, proceda ao provisionamento de um volume ou qtree.

- Se você quiser provisionar um volume ou qtree em uma SVM atual totalmente configurada para acesso NFS, siga as etapas em "adicionando storage NFS a uma SVM habilitado para NFS".

  Adição de storage NFS a uma SVM habilitada para NFS

Planilha para coletar informações de configuração de NFS

A Planilha de configuração NFS permite coletar as informações necessárias para configurar o acesso NFS para clientes.

Você deve completar uma ou ambas as seções da Planilha, dependendo da decisão tomada sobre onde provisionar o armazenamento:

Se você estiver configurando o acesso NFS a uma SVM, deve concluir ambas as seções.

- Configurando o acesso NFS a uma SVM
- Adição de capacidade de storage a um SVM habilitado para NFS

Se você estiver adicionando capacidade de storage a um SVM habilitado para NFS, deverá concluir apenas:

- Adição de capacidade de storage a um SVM habilitado para NFS

Configurar o acesso NFS a uma SVM

Parâmetros para criar um SVM

Você fornece esses valores com o `vserver create` comando se estiver criando um novo SVM.

Campo	Descrição	O seu valor
`-vserver`	Nome fornecido para o novo SVM que é um nome de domínio totalmente qualificado (FQDN) ou que segue outra convenção que impõe nomes exclusivos de SVM em um cluster.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para uma nova capacidade de storage NFS.	
`-rootvolume`	Um nome exclusivo fornecido para o volume raiz da SVM.	

`-rootvolume-security-style`	Use o estilo de segurança UNIX para SVM.	`unix`
`-language`	Use a configuração de idioma padrão neste fluxo de trabalho.	`C.UTF-8`
`ipspace`	Os IPspaces são espaços de endereço IP distintos nos quais residem (máquinas virtuais de armazenamento (SVMs)).	

Parâmetros para criar um servidor NFS

Você fornece esses valores com o `vserver nfs create` comando ao criar um novo servidor NFS e especificar versões NFS compatíveis.

Se estiver a ativar o NFSv4 ou posterior, deve utilizar o LDAP para melhorar a segurança.

Campo	Descrição	O seu valor
`-v3 -v4.0, , -v4.1, , -v4.1 -pnfs`	Habilite versões NFS conforme necessário. O v4,2 também é suportado no ONTAP 9.8 e posterior quando `v4.1` está ativado.	
`-v4-id-domain`	Nome de domínio de mapeamento de ID.	
`-v4-numeric-ids`	Suporte para IDs de proprietário numéricos (ativado ou desativado).	

Parâmetros para ativar a criptografia TLS para conexões NFS

Você fornece esses valores com o `vserver nfs tls interface enable` comando.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Campo	Descrição	O seu valor
`-vserver`	O vserver no qual a interface lógica existe.	

`-lif`	O nome da interface lógica na qual você deseja habilitar a criptografia em trânsito usando NFS sobre TLS.	
`-certificate-name`	O nome do certificado X,509 configurado na VM de armazenamento.	

Parâmetros para criar um LIF

Você fornece esses valores com o `network interface create` comando quando você está criando LIFs.

Se você estiver usando Kerberos, você deve habilitar Kerberos em várias LIFs.

Campo	Descrição	O seu valor
`-lif`	Um nome que você fornece para o novo LIF.	
`-role`	Use a função de LIF de dados neste fluxo de trabalho.	`data`
`-data-protocol`	Utilize apenas o protocolo NFS neste fluxo de trabalho.	`nfs`
`-home-node`	O nó ao qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-home-port`	A porta ou grupo de interface para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-address`	O endereço IPv4 ou IPv6 no cluster que será usado para acesso aos dados pelo novo LIF.	
`-netmask`	A máscara de rede e o gateway para o LIF.	
`-subnet`	Um conjunto de endereços IP. Usado em vez `-address` de e `-netmask` para atribuir endereços e netmasks automaticamente.	

`-firewall-policy`	Use a política de firewall de dados padrão neste fluxo de trabalho.	`data`

Parâmetros para resolução de nome de host DNS

Você fornece esses valores com o `vserver services name-service dns create` comando quando você está configurando o DNS.

Campo	Descrição	O seu valor
`-domains`	Até cinco nomes de domínio DNS.	
`-name-servers`	Até três endereços IP para cada servidor de nomes DNS.	

Informações do serviço de nomes

Parâmetros para criar usuários locais

Você fornece esses valores se estiver criando usuários locais usando o `vserver services name-service unix-user create` comando. Se você estiver configurando usuários locais carregando um arquivo contendo usuários UNIX de um identificador de recurso uniforme (URI), não será necessário especificar esses valores manualmente.

	Nome de utilizador (`-user`)	ID de utilizador (`-id`)	ID do grupo (`-primary-gid`)	Nome completo (`-full-name`)
Exemplo	johnm	123	100	John Miller
1				
2				
3				
…				
n				

Parâmetros para criar grupos locais

Você fornece esses valores se estiver criando grupos locais usando o `vserver services name-service unix-group create` comando. Se você estiver configurando grupos locais carregando um arquivo contendo grupos UNIX de um URI, não será necessário especificar esses valores manualmente.

	Nome do grupo (`-name`)	ID do grupo (`-id`)
Exemplo	Engenharia	100

1		
2		
3		
…		
n		

Parâmetros para NIS

Você fornece esses valores com o `vserver services name-service nis-domain create` comando.

A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

Campo	Descrição	O seu valor
`-domain`	O domínio NIS que o SVM usará para pesquisas de nomes.	
`-active`	O servidor de domínio NIS ativo.	`true` ou `false`
`-servers`	ONTAP 9.0, 9,1: Um ou mais endereços IP de servidores NIS usados pela configuração do domínio NIS.	
`-nis-servers`	ONTAP 9.2: Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores NIS usados pela configuração do domínio.	

Parâmetros para LDAP

Você fornece esses valores com o `vserver services name-service ldap client create` comando.

Você também precisará de um arquivo de certificado CA raiz autoassinado `.pem`.

A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM para o qual você deseja criar uma configuração de cliente LDAP.	
`-client-config`	O nome atribuído para a nova configuração de cliente LDAP.	
`-servers`	ONTAP 9.0, 9,1: Um ou mais servidores LDAP por endereço IP em uma lista separada por vírgulas.	
`-ldap-servers`	ONTAP 9.2: Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores LDAP.	
`-query-timeout`	Utilize os segundos predefinidos `3` para este fluxo de trabalho.	`3`
`-min-bind-level`	O nível mínimo de autenticação BIND. A predefinição é `anonymous`. Deve ser definido como `sasl` se a assinatura e a vedação estiverem configuradas.	
`-preferred-ad-servers`	Um ou mais servidores preferenciais do ative Directory por endereço IP em uma lista delimitada por vírgulas.	
`-ad-domain`	O domínio do ative Directory.	
`-schema`	O modelo de esquema a ser usado. Você pode usar um esquema padrão ou personalizado.	
`-port`	Utilize a porta de servidor LDAP predefinida `389` para este fluxo de trabalho.	`389`
`-bind-dn`	O nome distinto do usuário Bind.	
`-base-dn`	A base distinguiu o nome. O padrão é `""` (root).	

Campo	Descrição	O seu valor
`-base-scope`	Use o escopo de pesquisa base padrão `subnet` para esse fluxo de trabalho.	`subnet`
`-session-security`	Ativa a assinatura ou assinatura LDAP e a vedação. A predefinição é `none`.	
`-use-start-tls`	Ativa LDAP em TLS. A predefinição é `false`.	

Parâmetros para autenticação Kerberos

Você fornece esses valores com o `vserver nfs kerberos realm create` comando. Alguns dos valores serão diferentes dependendo se você usa o Microsoft ative Directory como um servidor KDC (Key Distribution Center), ou MIT ou outro servidor KDC UNIX.

Campo	Descrição	O seu valor
`-vserver`	O SVM que se comunicará com o KDC.	
`-realm`	O Reino Kerberos.	
`-clock-skew`	Desvio de relógio permitido entre clientes e servidores.	
`-kdc-ip`	Endereço IP KDC.	
`-kdc-port`	Número da porta KDC.	
`-adserver-name`	Apenas Microsoft KDC: Nome do servidor DE ANÚNCIOS.	
`-adserver-ip`	Apenas Microsoft KDC: Endereço IP do servidor DE ANÚNCIOS.	
`-adminserver-ip`	UNIX KDC apenas: Endereço IP do servidor de administração.	
`-adminserver-port`	UNIX KDC apenas: Número da porta do servidor de administração.	
`-passwordserver-ip`	UNIX KDC apenas: Endereço IP do servidor de senha.	

`-passwordserver-port`	UNIX KDC apenas: Porta do servidor de senha.	
`-kdc-vendor`	Fornecedor de KDC.	Clique `Microsoft` em `Other` OK
`-comment`	Quaisquer comentários desejados.	

Você fornece esses valores com o `vserver nfs kerberos interface enable` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM para o qual você deseja criar uma configuração Kerberos.	
`-lif`	O LIF de dados no qual você ativará o Kerberos. Você pode ativar o Kerberos em várias LIFs.	
`-spn`	O nome do princípio de serviço (SPN)	
`-permitted-enc-types`	Os tipos de criptografia permitidos para Kerberos sobre NFS; `aes-256` são recomendados, dependendo dos recursos do cliente.	
`-admin-username`	As credenciais do administrador do KDC para recuperar a chave secreta do SPN diretamente do KDC. É necessária uma palavra-passe	
`-keytab-uri`	O arquivo keytab do KDC que contém a chave SPN se você não tiver credenciais de administrador KDC.	
`-ou`	A unidade organizacional (ou) sob a qual a conta de servidor do Microsoft ative Directory será criada quando você ativar o Kerberos usando um realm para o Microsoft KDC.	

Parâmetros para criar políticas e regras de exportação

Você fornece esses valores com o `vserver export-policy create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM que hospedará o novo volume.	
`-policyname`	Um nome fornecido para uma nova política de exportação.	

Você fornece esses valores para cada regra com o `vserver export-policy rule create` comando.

Campo	Descrição	O seu valor
`-clientmatch`	Especificação de correspondência do cliente.	
`-ruleindex`	Posição da regra de exportação na lista de regras.	
`-protocol`	Use NFS neste fluxo de trabalho.	`nfs`
`-rorule`	Método de autenticação para acesso somente leitura.	
`-rwrule`	Método de autenticação para acesso de leitura e gravação.	
`-superuser`	Método de autenticação para acesso de superusuário.	
`-anon`	ID de usuário para o qual usuários anônimos são mapeados.	

Você deve criar uma ou mais regras para cada política de exportação.

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
Exemplos	0,0.0,0/0	qualquer	krb5	sistema	65534
1					
2					

3					
…					
n					

Parâmetros para criar um volume

Você fornece esses valores com o `volume create` comando se estiver criando um volume em vez de uma qtree.

Campo	Descrição	O seu valor
`-vserver`	Nome de uma SVM nova ou existente que hospedará o novo volume.	
`-volume`	Um nome descritivo exclusivo que você fornece para o novo volume.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para o novo volume NFS.	
`-size`	Um número inteiro fornecido para o tamanho do novo volume.	
`-user`	Nome ou ID do usuário que é definido como o proprietário da raiz do volume.	
`-group`	Nome ou ID do grupo definido como o proprietário da raiz do volume.	
`--security-style`	Use o estilo de segurança UNIX para este fluxo de trabalho.	`unix`
`-junction-path`	Localização sob a raiz (/) onde o novo volume deve ser montado.	
`-export-policy`	Se estiver a planear utilizar uma política de exportação existente, pode introduzir o respetivo nome quando criar o volume.	

Parâmetros para criar uma qtree

Você fornece esses valores com o `volume qtree create` comando se estiver criando uma qtree em vez de um volume.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual reside o volume que contém a qtree.	
`-volume`	O nome do volume que conterá a nova qtree.	
`-qtree`	Um nome descritivo exclusivo que você fornece para a nova qtree, 64 carateres ou menos.	
`-qtree-path`	O argumento de caminho de qtree no formato `/vol/volume_name/qtree_name\>` pode ser especificado em vez de especificar volume e qtree como argumentos separados.	
`-unix-permissions`	Opcional: As permissões UNIX para a qtree.	
`-export-policy`	Se você estiver planejando usar uma política de exportação existente, poderá inserir seu nome ao criar a qtree.	

Informações relacionadas

- "Referência do comando ONTAP"

Configurar o acesso NFS a uma SVM

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso a dados a clientes NFS, será necessário criá-lo.

Antes de começar

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

Passos

1. Criar um SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
```

ipspace_name

- Utilize a definição UNIX para a `-rootvolume-security-style` opção.
- Utilize a opção C.UTF-8 predefinida `-language`.
- A `ipspace` definição é opcional.

2. Verifique a configuração e o status do SVM recém-criado:

`vserver show -vserver` *vserver_name*

```
`Allowed Protocols`O campo deve incluir NFS. Você pode editar esta lista
mais tarde.
```

O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no ipspace ipspaceA:

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Verifique se o protocolo NFS está habilitado no SVM

Antes de configurar e usar NFS em SVMs, você deve verificar se o protocolo está ativado.

Sobre esta tarefa

Isso geralmente é feito durante a configuração do SVM, mas se você não ativou o protocolo durante a configuração, poderá ativá-lo mais tarde usando o `vserver add-protocols` comando.

Não é possível adicionar ou remover um protocolo de um LIF depois de criado.

Você também pode desativar protocolos em SVMs usando o `vserver remove-protocols` comando.

Passos

1. Verifique quais protocolos estão atualmente ativados e desativados para o SVM:

```
vserver show -vserver vserver_name -protocols
```

Você também pode usar o `vserver show-protocols` comando para exibir os protocolos atualmente habilitados em todos os SVMs no cluster.

2. Se necessário, ative ou desative um protocolo:
   - Para ativar o protocolo NFS
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - Para desativar um protocolo
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. Confirme se os protocolos ativados e desativados foram atualizados corretamente:

```
vserver show -vserver vserver_name -protocols
```

Exemplo

O comando a seguir exibe quais protocolos estão atualmente ativados e desativados (permitidos e não permitidos) no SVM chamado VS1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

O comando a seguir permite o acesso por NFS adicionando `nfs` à lista de protocolos habilitados no SVM chamado VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

Abra a política de exportação do volume raiz da SVM

A política de exportação padrão do volume raiz da SVM deve incluir uma regra para permitir que todos os clientes tenham acesso aberto por meio do NFS. Sem essa regra, todos os clientes NFS têm acesso negado ao SVM e seus volumes.

Sobre esta tarefa

Quando um novo SVM é criado, uma política de exportação padrão (chamada padrão) é criada automaticamente para o volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM.

Você deve verificar se o acesso está aberto a todos os clientes NFS na política de exportação padrão e, mais tarde, restringir o acesso a volumes individuais criando políticas de exportação personalizadas para volumes individuais ou qtrees.

Passos

1. Se você estiver usando uma SVM existente, verifique a política de exportação de volume raiz padrão:

```
vserver export-policy rule show
```

A saída do comando deve ser semelhante ao seguinte:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

Se existir uma regra que permita o acesso aberto, esta tarefa está concluída. Caso contrário, avance para o passo seguinte.

2. Crie uma regra de exportação para o volume raiz da SVM:

   ```
   vserver export-policy rule create -vserver vserver_name -policyname default
   -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
   -superuser any
   ```

   Se o SVM contiver apenas volumes protegidos pelo Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` ou `krb5i`. Por exemplo:

   ```
   -rorule krb5i -rwrule krb5i -superuser krb5i
   ```

3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultado

Qualquer cliente NFS agora pode acessar qualquer volume ou qtree criado no SVM.

Crie um servidor NFS

Depois de verificar se o NFS está licenciado no cluster, você pode usar o `vserver nfs create` comando para criar um servidor NFS no SVM e especificar as versões NFS compatíveis.

Sobre esta tarefa

O SVM pode ser configurado para dar suporte a uma ou mais versões de NFS. Se você estiver apoiando NFSv4 ou posterior:

- O nome de domínio de mapeamento de ID de usuário NFSv4 deve ser o mesmo no servidor NFSv4 e nos clientes de destino.

  Ele não precisa necessariamente ser o mesmo que um nome de domínio LDAP ou NIS, desde que o servidor NFSv4 e os clientes estejam usando o mesmo nome.

- Os clientes-alvo devem suportar a configuração de ID numérica NFSv4.
- Por motivos de segurança, você deve usar o LDAP para serviços de nome em implantações NFSv4.

Antes de começar

O SVM deve ter sido configurado para permitir o protocolo NFS.

Passos

1. Verifique se o NFS está licenciado no cluster:

   ```
   system license show -package nfs
   ```

   Se não estiver, contacte o seu representante de vendas.

2. Criar um servidor NFS:

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   Você pode optar por ativar qualquer combinação de versões NFS. Se você quiser dar suporte ao pNFS, habilite as `-v4.1` opções e `-v4.1-pnfs` .

   Se você ativar o v4 ou posterior, também deve ter certeza de que as seguintes opções estão definidas corretamente:

   - `-v4-id-domain`

     Este parâmetro opcional especifica a parte do domínio da forma de cadeia de carateres de nomes de usuário e grupo, conforme definido pelo protocolo NFSv4. Por padrão, o ONTAP usa o domínio NIS se um estiver definido; caso contrário, o domínio DNS será usado. Você deve fornecer um valor que corresponda ao nome de domínio usado pelos clientes de destino.

   - `-v4-numeric-ids`

     Este parâmetro opcional especifica se o suporte para identificadores de cadeia de carateres numéricos em atributos de proprietário NFSv4 está habilitado. A configuração padrão é ativada, mas você deve verificar se os clientes de destino a suportam.

   Você pode ativar recursos NFS adicionais mais tarde usando o `vserver nfs modify` comando.

3. Verifique se o NFS está em execução:

   ```
   vserver nfs status -vserver vserver_name
   ```

4. Verifique se o NFS está configurado conforme desejado:

   ```
   vserver nfs show -vserver vserver_name
   ```

Exemplos

O comando a seguir cria um servidor NFS no SVM chamado VS1 com NFSv3 e NFSv4,0 ativados:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

Os comandos a seguir verificam os valores de status e configuração do novo servidor NFS chamado VS1:

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                    General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                  Default Windows User: -
                   NFSv4.0 ACL Support: disabled
      NFSv4.0 Read Delegation Support: disabled
     NFSv4.0 Write Delegation Support: disabled
              NFSv4 ID Mapping Domain: my_domain.com
...
```

Crie um LIF

Um LIF é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

O que você vai precisar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.

- Se você estiver usando a autenticação Kerberos, ative o Kerberos em várias LIFs.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

A partir do ONTAP 9.4, o FC-NVMe é compatível. Se você estiver criando um LIF FC-NVMe, deve estar ciente do seguinte:

- O protocolo NVMe precisa ser compatível com o adaptador FC no qual o LIF é criado.
- O FC-NVMe pode ser o único protocolo de dados em LIFs de dados.
- Um tráfego de gerenciamento de manipulação de LIF deve ser configurado para cada máquina virtual de storage (SVM) que suporte SAN.
- Os LIFs e namespaces NVMe devem ser hospedados no mesmo nó.
- Somente um LIF NVMe que manipula o tráfego de dados pode ser configurado por SVM

Passos

1. Criar um LIF:

   `network interface create -vserver vserver_name -lif lif_name -role data -data -protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto -revert {true|false}`

Opção	Descrição
ONTAP 9 .5 e anteriores	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
ONTAP 9 1.6 e posterior	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

   - `-role`O parâmetro não é necessário ao criar um LIF usando uma política de serviço (a partir do ONTAP 9,6).
   - O `-data-protocol` parâmetro deve ser especificado quando o LIF é criado e não pode ser modificado mais tarde sem destruir e recriar o LIF de dados.

O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).

- `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

  Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.

2. Verifique se o LIF foi criado com sucesso usando o `network interface show` comando.
3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

4. Se você estiver usando Kerberos, repita as etapas 1 a 3 para criar LIFs adicionais.

   O Kerberos deve ser habilitado separadamente em cada um desses LIFs.

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

O comando a seguir mostra como criar um LIF de dados nas atribuído com a `default-data-files` política de serviço:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Ative DNS para resolução de nome de host

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os

nomes de host são resolvidos usando servidores DNS externos.

O que você vai precisar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

O *Network Management Guide* contém informações sobre a configuração de DNS dinâmico na SVM.

Passos

1. Habilite o DNS na SVM:

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ⓘ A partir do ONTAP 9.2, o `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Exiba as configurações do domínio DNS usando o `vserver services name-service dns show` comando.

   O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

   ```
   vserver services name-service dns show
                                                Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

   O `vserver services name-service dns check` comando está disponível a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configurar serviços de nomes

Configure a visão geral dos serviços de nome

Dependendo da configuração do seu sistema de storage, o ONTAP precisa ser capaz de procurar informações de host, usuário, grupo ou netgroup para fornecer acesso adequado aos clientes. Você deve configurar serviços de nomes para permitir que o ONTAP acesse serviços de nomes locais ou externos para obter essas informações.

Você deve usar um serviço de nomes como NIS ou LDAP para facilitar pesquisas de nomes durante a autenticação do cliente. É melhor usar o LDAP sempre que possível para maior segurança, especialmente ao implantar o NFSv4 ou posterior. Você também deve configurar usuários e grupos locais caso os servidores de nomes externos não estejam disponíveis.

As informações do serviço de nomes devem ser mantidas sincronizadas em todas as fontes.

Configure a tabela do switch do serviço de nomes

Você deve configurar a tabela de switch de serviço de nomes corretamente para permitir que o ONTAP consulte serviços de nome locais ou externos para recuperar informações de mapeamento de host, usuário, grupo, netgroup ou nome.

O que você vai precisar

Você deve ter decidido quais serviços de nome deseja usar para o mapeamento de host, usuário, grupo, grupo de rede ou nome, conforme aplicável ao seu ambiente.

Se você planeja usar netgroups, todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

Sobre esta tarefa

Não inclua fontes de informação que não estejam a ser utilizadas. Por exemplo, se o NIS não estiver sendo usado em seu ambiente, não especifique a `-sources nis` opção.

Passos

1. Adicione as entradas necessárias à tabela do switch de serviço de nomes:

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. Verifique se a tabela do switch de serviço de nomes contém as entradas esperadas na ordem desejada:

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   Se pretender efetuar quaisquer correções, tem de utilizar os `vserver services name-service ns-switch modify` comandos ou `vserver services name-service ns-switch delete`.

Exemplo

O exemplo a seguir cria uma nova entrada na tabela de opções de serviço de nomes para o SVM VS1 usar o arquivo netgroup local e um servidor NIS externo para procurar informações de netgroup nessa ordem:

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

Depois de terminar

- Você precisa configurar os serviços de nome especificados para o SVM para fornecer acesso aos dados.
- Se você excluir qualquer serviço de nomes para o SVM, também será necessário removê-lo da tabela de opções de serviços de nomes.

  O acesso do cliente ao sistema de armazenamento pode não funcionar como esperado, se você não conseguir excluir o serviço de nomes da tabela de opções do serviço de nomes.

Configurar usuários e grupos UNIX locais

Configure a visão geral de usuários e grupos UNIX locais

Você pode usar usuários e grupos UNIX locais no SVM para mapeamentos de nomes e autenticação. Você pode criar usuários e grupos UNIX manualmente ou carregar um arquivo contendo usuários ou grupos UNIX a partir de um identificador de recurso uniforme (URI).

Há um limite máximo padrão de 32.768 grupos de usuários UNIX locais e membros de grupo combinados no cluster. O administrador do cluster pode modificar este limite.

Crie um usuário local do UNIX

Você pode usar o `vserver services name-service unix-user create` comando para criar usuários UNIX locais. Um usuário UNIX local é um usuário UNIX criado no SVM como uma opção de serviços de nome UNIX para ser usado no processamento de mapeamentos de nomes.

Passo

1. Criar um usuário local UNIX:

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* especifica o nome de usuário. O comprimento do nome de utilizador tem de ter 64 carateres ou menos.

   `-id` *`integer`* Especifica a ID de usuário que você atribui.

   `-primary-gid` *`integer`* Especifica o ID do grupo principal. Isso adiciona o usuário ao grupo principal. Depois de criar o usuário, você pode adicionar manualmente o usuário a qualquer grupo adicional desejado.

Exemplo

O comando a seguir cria um usuário UNIX local chamado johnm (nome completo "John Miller") no SVM chamado VS1. O usuário tem o ID 123 e o ID do grupo principal 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

Carregue usuários UNIX locais a partir de um URI

Como alternativa à criação manual de usuários UNIX locais individuais em SVMs, você pode simplificar a tarefa carregando uma lista de usuários UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI(`vserver services name-service unix-user load-from-uri`)).

Passos

1. Crie um arquivo contendo a lista de usuários UNIX locais que você deseja carregar.

   O arquivo deve conter informações do usuário no formato UNIX `/etc/passwd`:

   `user_name: password: user_ID: group_ID: full_name`

   O comando descarta o valor *`password`* do campo e os valores dos campos após o *`full_name`* campo (*`home_directory`* e *`shell`*).

   O tamanho máximo de ficheiro suportado é de 2,5 MB.

2. Verifique se a lista não contém informações duplicadas.

   Se a lista contiver entradas duplicadas, o carregamento da lista falhará com uma mensagem de erro.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de usuários UNIX locais em SVMs a partir do URI:

   `vserver services name-service unix-user load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite {true false` `especifica se pretende substituir as entradas. A predefinição é` `false`.

Exemplo

O comando a seguir carrega uma lista de usuários UNIX locais do URI `ftp://ftp.example.com/passwd` para o SVM chamado VS1. Os usuários existentes no SVM não são sobrescritos pelas informações do URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

Crie um grupo UNIX local

Você pode usar o `vserver services name-service unix-group create` comando para criar grupos UNIX locais para o SVM. Grupos UNIX locais são usados com usuários UNIX locais.

Passo

1. Criar um grupo UNIX local:

   `vserver services name-service unix-group create -vserver` *`vserver_name`* `-name` *`group_name`* `-id` *`integer`*

   `-name` *`group_name`* especifica o nome do grupo. O comprimento do nome do grupo deve ter 64 carateres ou menos.

   `-id` *`integer`* Especifica o ID do grupo que você atribui.

Exemplo

O comando a seguir cria um grupo local chamado eng no SVM chamado VS1. O grupo tem o ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

Adicione um usuário a um grupo UNIX local

Você pode usar o `vserver services name-service unix-group adduser` comando para adicionar um usuário a um grupo UNIX suplementar que seja local para o SVM.

Passo

1. Adicionar um usuário a um grupo UNIX local:

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* Especifica o nome do grupo UNIX ao qual o usuário será adicionado, além do grupo principal do usuário.

Exemplo

O comando a seguir adiciona um usuário chamado Max a um grupo UNIX local chamado eng no SVM chamado VS1:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

Carregue grupos UNIX locais a partir de um URI

Como alternativa à criação manual de grupos UNIX locais individuais, você pode carregar uma lista de grupos UNIX locais em SVMs a partir de um identificador de recurso uniforme (URI) usando o `vserver services name-service unix-group load-from-uri` comando.

Passos

1. Crie um arquivo contendo a lista de grupos UNIX locais que você deseja carregar.

   O arquivo deve conter informações de grupo no formato UNIX `/etc/group`:

   `group_name: password: group_ID: comma_separated_list_of_users`

   O comando descarta o valor *`password`* do campo.

   O tamanho máximo de ficheiro suportado é de 1 MB.

   O comprimento máximo de cada linha no arquivo de grupo é de 32.768 carateres.

2. Verifique se a lista não contém informações duplicadas.

A lista não deve conter entradas duplicadas, ou então carregar a lista falha. Se já houver entradas presentes no SVM, você deve definir o `-overwrite` parâmetro para `true` substituir todas as entradas existentes pelo novo arquivo ou garantir que o novo arquivo não contenha entradas que dupliquem entradas existentes.

3. Copie o arquivo para um servidor.

   O servidor deve ser acessível pelo sistema de armazenamento em HTTP, HTTPS, FTP ou FTPS.

4. Determine qual é o URI para o arquivo.

   O URI é o endereço que você fornece ao sistema de armazenamento para indicar onde o arquivo está localizado.

5. Carregue o arquivo que contém a lista de grupos UNIX locais no SVM a partir do URI:

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`especifica se pretende substituir as entradas. A predefinição é `false`. Se você especificar esse parâmetro como `true`, o ONTAP substituirá todo o banco de dados de grupo UNIX local existente do SVM especificado pelas entradas do arquivo que você está carregando.

Exemplo

O comando a seguir carrega uma lista de grupos UNIX locais do URI `ftp://ftp.example.com/group` para o SVM chamado VS1. Os grupos existentes no SVM não são sobrescritos pelas informações do URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

Trabalhar com netgroups

Trabalhando com netgroups visão geral

Você pode usar netgroups para autenticação de usuário e para corresponder clientes em regras de política de exportação. Você pode fornecer acesso a netgroups de servidores de nomes externos (LDAP ou NIS) ou pode carregar netgroups de um identificador de recurso uniforme (URI) em SVMs usando o `vserver services name-service netgroup load` comando.

O que você vai precisar

Antes de trabalhar com netgroups, você deve garantir que as seguintes condições sejam atendidas:

- Todos os hosts em netgroups, independentemente da origem (NIS, LDAP ou arquivos locais), devem ter Registros DNS de encaminhamento (A) e reverso (PTR) para fornecer pesquisas de DNS consistentes de encaminhamento e reversão.

  Além disso, se um endereço IP de um cliente tiver vários Registros PTR, todos esses nomes de host devem ser membros do netgroup e ter Registros correspondentes A.

- Os nomes de todos os hosts em netgroups, independentemente de sua origem (NIS, LDAP ou arquivos locais), devem ser corretamente escritos e usar o caso correto. As inconsistências em nomes de host usados em netgroups podem levar a um comportamento inesperado, como verificações de exportação com falha.
- Todos os endereços IPv6 especificados em netgroups devem ser encurtados e compatados conforme especificado no RFC 5952.

  Por exemplo, 2011:hu9:0:0:0:0:3:1 tem de ser encurtado para 2011:hu9::3:1.

Sobre esta tarefa

Quando você trabalha com netgroups, você pode executar as seguintes operações:

- Você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.
- Você pode usar o `vserver services name-service getxxbyyy netgrp` comando para verificar se um cliente faz parte de um netgroup.

  O serviço subjacente para fazer a pesquisa é selecionado com base na ordem configurada do switch do serviço de nomes.

Carregue netgroups em SVMs

Um dos métodos que você pode usar para combinar clientes em regras de política de exportação é usando hosts listados em netgroups. Você pode carregar netgroups de um URI (identificador de recurso uniforme) em SVMs como uma alternativa ao uso de netgroups armazenados em servidores de nomes externos (`vserver services name-service netgroup load`).

O que você vai precisar

Os arquivos netgroup devem atender aos seguintes requisitos antes de serem carregados em um SVM:

- O arquivo deve usar o mesmo formato de arquivo de texto netgroup apropriado que é usado para preencher NIS.

  O ONTAP verifica o formato do arquivo de texto do netgroup antes de carregá-lo. Se o arquivo contiver erros, ele não será carregado e uma mensagem será exibida indicando as correções que você tem que executar no arquivo. Depois de corrigir os erros, você pode recarregar o arquivo netgroup no SVM especificado.

- Todos os carateres alfabéticos nos nomes de host no arquivo netgroup devem estar em minúsculas.
- O tamanho máximo de ficheiro suportado é de 5 MB.
- O nível máximo suportado para netgroups de aninhamento é 1000.
- Somente nomes de host DNS primários podem ser usados ao definir nomes de host no arquivo netgroup.

  Para evitar problemas de acesso à exportação, os nomes de host não devem ser definidos usando Registros DNS CNAME ou round robin.

- As partes de usuário e domínio de triplos no arquivo netgroup devem ser mantidas vazias porque o ONTAP não as suporta.

Apenas a parte host/IP é suportada.

Sobre esta tarefa

O ONTAP suporta pesquisas netgroup-by-host para o arquivo netgroup local. Depois de carregar o arquivo netgroup, o ONTAP cria automaticamente um mapa netgroup.byhost para ativar as pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas de netgroup locais ao processar regras de política de exportação para avaliar o acesso do cliente.

Passo

1. Carregue netgroups em SVMs a partir de um URI:

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   Carregar o arquivo netgroup e construir o mapa netgroup.byhost pode levar vários minutos.

   Se quiser atualizar os netgroups, você pode editar o arquivo e carregar o arquivo netgroup atualizado no SVM.

Exemplo

O comando a seguir carrega definições de netgroup no SVM chamado VS1 a partir do URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

Verifique o status das definições do netgroup

Depois de carregar netgroups no SVM, você pode usar o `vserver services name-service netgroup status` comando para verificar o status das definições do netgroup. Isso permite determinar se as definições de netgroup são consistentes em todos os nós que fazem backup do SVM.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Verifique o status das definições do netgroup:

   `vserver services name-service netgroup status`

   Pode apresentar informações adicionais numa vista mais detalhada.

3. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Exemplo

Depois que o nível de privilégio é definido, o seguinte comando exibe o status do netgroup para todos os SVMs:

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
---------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

Crie uma configuração de domínio NIS

Se um NIS (Network Information Service) for usado em seu ambiente para serviços de nome, você deverá criar uma configuração de domínio NIS para o SVM usando o `vserver services name-service nis-domain create` comando.

Antes de começar

Todos os servidores NIS configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.

Se você pretende usar NIS para pesquisas de diretório, os mapas em seus servidores NIS não podem ter mais de 1.024 carateres para cada entrada. Não especifique o servidor NIS que não está em conformidade com este limite. Caso contrário, o acesso do cliente dependente de entradas NIS pode falhar.

Sobre esta tarefa

Se o seu banco de dados NIS contiver um `netgroup.byhost` mapa, o ONTAP poderá usá-lo para pesquisas mais rápidas. Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente. A partir do ONTAP 9.7, as entradas do NIS `netgroup.byhost` podem ser armazenadas em cache usando os `vserver services name-service nis-domain netgroup-database` comandos.

O uso do NIS para resolução de nome de host não é suportado.

Passos

1. Criar uma configuração de domínio NIS:

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

   Pode especificar até 10 servidores NIS.

   > A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

2. Verifique se o domínio foi criado:

   ```
   vserver services name-service nis-domain show
   ```

Exemplo

O comando a seguir cria uma configuração de domínio NIS para um domínio NIS chamado `nisdomain` no SVM nomeado `vs1` com um servidor NIS em endereço IP `192.0.2.180` :

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

Utilize LDAP

Visão geral do uso do LDAP

Se o LDAP for usado no ambiente para serviços de nomes, você precisará trabalhar com o administrador LDAP para determinar os requisitos e as configurações do sistema de storage apropriadas e, em seguida, ativar o SVM como cliente LDAP.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative Directory e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores de nomes, use o `-try-channel -binding` parâmetro com o `ldap client modify` comando.

Para obter mais informações, "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows"consulte .

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
  - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
  - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
    - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
    - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e SSHA-512) também são suportados.

- Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

  As seguintes opções de segurança de sessão estão disponíveis:

  - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
  - INICIE O TLS
  - LDAPS (LDAP sobre TLS ou SSL)
- Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
  - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
  - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
  - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
- Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
  - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
  - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
  - Um servidor de certificados já deve estar configurado no domínio.
- Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
  - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
    - Bidirecional
    - One-way, onde o primário confia no domínio de referência
    - Pai-filho
  - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
  - As senhas de domínio devem ser as mesmas para autenticar quando --bind-as-cifs-server definido como true.

  > As configurações a seguir não são suportadas com a busca por referência LDAP.
  >
  > - Para todas as versões do ONTAP:
  >   - Clientes LDAP em um SVM admin
  > - Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
  >   - Assinatura e selagem LDAP (a `-session-security` opção)
  >   - Conexões TLS criptografadas (a `-use-start-tls` opção)
  >   - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

  Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para mais informações

- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"
- "Instale o certificado de CA raiz autoassinado no SVM"

Crie um novo esquema de cliente LDAP

Se o esquema LDAP no ambiente for diferente dos padrões do ONTAP, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar a configuração do cliente LDAP.

Sobre esta tarefa

A maioria dos servidores LDAP pode usar os esquemas padrão fornecidos pelo ONTAP:

- MS-AD-BIS (o esquema preferido para a maioria dos servidores AD do Windows 2012 e posteriores)
- Ad-IDMU (Windows 2008, Windows 2012 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

Se você precisar usar um esquema LDAP não padrão, você deve criá-lo antes de criar a configuração do cliente LDAP. Consulte o administrador LDAP antes de criar um novo esquema.

Os esquemas LDAP padrão fornecidos pelo ONTAP não podem ser modificados. Para criar um novo esquema, você cria uma cópia e modifica a cópia de acordo.

Passos

1. Exiba os modelos de esquema de cliente LDAP existentes para identificar o que deseja copiar:

   ```
   vserver services name-service ldap client schema show
   ```

2. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

3. Faça uma cópia de um esquema cliente LDAP existente:

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. Modifique o novo esquema e personalize-o para o seu ambiente:

   ```
   vserver services name-service ldap client schema modify
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Crie uma configuração de cliente LDAP

Se você quiser que o ONTAP acesse os serviços LDAP ou ative Directory externos em seu ambiente, primeiro é necessário configurar um cliente LDAP no sistema de armazenamento.

O que você vai precisar

Um dos três primeiros servidores na lista de domínios resolvidos do ative Directory deve estar ativo e fornecendo dados. Caso contrário, esta tarefa falha.

> Existem vários servidores, dos quais mais de dois servidores estão inativos a qualquer momento.

Passos

1. Consulte o administrador LDAP para determinar os valores de configuração apropriados para o `vserver services name-service ldap client create` comando:

   a. Especifique uma conexão baseada em domínio ou baseada em endereço para servidores LDAP.

      As `-ad-domain` opções e `-servers` são mutuamente exclusivas.

      - Utilize a `-ad-domain` opção para ativar a deteção de servidor LDAP no domínio do ative Directory.
        - Você pode usar a `-restrict-discovery-to-site` opção para restringir a descoberta de servidor LDAP ao site padrão CIFS para o domínio especificado. Se você usar essa opção, também precisará especificar o site padrão CIFS com `-default-site`.
      - Você pode usar a `-preferred-ad-servers` opção para especificar um ou mais servidores preferenciais do ative Directory por endereço IP em uma lista delimitada por vírgulas. Depois que o cliente é criado, você pode modificar esta lista usando o `vserver services name-service ldap client modify` comando.
      - Use a `-servers` opção para especificar um ou mais servidores LDAP (ative Directory ou UNIX) por endereço IP em uma lista delimitada por vírgulas.

        > A `-servers` opção está obsoleta no ONTAP 9.2. A partir de ONTAP 9.2, o `-ldap -servers` campo substitui o `-servers` campo. Este campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

   b. Especifique um esquema LDAP padrão ou personalizado.

      A maioria dos servidores LDAP pode usar os esquemas somente leitura padrão fornecidos pelo ONTAP. É melhor usar esses esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão (eles são somente leitura) e, em seguida, modificando a cópia.

      Esquemas predefinidos:

      - MS-AD-BIS

        Baseado em RFC-2307bis, este é o esquema LDAP preferido para a maioria das implantações padrão do Windows 2012 e LDAP posteriores.

- `AD-IDMU`

  Baseado no ative Directory Identity Management para UNIX, esse esquema é apropriado para a maioria dos servidores Windows 2008, Windows 2012 e AD posteriores.

- `AD-SFU`

  Baseado nos Serviços do ative Directory para UNIX, esse esquema é apropriado para a maioria dos servidores do Windows 2003 e AD anteriores.

- `RFC-2307`

  Baseado em RFC-2307 (*an Approach for using LDAP as Network Information Service*), este esquema é apropriado para a maioria dos servidores UNIX AD.

c. Selecione vincular valores.

- `-min-bind-level {anonymous|simple|sasl}` especifica o nível mínimo de autenticação bind.

  O valor padrão é **`anonymous`**.

- `-bind-dn` *`LDAP_DN`* especifica o usuário de vinculação.

  Para servidores do ative Directory, você deve especificar o usuário no formulário conta (DOMÍNIO/usuário) ou principal (user@domain.com). Caso contrário, você deve especificar o usuário em forma de nome distinto.

- `-bind-password` *`password`* especifica a senha de vinculação.

d. Selecione as opções de segurança da sessão, se necessário.

Pode ativar a assinatura e a selagem LDAP ou o LDAP através de TLS, se necessário pelo servidor LDAP.

- `--session-security {none|sign|seal}`

  Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

  Você também deve definir `-min-bind-level {sasl`, a menos que você queira que a autenticação de vinculação retorne **`anonymous`** ou **`simple`** se a vinculação de assinatura e vedação falhar.

- `-use-start-tls {true|`false`Selecione`

  Se definido como **`true`** e o servidor LDAP o suportar, o cliente LDAP utiliza uma ligação TLS encriptada ao servidor. O valor padrão é **`false`**. Você deve instalar um certificado de CA raiz autoassinado do servidor LDAP para usar essa opção.

Se a VM de armazenamento tiver um servidor SMB adicionado a um domínio e o servidor LDAP for um dos controladores de domínio do domínio inicial do servidor SMB, poderá modificar a `-session-security-for-ad-ldap` opção utilizando o `vserver cifs security modify` comando.

e. Selecione valores de porta, consulta e base.

Os valores padrão são recomendados, mas você deve verificar com o administrador LDAP se eles são apropriados para o seu ambiente.

- `-port` *`port`* Especifica a porta do servidor LDAP.

  O valor padrão é `389`.

Se pretender utilizar Iniciar TLS para proteger a ligação LDAP, tem de utilizar a porta predefinida 389. Iniciar TLS começa como uma conexão de texto simples através da porta padrão LDAP 389, e essa conexão é então atualizada para TLS. Se você alterar a porta, Iniciar TLS falhará.

- `-query-timeout` *`integer`* especifica o tempo limite da consulta em segundos.

  O intervalo permitido é de 1 a 10 segundos. O valor padrão é `3` segundos.

- `-base-dn` *`LDAP_DN`* Especifica o DN base.

  Vários valores podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada). O valor padrão é `""` (root).

- `-base-scope` {`base`|`onelevel`|`subtree`especifica o escopo de pesquisa base.

  O valor padrão é `subtree`.

- `-referral-enabled` {`true`|`false`Especifica se a busca por referência LDAP está ativada.

  A partir do ONTAP 9.5, isso permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP for retornada pelo servidor LDAP primário indicando que os Registros desejados estão presentes nos servidores LDAP referidos. O valor padrão é **`false`**.

Para pesquisar Registros presentes nos servidores LDAP referidos, o base-DN dos Registros referidos deve ser adicionado ao base-DN como parte da configuração do cliente LDAP.

2. Crie uma configuração de cliente LDAP na VM de armazenamento:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

Você deve fornecer o nome da VM de armazenamento ao criar uma configuração de cliente LDAP.

3. Verifique se a configuração do cliente LDAP foi criada com sucesso:

```
vserver services name-service ldap client show -client-config
client_config_name
```

Exemplos

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP no qual a assinatura e a vedação são necessárias, e a descoberta de servidor LDAP é restrita a um site específico para o domínio especificado:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

O comando a seguir cria uma nova configuração de cliente LDAP chamada ldap1 para que a VM de armazenamento VS1 funcione com um servidor do ative Directory para LDAP onde a busca por referência LDAP é necessária:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1 especificando o DN base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

O comando a seguir modifica a configuração do cliente LDAP chamada ldap1 para a VM de armazenamento VS1, ativando a busca de referência:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

Associe a configuração do cliente LDAP a SVMs

Para ativar o LDAP em um SVM, você deve usar o `vserver services name-service ldap create` comando para associar uma configuração de cliente LDAP ao SVM.

O que você vai precisar

- Um domínio LDAP já deve existir na rede e deve estar acessível ao cluster no qual o SVM está localizado.
- Uma configuração de cliente LDAP deve existir no SVM.

Passos

1. Ative o LDAP no SVM:

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > ⓘ A partir do ONTAP 9.2, o `vserver services name-service ldap create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não conseguir entrar em Contato com o servidor de nomes.

   O comando a seguir habilita o LDAP no "VS1"SVM e o configura para usar a configuração de cliente LDAP "ldap1":

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. Valide o status dos servidores de nomes usando o comando de verificação ldap do serviço de nomes dos serviços vserver.

   O comando a seguir valida servidores LDAP no SVM VS1.

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                   |
```

O comando name Service check está disponível a partir de ONTAP 9.2.

Verifique as fontes LDAP na tabela do switch do serviço de nomes

Você deve verificar se as fontes LDAP para serviços de nome estão listadas corretamente na tabela de opções de serviço de nomes para o SVM.

Passos

1. Exibir o conteúdo da tabela de opções de serviço de nomes atual:

   `vserver services name-service ns-switch show -vserver svm_name`

   O comando a seguir mostra os resultados do SVM My_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                Source
Vserver         Database        Order
--------------- ------------    ---------
My_SVM          hosts           files,
                                dns
My_SVM          group           files,ldap
My_SVM          passwd          files,ldap
My_SVM          netgroup        files
My_SVM          namemap         files
5 entries were displayed.
```

   `namemap` especifica as fontes para procurar informações de mapeamento de nomes e em que ordem. Em um ambiente somente UNIX, essa entrada não é necessária. O mapeamento de nomes só é necessário em um ambiente misto usando UNIX e Windows.

2. Atualize a `ns-switch` entrada conforme apropriado:

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do utilizador	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

Se quiser atualizar a entrada ns-switch para…	Digite o comando…
Informações do grupo	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
Informações do netgroup	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

Use Kerberos com NFS para segurança forte

Visão geral do uso do Kerberos com NFS para segurança forte

Se o Kerberos for usado em seu ambiente para autenticação forte, você precisará trabalhar com o administrador do Kerberos para determinar os requisitos e as configurações apropriadas do sistema de armazenamento e, em seguida, ativar o SVM como um cliente Kerberos.

Seu ambiente deve atender às seguintes diretrizes:

- A implantação do seu site deve seguir as práticas recomendadas para a configuração do servidor Kerberos e do cliente antes de configurar o Kerberos para ONTAP.
- Se possível, use NFSv4 ou posterior se a autenticação Kerberos for necessária.

  NFSv3 pode ser usado com Kerberos. No entanto, os benefícios completos de segurança do Kerberos só são realizados em implantações ONTAP de NFSv4 ou posterior.

- Para promover o acesso redundante ao servidor, o Kerberos deve ser habilitado em várias LIFs de dados em vários nós no cluster usando o mesmo SPN.
- Quando o Kerberos está habilitado no SVM, um dos seguintes métodos de segurança deve ser especificado em regras de exportação para volumes ou qtrees, dependendo da configuração do cliente NFS.
  - `krb5` (Protocolo Kerberos v5)
  - `krb5i` (Protocolo Kerberos v5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos v5 com serviço de privacidade)

Além do servidor Kerberos e clientes, os seguintes serviços externos devem ser configurados para que o ONTAP suporte Kerberos:

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como o ative Directory ou o OpenLDAP, configurado para usar LDAP em SSL/TLS. Não use NIS, cujos pedidos são enviados em texto não criptografado e, portanto, não são seguros.

- NTP

  Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de

autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

  Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

Verifique as permissões para a configuração Kerberos

O Kerberos requer que certas permissões UNIX sejam definidas para o volume raiz do SVM e para usuários e grupos locais.

Passos

1. Exiba as permissões relevantes no volume raiz da SVM:

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   O volume raiz do SVM precisa ter a seguinte configuração:

Nome…	A definir…
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	755

   Se esses valores não forem exibidos, use o `volume modify` comando para atualizá-los.

2. Exibir os usuários locais do UNIX:

   `vserver services name-service unix-user show -vserver` *`vserver_name`*

   O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS. O primeiro componente do usuário cliente NFS SPN é usado como usuário. O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.
raiz	0	0	Necessário para a montagem.

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-user modify` comando para atualizá-los.

3. Exibir os grupos UNIX locais:

   `vserver services name-service unix-group show -vserver` *`vserver`* `_name`

   O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0

Se esses valores não forem exibidos, você pode usar o `vserver services name-service unix-group modify` comando para atualizá-los.

Crie uma configuração NFS Kerberos realm

Se você quiser que o ONTAP acesse servidores Kerberos externos em seu ambiente, primeiro configure o SVM para usar um realm Kerberos existente. Para fazer isso, você precisa reunir valores de configuração para o servidor KDC Kerberos e, em seguida, usar o `vserver nfs kerberos realm create` comando para criar a configuração de realm Kerberos em um SVM.

O que você vai precisar

O administrador do cluster deve ter configurado o NTP no sistema de armazenamento, cliente e servidor KDC para evitar problemas de autenticação. As diferenças de tempo entre um cliente e um servidor (desvio de relógio) são uma causa comum de falhas de autenticação.

Passos

1. Consulte o administrador do Kerberos para determinar os valores de configuração apropriados para fornecer com o `vserver nfs kerberos realm create` comando.
2. Crie uma configuração de realm Kerberos no SVM:

   `vserver nfs kerberos realm create -vserver` *`vserver_name`* `-realm` *`realm_name`* *`{AD_KDC_server_values |AD_KDC_server_values}`* `-comment "`*`text`*`"`

3. Verifique se a configuração do realm Kerberos foi criada com sucesso:

   `vserver nfs kerberos realm show`

Exemplos

O comando a seguir cria uma configuração NFS Kerberos Realm para o SVM VS1 que usa um servidor Microsoft ative Directory como servidor KDC. O Reino Kerberos é AUTH.EXAMPLE.COM. O servidor do ative Directory tem o nome ad-1 e seu endereço IP é 10.10.8.14. O desvio de relógio permitido é de 300 segundos (o padrão). O endereço IP do servidor KDC é 10.10.8.14, e seu número de porta é 88 (o padrão). "Configuração do Microsoft Kerberos" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

O comando a seguir cria uma configuração NFS Kerberos realm para o SVM VS1 que usa um MIT KDC. O Reino Kerberos é SECURITY.EXAMPLE.COM. A inclinação permitida do relógio é de 300 segundos. O endereço IP do servidor KDC é 10.10.9.1, e seu número de porta é 88. O fornecedor KDC é outro para indicar um fornecedor UNIX. O endereço IP do servidor administrativo é 10.10.9.1, e seu número de porta é 749 (o padrão). O endereço IP do servidor de senhas é 10.10.9.1, e seu número de porta é 464 (o padrão). "UNIX Kerberos config" é o comentário.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

Configurar os tipos de criptografia permitidos do NFS Kerberos

Por padrão, o ONTAP oferece suporte aos seguintes tipos de criptografia para o Kerberos NFS: DES, 3DES, AES-128 e AES-256. Você pode configurar os tipos de criptografia permitidos para cada SVM de acordo com os requisitos de segurança do seu ambiente específico usando o `vserver nfs modify` comando com o `-permitted -enc-types` parâmetro.

Sobre esta tarefa

Para maior compatibilidade com clientes, o ONTAP suporta criptografia DES fraca e AES forte por padrão. Isso significa, por exemplo, que se você quiser aumentar a segurança e seu ambiente a suportar, você pode usar este procedimento para desativar DES e 3DES e exigir que os clientes usem apenas criptografia AES.

Você deve usar a criptografia mais forte disponível. Para ONTAP, isso é AES-256. Deve confirmar com o administrador do KDC que este nível de encriptação é suportado no seu ambiente.

- Ativar ou desativar totalmente AES (AES-128 e AES-256) em SVMs é disruptivo porque destrói o arquivo DES principal/keytab original, exigindo assim que a configuração Kerberos seja desativada em todos os LIFs para o SVM.

  Antes de fazer essa alteração, você deve verificar se os clientes NFS não dependem da criptografia AES no SVM.

- Ativar ou desativar DES ou 3DES não requer alterações na configuração Kerberos em LIFs.

Passo

1. Ative ou desative o tipo de encriptação permitido que pretende:

Se quiser ativar ou desativar…	Siga estes passos…
DES ou 3DES	a. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* Separe vários tipos de criptografia com uma vírgula. b. Verifique se a alteração foi bem-sucedida `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

Se quiser ativar ou desativar…	Siga estes passos…

AES-128 ou AES-256	a. Identifique em que SVM e LIF Kerberos estão ativados
	`vserver nfs kerberos interface show`
	b. Desative o Kerberos em todos os LIFs no SVM cujo tipo de criptografia NFS Kerberos permitido você deseja modificar
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	c. Configure os tipos de criptografia permitidos do NFS Kerberos da SVM
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	Separe vários tipos de criptografia com uma vírgula.
	d. Verifique se a alteração foi bem-sucedida
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	e. Reative o Kerberos em todos os LIFs na SVM
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	f. Verifique se o Kerberos está ativado em todos os LIFs
	`vserver nfs kerberos interface show`

Ative o Kerberos em um LIF de dados

Você pode usar o `vserver nfs kerberos interface enable` comando para habilitar o Kerberos em um LIF de dados. Isso permite que o SVM use os serviços de segurança Kerberos para NFS.

Sobre esta tarefa

Se você estiver usando um KDC do ative Directory, os primeiros 15 carateres de qualquer SPNs usados devem ser exclusivos em SVMs dentro de um Reino ou domínio.

Passos

1. Crie a configuração NFS Kerberos:

   `vserver nfs kerberos interface enable -vserver` *`vserver_name`* `-lif` *`logical_interface`* `-spn` *`service_principal_name`*

   O ONTAP requer a chave secreta para o SPN do KDC para habilitar a interface Kerberos.

Para os KDCs da Microsoft, o KDC é contatado e um prompt de nome de usuário e senha são emitidos na CLI para obter a chave secreta. Se você precisar criar o SPN em uma ou diferente do realm Kerberos, você poderá especificar o parâmetro opcional `-ou`.

Para KDCs não Microsoft, a chave secreta pode ser obtida usando um de dois métodos:

Se você…	Você também deve incluir o seguinte parâmetro com o comando…
Peça às credenciais do administrador do KDC para recuperar a chave diretamente do KDC	`-admin-username` *kdc_admin_username*
Não tem as credenciais de administrador do KDC, mas tem um arquivo keytab do KDC que contém a chave	`-keytab-uri` digite seu comentário aqui:// *uri*

2. Verifique se o Kerberos foi ativado no LIF:

   `vserver nfs kerberos-config show`

3. Repita as etapas 1 e 2 para ativar o Kerberos em várias LIFs.

Exemplo

O comando a seguir cria e verifica uma configuração NFS Kerberos para o SVM chamado VS1 na interface lógica ves03-D1, com o SPN nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM na ou lab2ou:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- --------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

Use o TLS com NFS para ter uma segurança forte

Visão geral do uso do TLS com NFS para uma segurança forte

O TLS permite comunicações de rede criptografadas com segurança equivalente e menos complexidade do que o Kerberos e o IPsec. Como administrador, você pode habilitar, configurar e desabilitar o TLS para segurança forte com conexões NFSv3 e NFSv4.x usando o Gerenciador de sistema, a CLI do ONTAP ou a API REST do ONTAP.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

O ONTAP usa o TLS 1,3 para conexões NFS em TLS.

Requisitos

O NFS em TLS requer certificados X,509. Você pode criar e instalar um certificado de servidor assinado pela CA no cluster do ONTAP ou instalar um certificado que o serviço NFS usa diretamente. Seus certificados devem atender às seguintes diretrizes:

- O nome comum (CN) de cada certificado deve ser configurado com o nome de domínio totalmente qualificado (FQDN) do LIF de dados no qual o TLS será ativado.
- O nome alternativo do assunto (SAN) de cada certificado deve ser configurado com o endereço IP do LIF de dados no qual o TLS será ativado. Opcionalmente, você também pode adicionar FQDN do LIF de dados. Se o endereço IP e o FQDN estiverem configurados, os clientes NFS podem se conetar usando o endereço IP ou o FQDN.
- Você pode instalar vários certificados de serviço NFS para o mesmo LIF, mas apenas um deles pode ser usado de cada vez como parte da configuração TLS NFS.

Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode ativar ou desativar o TLS em um data LIF para clientes NFS. Quando você ativa o NFS em TLS, o SVM usa o TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

- Consulte "requisitos"o para NFS sobre TLS antes de começar.
- Saiba mais sobre `vserver nfs tls interface enable` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir habilita o NFS sobre TLS no `data1` LIF da `vs1` VM de storage:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

> Quando você desativa o NFS em TLS, o certificado TLS usado para a conexão NFS é removido. Se você precisar habilitar o NFS em TLS no futuro, precisará especificar novamente um nome de certificado durante a capacitação.

Antes de começar

Saiba mais sobre `vserver nfs tls interface disable` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.
2. Desative TLS para conexões NFS nessa VM e interface de storage. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir desativa NFS sobre TLS no `data1` LIF da `vs1` VM de armazenamento:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Editar uma configuração TLS

Você pode alterar as configurações de uma configuração NFS em TLS existente. Por exemplo, você pode usar este procedimento para atualizar o certificado TLS.

Antes de começar

Saiba mais sobre `vserver nfs tls interface modify` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de storage e uma interface lógica (LIF) para modificar a configuração TLS para clientes NFS.
2. Modificar a configuração. Se especificar um `status` de `enable`, também terá de especificar o `certificate-name` parâmetro. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir modifica a configuração NFS sobre TLS no `data2` LIF da `vs2` VM de armazenamento:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

Adicionar capacidade de storage a um SVM habilitado para NFS

Adicionar capacidade de storage a uma visão geral da SVM habilitada para NFS

Para adicionar capacidade de storage a um SVM habilitado para NFS, você precisa criar um volume ou qtree para fornecer um contêiner de storage e criar ou modificar uma política de exportação para esse contêiner. Em seguida, você pode verificar o acesso do cliente NFS a partir do cluster e testar o acesso a partir de sistemas cliente.

O que você vai precisar

- O NFS precisa estar completamente configurado no SVM.
- A política de exportação padrão do volume raiz da SVM deve conter uma regra que permita acesso a todos os clientes.
- Todas as atualizações da configuração dos serviços de nome devem estar concluídas.
- Quaisquer adições ou modificações a uma configuração Kerberos devem estar concluídas.

Crie uma política de exportação

Antes de criar regras de exportação, você deve criar uma política de exportação para mantê-las. Você pode usar o `vserver export-policy create` comando para criar uma política de exportação.

Passos

1. Criar uma política de exportação:

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

O nome da política pode ter até 256 carateres.

2. Verifique se a política de exportação foi criada:

   `vserver export-policy show -policyname policy_name`

Exemplo

Os comandos a seguir criam e verificam a criação de uma política de exportação chamada exp1 no SVM chamado VS1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

Adicione uma regra a uma política de exportação

Sem regras, a política de exportação não pode fornecer acesso de cliente aos dados. Para criar uma nova regra de exportação, você deve identificar clientes e selecionar um formato de correspondência de cliente, selecionar os tipos de acesso e segurança, especificar um mapeamento de ID de usuário anônimo, selecionar um número de índice de regras e selecionar o protocolo de acesso. Em seguida, você pode usar o `vserver export-policy rule create` comando para adicionar a nova regra a uma política de exportação.

O que você vai precisar

- A política de exportação à qual deseja adicionar as regras de exportação já deve existir.
- O DNS deve ser configurado corretamente nos dados SVM e os servidores DNS devem ter entradas corretas para clientes NFS.

  Isso ocorre porque o ONTAP executa pesquisas de DNS usando a configuração DNS do SVM de dados para determinados formatos de correspondência de clientes, e falhas na correspondência de regras de política de exportação podem impedir o acesso aos dados do cliente.

- Se você estiver autenticando com Kerberos, você deve ter determinado qual dos seguintes métodos de segurança é usado em seus clientes NFS:
  - `krb5` (Protocolo Kerberos V5)
  - `krb5i` (Protocolo Kerberos V5 com verificação de integridade usando checksums)
  - `krb5p` (Protocolo Kerberos V5 com serviço de privacidade)

Sobre esta tarefa

Não é necessário criar uma nova regra se uma regra existente em uma política de exportação abranger seus requisitos de correspondência de cliente e acesso.

Se você estiver autenticando com Kerberos e se todos os volumes da SVM forem acessados por Kerberos,

poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5`, `krb5i` ou `krb5p`.

Passos

1. Identificar os clientes e o formato de correspondência do cliente para a nova regra.

   A `-clientmatch` opção especifica os clientes aos quais a regra se aplica. Valores de correspondência de cliente único ou múltiplo podem ser especificados; as especificações de vários valores devem ser separadas por vírgulas. Você pode especificar a correspondência em qualquer um dos seguintes formatos:

Formato de correspondência do cliente	Exemplo
Nome de domínio precedido pelo caractere "."	`.example.com` ou `.example.com,.example.net,...`
Nome do host	`host1` ou `host1,host2, ...`
Endereço IPv4	`10.1.12.24` ou `10.1.12.24,10.1.12.25, ...`
Endereço IPv4 com uma máscara de sub-rede expressa como um número de bits	`10.1.12.10/4` ou `10.1.12.10/4,10.1.12.11/4,...`
Endereço IPv4 com uma máscara de rede	`10.1.16.0/255.255.255.0` ou `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
Endereço IPv6 no formato pontilhado	`::1.2.3.4` ou `::1.2.3.4,::1.2.3.5,...`
Endereço IPv6 com uma máscara de sub-rede expressa como um número de bits	`ff::00/32` ou `ff::00/32,ff::01/32,...`
Um único netgroup com o nome netgroup precedido pelo caractere at	`@netgroup1` ou `@netgroup1,@netgroup2,...`

   Você também pode combinar tipos de definições de cliente; por exemplo `.example.com,@netgroup1,.`

   Ao especificar endereços IP, observe o seguinte:

   - Não é permitido introduzir um intervalo de endereços IP, como 10,1.12,10-10,1.12,70.

     As entradas neste formato são interpretadas como uma cadeia de texto e tratadas como um nome de host.

   - Ao especificar endereços IP individuais em regras de exportação para gerenciamento granular do acesso do cliente, não especifique endereços IP que sejam atribuídos dinamicamente (por exemplo, DHCP) ou temporariamente (por exemplo, IPv6).

     Caso contrário, o cliente perde o acesso quando seu endereço IP muda.

- Não é permitido inserir um endereço IPv6 com uma máscara de rede, como ff::12/FF::00.

2. Selecione os tipos de acesso e segurança para correspondências de clientes.

   Você pode especificar um ou mais dos seguintes modos de acesso aos clientes que se autenticam com os tipos de segurança especificados:

   - `-rorule` (acesso somente leitura)
   - `-rwrule` (acesso de leitura e gravação)
   - `-superuser` (acesso à raiz)

   > Um cliente só pode obter acesso de leitura e gravação para um tipo de segurança específico se a regra de exportação também permitir acesso somente leitura para esse tipo de segurança. Se o parâmetro somente leitura for mais restritivo para um tipo de segurança do que o parâmetro leitura-gravação, o cliente poderá não obter acesso de leitura-gravação. O mesmo se aplica ao acesso do superusuário.

   Você pode especificar uma lista separada por vírgulas de vários tipos de segurança para uma regra. Se especificar o tipo de segurança `any` como ou `never`, não especifique outros tipos de segurança. Escolha entre os seguintes tipos de segurança válidos:

Quando o tipo de segurança está definido como…	Um cliente correspondente pode acessar os dados exportados…
`any`	Sempre, independentemente do tipo de segurança de entrada.
`none`	Se listado sozinho, os clientes com qualquer tipo de segurança recebem acesso como anônimo. Se listado com outros tipos de segurança, os clientes com um tipo de segurança especificado recebem acesso e os clientes com qualquer outro tipo de segurança recebem acesso como anônimos.
`never`	Nunca, independentemente do tipo de segurança de entrada.
`krb5`	Se for autenticado pelo Kerberos 5. Somente autenticação: O cabeçalho de cada solicitação e resposta é assinado.
`krb5i`	Se for autenticado pelo Kerberos 5i. Autenticação e integridade: O cabeçalho e o corpo de cada solicitação e resposta são assinados.

Quando o tipo de segurança está definido como…	Um cliente correspondente pode acessar os dados exportados…
`krb5p`	Se for autenticado pelo Kerberos 5P. Autenticação, integridade e privacidade: O cabeçalho e o corpo de cada solicitação e resposta são assinados e a carga útil de dados NFS é criptografada.
`ntlm`	Se for autenticado pelo CIFS NTLM.
`sys`	Se for autenticado por NFS AUTH_SYS.

O tipo de segurança recomendado é `sys`, ou se o Kerberos for usado, `krb5` `krb5i` , ou `krb5p`.

Se você estiver usando Kerberos com NFSv3, a regra de política de exportação deverá permitir `-rorule` e `-rwrule` acessar `sys` além `krb5` do . Isso ocorre devido à necessidade de permitir o acesso do Network Lock Manager (NLM) à exportação.

3. Especifique um mapeamento de ID de usuário anônimo.

   A `-anon` opção especifica um ID de usuário UNIX ou nome de usuário que é mapeado para solicitações de cliente que chegam com um ID de usuário de 0 (zero), que normalmente é associado à raiz do nome de usuário. O valor padrão é `65534`. Os clientes NFS normalmente associam o ID de usuário 65534 ao nome de usuário nobody (também conhecido como *root squashing*). No ONTAP, esse ID de usuário está associado ao usuário pcuser. Para desativar o acesso por qualquer cliente com uma ID de usuário de 0, especifique um valor `65535` de .

4. Selecione a ordem do índice de regras.

   A `-ruleindex` opção especifica o número do índice para a regra. As regras são avaliadas de acordo com sua ordem na lista de números de índice; regras com números de índice mais baixos são avaliadas primeiro. Por exemplo, a regra com índice número 1 é avaliada antes da regra com índice número 2.

Se você está adicionando…	Então…
A primeira regra para uma política de exportação	Introduza `1`.
Regras adicionais para uma política de exportação	a. Exibir regras existentes na política `vserver export-policy rule show -instance -policyname` *`your_policy`* b. Selecione um número de índice para a nova regra, dependendo da ordem em que ela deve ser avaliada.

5. Selecione o valor de acesso NFS aplicável:{`nfs`|`nfs3`|`nfs4`.

   `nfs` corresponde a qualquer versão e `nfs3` `nfs4` corresponde apenas a essas versões específicas.

6. Crie a regra de exportação e adicione-a a uma política de exportação existente:

```
vserver export-policy rule create -vserver vserver_name -policyname
policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text |
"text,text,…" } -rorule security_type -rwrule security_type -superuser
security_type -anon user_ID
```

7. Exiba as regras da política de exportação para verificar se a nova regra está presente:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   O comando exibe um resumo para essa política de exportação, incluindo uma lista de regras aplicadas a essa política. O ONTAP atribui a cada regra um número de índice de regra. Depois de saber o número do índice da regra, você pode usá-lo para exibir informações detalhadas sobre a regra de exportação especificada.

8. Verifique se as regras aplicadas à política de exportação estão configuradas corretamente:

   ```
   vserver export-policy rule show -policyname policy_name -vserver vserver_name
   -ruleindex integer
   ```

Exemplos

Os comandos a seguir criam e verificam a criação de uma regra de exportação no SVM chamado VS1 em uma política de exportação chamada RS1. A regra tem o índice número 1. A regra corresponde a qualquer cliente no domínio eng.company.com e o netgroup netgroup1. A regra habilita todo o acesso NFS. Ele permite acesso somente leitura e leitura-gravação a usuários autenticados com AUTH_SYS. Os clientes com o ID de usuário UNIX 0 (zero) são anonimizados, a menos que autenticados com o Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                            RO Access Rule: sys
                            RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Os comandos a seguir criam e verificam a criação de uma regra de exportação no SVM chamado VS2 em uma política de exportação chamada expol2. A regra tem o índice número 21. A regra corresponde clientes aos membros do netgroup dev_netgroup_main. A regra habilita todo o acesso NFS. Ele permite acesso somente leitura para usuários autenticados com AUTH_SYS e requer autenticação Kerberos para leitura-gravação e acesso root. Os clientes com a ID de usuário UNIX 0 (zero) têm acesso root negado, a menos que autenticados com Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client              RO
Server   Name         Index   Protocol  Match               Rule
-------- ------------ ------  --------  ------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

Crie um volume ou um contêiner de storage de qtree

Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

Antes de começar

- O NFS deve estar configurado e em execução.
- O estilo de segurança da SVM deve ser UNIX.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume com um ponto de junção:

   `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number -group group_name_or_number -junction-path junction_path [-policy export_policy_name]`

   As opções para `-junction-path` são as seguintes:

   - Diretamente sob a raiz, por exemplo, `/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

   - Em um diretório existente, por exemplo, `/existing_dir/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

     Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, `/new_dir/new_vol` será necessário criar primeiro um novo volume pai que seja juntado ao volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

   Se você pretende usar uma política de exportação existente, você pode especificá-la quando você cria o volume. Você também pode adicionar uma política de exportação mais tarde com o `volume modify` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado:

   `volume show -vserver svm_name -volume volume_name -junction`

Exemplos

O comando a seguir cria um novo volume chamado users1 no SVM vs1.example.com e no agregado aggr1. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo volume (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1    true     /users          RW_volume
```

O comando a seguir cria um novo volume chamado "home4" no SVM "vs1.example.com" e o agregado "aggr1". O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório home do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- -------  -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Crie uma qtree

Você pode criar uma qtree para conter seus dados e especificar suas propriedades usando o `volume qtree create` comando.

O que você vai precisar

- O SVM e o volume que conterá a nova qtree já devem existir.
- O estilo de segurança da SVM deve ser UNIX, e o NFS deve ser configurado e executado.

Passos

1. Crie a qtree:

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   Você pode especificar o volume e a qtree como argumentos separados ou especificar o argumento de caminho de qtree no formato `/vol/`*`volume_name/_qtree_name`*.

   Por padrão, qtrees herdam as políticas de exportação de seu volume pai, mas eles podem ser configurados para usar suas próprias políticas. Se você pretende usar uma política de exportação existente, pode especificá-la quando criar a qtree. Você também pode adicionar uma política de exportação mais tarde com o `volume qtree modify` comando.

2. Verifique se a qtree foi criada com o caminho de junção desejado:

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

Exemplo

O exemplo a seguir cria uma qtree chamada qt01 localizada no SVM vs1.example.com que tem um caminho de junção `/vol/data1` :

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Proteja o acesso NFS usando políticas de exportação

Proteja o acesso NFS usando políticas de exportação

Você pode usar políticas de exportação para restringir o acesso NFS a volumes ou qtrees a clientes que correspondem a parâmetros específicos. Ao provisionar um novo storage, você pode usar uma política e regras existentes, adicionar regras a uma política existente ou criar uma nova política e regras. Você também pode verificar a configuração das políticas de exportação

> A partir do ONTAP 9.3, você pode habilitar a verificação de configuração de política de exportação como uma tarefa em segundo plano que Registra quaisquer violações de regras em uma lista de regras de erro. Os `vserver export-policy config-checker` comandos invocam o verificador e exibem resultados, que podem ser usados para verificar sua configuração e excluir regras errôneas da política.os comandos validam somente a configuração de exportação para nomes de host, netgroups e usuários anônimos.

Gerenciar a ordem de processamento das regras de exportação

Você pode usar o `vserver export-policy rule setindex` comando para definir manualmente o número de índice de uma regra de exportação existente. Isso permite que você especifique a precedência pela qual o ONTAP aplica regras de exportação para solicitações de cliente.

Sobre esta tarefa

Se o novo número de índice já estiver em uso, o comando insere a regra no local especificado e reordena a lista de acordo.

Passo

1. Modifique o número de índice de uma regra de exportação especificada:

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

Exemplo

O comando a seguir altera o número de índice de uma regra de exportação no número de índice 3 para o número de índice 2 em uma política de exportação chamada RS1 no SVM chamado VS1:

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

Atribua uma política de exportação a um volume

Cada volume contido no SVM deve estar associado a uma política de exportação que contenha regras de exportação para que os clientes acessem os dados no volume.

Sobre esta tarefa

Você pode associar uma política de exportação a um volume ao criar o volume ou a qualquer momento depois de criar o volume. Você pode associar uma política de exportação ao volume, embora uma política possa ser associada a muitos volumes.

Passos

1. Se uma política de exportação não foi especificada quando o volume foi criado, atribua uma política de exportação ao volume:

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. Verifique se a política foi atribuída ao volume:

   ```
   volume show -volume volume_name -fields policy
   ```

Exemplo

Os comandos a seguir atribuem a política de exportação nfs_policy ao volume vol1 no SVM VS1 e verificam a atribuição:

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

Atribua uma política de exportação a uma qtree

Em vez de exportar um volume inteiro, você também pode exportar uma qtree específica em um volume para torná-lo diretamente acessível aos clientes. Você pode exportar uma qtree atribuindo uma política de exportação a ela. Você pode atribuir a política de exportação ao criar uma nova qtree ou modificando uma qtree existente.

O que você vai precisar

A política de exportação tem de existir.

Sobre esta tarefa

Por padrão, qtrees herdam a política de exportação pai do volume contendo se não for especificado de outra forma no momento da criação.

Você pode associar uma política de exportação a uma qtree quando você cria a qtree ou a qualquer momento depois de criar a qtree. Você pode associar uma política de exportação à qtree, embora uma política possa ser associada a muitos qtrees.

Passos

1. Se uma política de exportação não foi especificada quando a qtree foi criada, atribua uma política de exportação à qtree:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. Verifique se a política foi atribuída à qtree:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Exemplo

Os comandos a seguir atribuem a política de exportação nfs_policy à qtree qt1 no SVM VS1 e verificam a atribuição:

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

Verifique o acesso do cliente NFS a partir do cluster

Você pode dar a clientes selecionados acesso ao compartilhamento definindo permissões de arquivo UNIX em um host de administração UNIX. Você pode verificar o acesso do cliente usando o `vserver export-policy check-access` comando, ajustando as regras de exportação conforme necessário.

Passos

1. No cluster, verifique o acesso do cliente às exportações usando o `vserver export-policy check-access` comando.

   O comando a seguir verifica o acesso de leitura/gravação para um cliente NFSv3 com o endereço IP 1.2.3.4 para o volume Home2. O comando output mostra que o volume usa a política de exportação `exp-home-dir` e que o acesso é negado.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                    Policy    Policy     Rule
Path                    Policy      Owner     Owner Type Index  Access
----------------------- ----------- --------- ---------- ------
----------
/                       default     vs1_root  volume          1 read
/eng                    default     vs1_root  volume          1 read
/eng/home2              exp-home-dir home2    volume          1 denied

3 entries were displayed.
```

2. Examine a saída para determinar se a política de exportação funciona conforme o pretendido e o acesso do cliente se comporta como esperado.

   Especificamente, você deve verificar qual política de exportação é usada pelo volume ou qtree e o tipo de acesso que o cliente tem como resultado.

3. Se necessário, reconfigure as regras da política de exportação.

Testar o acesso NFS a partir de sistemas cliente

Depois de verificar o acesso NFS ao novo objeto de storage, você deve testar a configuração fazendo login em um host de administração NFS, lendo e gravando dados no SVM. Você deve repetir o processo como um usuário não-root em um sistema cliente.

O que você vai precisar

- O sistema cliente deve ter um endereço IP permitido pela regra de exportação especificada anteriormente.
- Você deve ter as informações de login para o usuário root.

Passos

1. No cluster, verifique o endereço IP do LIF que está hospedando o novo volume:

   `network interface show –vserver` *`svm_name`*

2. Faça login como o usuário raiz no sistema de cliente de host de administração.
3. Altere o diretório para a pasta de montagem:

   `cd /mnt/`

4. Crie e monte uma nova pasta usando o endereço IP do SVM:

   a. Criar uma nova pasta
   `mkdir /mnt/folder`

   b. Monte o novo volume neste novo diretório
   `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

   c. Mude o diretório para a nova pasta
   `cd folder`

   Os comandos a seguir criam uma pasta chamada test1, montam o volume vol1 no endereço IP 192.0.2.130 na pasta de montagem test1 e mudam para o novo diretório test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Crie um novo arquivo, verifique se ele existe e escreva texto nele:

   a. Criar um arquivo de teste
   `touch filename`

   b. Verifique se o arquivo existe
   `ls -l filename`

   c. Digite
   `cat > filename`

   Digite algum texto e pressione Ctrl-D para escrever texto no arquivo de teste.

   d. Exibir o conteúdo do arquivo de teste. E
   `cat filename`

   e. Remova o arquivo de teste
   `rm filename`

   f. Retornar para o diretório pai
   `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Como root, defina qualquer propriedade e permissões UNIX desejadas no volume montado.

7. Em um sistema cliente UNIX identificado em suas regras de exportação, faça login como um dos usuários autorizados que agora tem acesso ao novo volume e repita os procedimentos nas etapas 3 a 5 para verificar se você pode montar o volume e criar um arquivo.

Onde encontrar informações adicionais

Depois de testar com êxito o acesso ao cliente NFS, você pode executar uma configuração NFS adicional ou adicionar acesso SAN. Quando o acesso ao protocolo estiver concluído, você deverá proteger o volume raiz da máquina virtual de storage (SVM).

Configuração NFS

Você pode configurar ainda mais o acesso NFS usando as seguintes informações e relatórios técnicos:

- "Gerenciamento de NFS"

  Descreve como configurar e gerenciar o acesso a arquivos usando NFS.

- "Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"

  Serve como um guia operacional NFSv3 e NFSv4 e fornece uma visão geral do sistema operacional ONTAP com foco em NFSv4.

- "Relatório técnico da NetApp 4073: Autenticação unificada segura"

  Explica como configurar o ONTAP para uso com servidores Kerberos baseados em UNIX versão 5 (krb5) para autenticação de armazenamento NFS e AD (AD) como provedor de identidade KDC e LDAP (Lightweight Directory Access Protocol).

- "Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

  Descreve as práticas recomendadas que devem ser seguidas durante a implementação de componentes NFSv4 em clientes AIX, Linux ou Solaris conetados a sistemas que executam o ONTAP.

Configuração de rede

Você pode configurar ainda mais recursos de rede e serviços de nome usando as seguintes informações e relatórios técnicos:

- "Gerenciamento de NFS"

  Descreve como configurar e gerenciar redes ONTAP.

- "Relatório técnico da NetApp 4182: Considerações sobre o projeto de armazenamento Ethernet e práticas recomendadas para configurações de Data ONTAP em cluster"

  Descreve a implementação das configurações de rede ONTAP e fornece cenários comuns de implantação de rede e recomendações de práticas recomendadas.

- "Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

  Explica como configurar LDAP, NIS, DNS e configuração de arquivos locais para fins de autenticação.

Configuração do protocolo SAN

Se quiser fornecer ou modificar o acesso SAN ao novo SVM, você pode usar as informações de configuração FC ou iSCSI, que estão disponíveis para vários sistemas operacionais de host.

Proteção do volume raiz

Depois de configurar protocolos no SVM, você deve garantir que seu volume raiz esteja protegido:

- "Proteção de dados"

  Descreve como criar um espelhamento de compartilhamento de carga para proteger o volume raiz da SVM, que é uma prática recomendada do NetApp para SVMs habilitadas para nas. Também descreve como recuperar rapidamente de falhas ou perdas de volume promovendo o volume raiz do SVM a partir de um espelhamento de compartilhamento de carga.

Como as exportações do ONTAP diferem das exportações do modo 7

Como as exportações do ONTAP diferem das exportações do modo 7

Se não estiver familiarizado com a forma como o ONTAP implementa as exportações de NFS, pode comparar as ferramentas de configuração de exportação de modo 7D e ONTAP, bem como exemplos de arquivos de modo 7D `/etc/exports` com políticas e regras em cluster.

No ONTAP não há `/etc/exports` nenhum arquivo e nenhum `exportfs` comando. Em vez disso, você deve definir uma política de exportação. As políticas de exportação permitem que você controle o acesso do cliente da mesma forma que você fez no modo 7, mas oferecem funcionalidades adicionais, como a capacidade de reutilizar a mesma política de exportação para vários volumes.

Informações relacionadas

"Gerenciamento de NFS"

"Relatório técnico da NetApp 4067: Guia de práticas recomendadas e implementação de NFS"

Comparação de exportações em modo 7D e ONTAP

As exportações no ONTAP são definidas e usadas de forma diferente do que em ambientes de 7 modos.

Áreas de diferença	Modo 7D.	ONTAP
Como as exportações são definidas	As exportações são definidas `/etc/exports` no arquivo.	As exportações são definidas criando uma política de exportação em um SVM. O SVM pode incluir mais de uma política de exportação.

Âmbito de exportação	• As exportações se aplicam a um caminho ou qtree de arquivo especificado. • Você deve criar uma entrada separada em `/etc/exports` para cada caminho ou qtree de arquivo. • As exportações são persistentes somente se forem definidas no `/etc/exports` arquivo.	• As políticas de exportação se aplicam a um volume inteiro, incluindo todos os caminhos de arquivo e qtrees contidos no volume. • As políticas de exportação podem ser aplicadas a mais de um volume, se desejar. • Todas as políticas de exportação são persistentes nas reinicializações do sistema.
Esgrima (especificando acesso diferente para clientes específicos aos mesmos recursos)	Para fornecer a clientes específicos acesso diferente a um único recurso exportado, você tem que listar cada cliente e seu acesso permitido no `/etc/exports` arquivo.	As políticas de exportação são compostas por várias regras de exportação individuais. Cada regra de exportação define permissões de acesso específicas para um recurso e lista os clientes que têm essas permissões. Para especificar um acesso diferente para clientes específicos, você precisa criar uma regra de exportação para cada conjunto específico de permissões de acesso, listar os clientes que têm essas permissões e, em seguida, adicionar as regras à política de exportação.
Alias de nome	Ao definir uma exportação, pode optar por tornar o nome da exportação diferente do nome do caminho do ficheiro. Você deve usar o `-actual` parâmetro ao definir tal exportação no `/etc/exports` arquivo.	Pode optar por tornar o nome do volume exportado diferente do nome do volume real. Para fazer isso, é necessário montar o volume com um nome de caminho de junção personalizado no namespace SVM. Por padrão, os volumes são montados com seu nome de volume. Para personalizar o nome do caminho de junção de um volume, você precisa desmontá-lo, renomeá-lo e remontá-lo.

Exemplos de políticas de exportação do ONTAP

Você pode revisar exemplos de políticas de exportação para entender melhor como as políticas de exportação funcionam no ONTAP.

Exemplo de implementação do ONTAP de uma exportação de 7 modos

O exemplo a seguir mostra uma exportação do modo 7 como aparece no `/etc/export` arquivo:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Para reproduzir essa exportação como uma política de exportação em cluster, você precisa criar uma política de exportação com três regras de exportação e atribuir a política de exportação ao volume vol1.

Regra	Elemento	Valor
Regra 1	`-clientmatch` (especificação do cliente)	`@readonly_netgroup`
`-ruleindex`(posição da regra de exportação na lista de regras)	`1`	`-protocol`
`nfs`	`-rorule`(permitir acesso somente leitura)	`sys` (Cliente autenticado com AUTH_SYS)
`-rwrule`(permitir acesso de leitura e gravação)	`never`	`-superuser`(permitir acesso ao superusuário)
`none`(root *squashed* para anon)	Regra 2	`-clientmatch`
`@rootaccess_netgroup`	`-ruleindex`	`2`
`-protocol`	`nfs`	`-rorule`
`sys`	`-rwrule`	`sys`
`-superuser`	`sys`	Regra 3
`-clientmatch`	`@readwrite_netgroup1,@readwrite_netgroup2`	`-ruleindex`
`3`	`-protocol`	`nfs`
`-rorule`	`sys`	`-rwrule`

Regra	Elemento	Valor
sys	-superuser	none

1. Crie uma política de exportação chamada exp_vol1:

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. Crie três regras com os seguintes parâmetros para o comando base:
   - Base de comando
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - Parâmetros da regra
     `-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys -rwrule never -superuser none -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys -rwrule sys -superuser sys -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule sys -rwrule sys -superuser none`

3. Atribua a política ao volume vol1:

   ```
   volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
   ```

Consolidação de amostra de exportações de 7 modos

O exemplo a seguir mostra um arquivo de 7 modos `/etc/export` que inclui uma linha para cada um dos 10 qtrees:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

No ONTAP, uma de duas políticas é necessária para cada qtree: Uma com uma regra que inclui `-clientmatch host1519s`, ou outra com uma regra que `-clientmatch host2057s`inclui .

1. Crie duas políticas de exportação chamadas exp_vol1q1 e exp_vol1q2:
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. Crie uma regra para cada política:
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1`

```
-clientmatch host1519s -rwrule sys -superuser sys
```

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`

3. Aplique as políticas ao qtrees:
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [next 4 qtrees…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [next 4 qtrees…]

Se você precisar adicionar qtrees adicionais para esses hosts mais tarde, você usaria as mesmas políticas de exportação.

Gerencie o NFS com a CLI

Visão geral de referência de NFS

O ONTAP inclui recursos de acesso a arquivos disponíveis para o protocolo NFS. Você pode habilitar um servidor NFS e exportar volumes ou qtrees.

Você executa este procedimento nas seguintes circunstâncias:

- Você quer entender a variedade de funcionalidades do protocolo NFS da ONTAP.
- Você deseja executar tarefas menos comuns de configuração e manutenção, não configuração básica de NFS.
- Você deseja usar a interface de linha de comando (CLI), não o System Manager ou uma ferramenta de script automatizado.

Entenda o acesso a arquivos nas

Namespaces e pontos de junção

Visão geral de namespaces e pontos de junção

Um nas *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem residir em qualquer lugar do cluster.

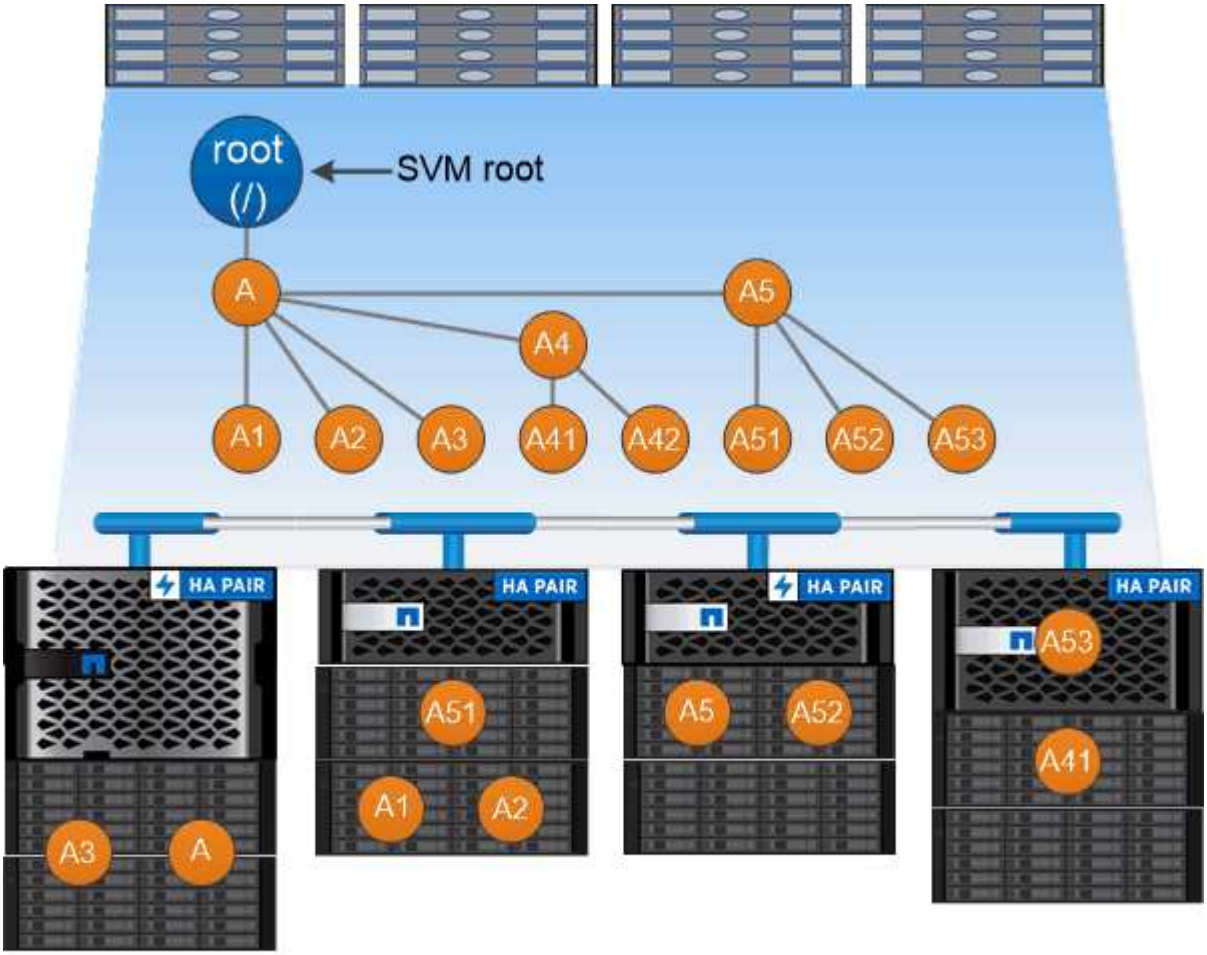
Em vez de montar cada volume contendo um arquivo de interesse, os clientes nas montam um NFS *export* ou acessam um SMB *share.* a exportação ou compartilhamento representa todo o namespace ou um local intermediário dentro do namespace. O cliente acessa apenas os volumes montados abaixo do seu ponto de acesso.

Você pode adicionar volumes ao namespace conforme necessário. Você pode criar pontos de junção diretamente abaixo de uma junção de volume pai ou em um diretório dentro de um volume. Um caminho para

uma junção de volume para um volume chamado "'vol3" pode ser `/vol1/vol2/vol3`, ou `/vol1/dir2/vol3`, ou mesmo `/dir1/dir2/vol3`. O caminho é chamado de *caminho de junção.*

Cada SVM tem um namespace único. O volume raiz da SVM é o ponto de entrada para a hierarquia de namespace.

Para garantir que os dados permaneçam disponíveis no caso de uma interrupção do nó ou failover, você deve criar uma cópia de *load-sharing mirror* para o volume raiz da SVM.



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

Quais são as arquiteturas típicas de namespace nas

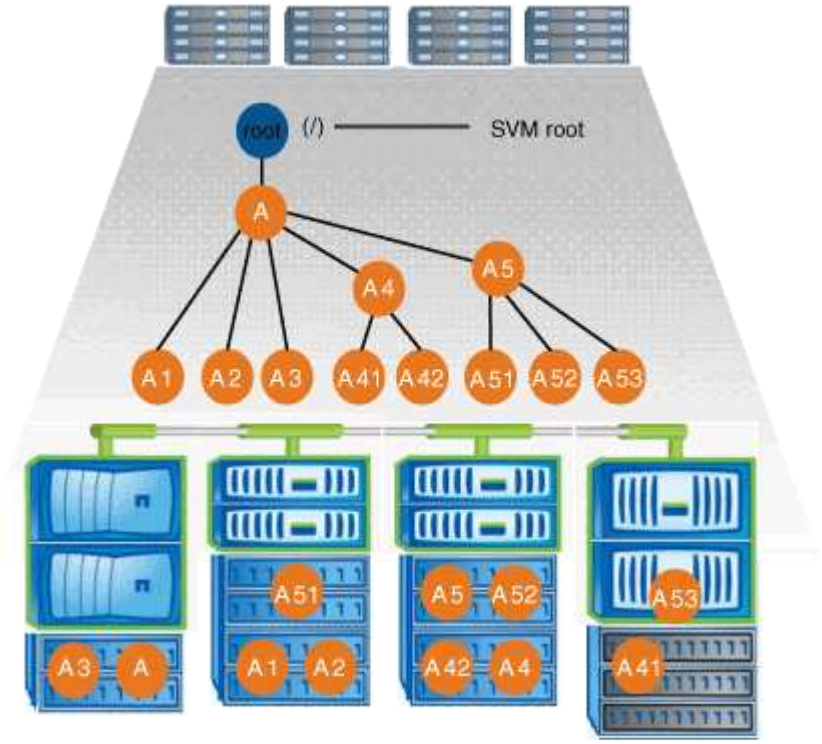
Há várias arquiteturas típicas de namespace nas que você pode usar ao criar seu espaço de nomes SVM. Você pode escolher a arquitetura de namespace que corresponde às necessidades da sua empresa e do fluxo de trabalho.

A parte superior do namespace é sempre o volume raiz, que é representado por uma barra (/). A arquitetura de namespace sob a raiz se enquadra em três categorias básicas:

- Uma única árvore ramificada, com apenas uma única junção para a raiz do namespace
- Várias árvores ramificadas, com vários pontos de junção para a raiz do namespace
- Vários volumes independentes, cada um com um ponto de junção separado para a raiz do espaço de nomes

Namespace com árvore ramificada única

Uma arquitetura com uma única árvore ramificada tem um único ponto de inserção para a raiz do namespace SVM. O ponto de inserção único pode ser um volume juntado ou um diretório sob a raiz. Todos os outros volumes são montados em pontos de junção abaixo do ponto de inserção único (que pode ser um volume ou um diretório).

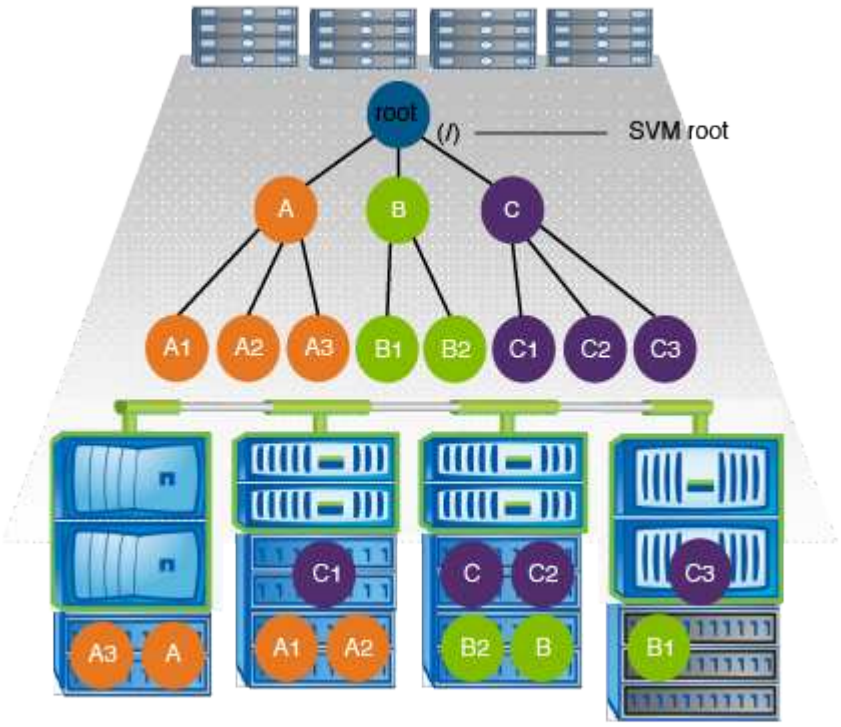


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde todos os volumes são juntados abaixo do ponto de inserção único, que é um diretório chamado "data":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     corp1       true     /data/dir1/corp1       RW_volume
vs1     corp2       true     /data/dir1/corp2       RW_volume
vs1     data1       true     /data/data1            RW_volume
vs1     eng1        true     /data/data1/eng1       RW_volume
vs1     eng2        true     /data/data1/eng2       RW_volume
vs1     sales       true     /data/data1/sales      RW_volume
vs1     vol1        true     /data/vol1             RW_volume
vs1     vol2        true     /data/vol2             RW_volume
vs1     vol3        true     /data/vol3             RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com várias árvores ramificadas

Uma arquitetura com várias árvores ramificadas tem vários pontos de inserção na raiz do namespace SVM. Os pontos de inserção podem ser volumes juntados ou diretórios abaixo da raiz. Todos os outros volumes são montados em pontos de junção abaixo dos pontos de inserção (que podem ser volumes ou diretórios).

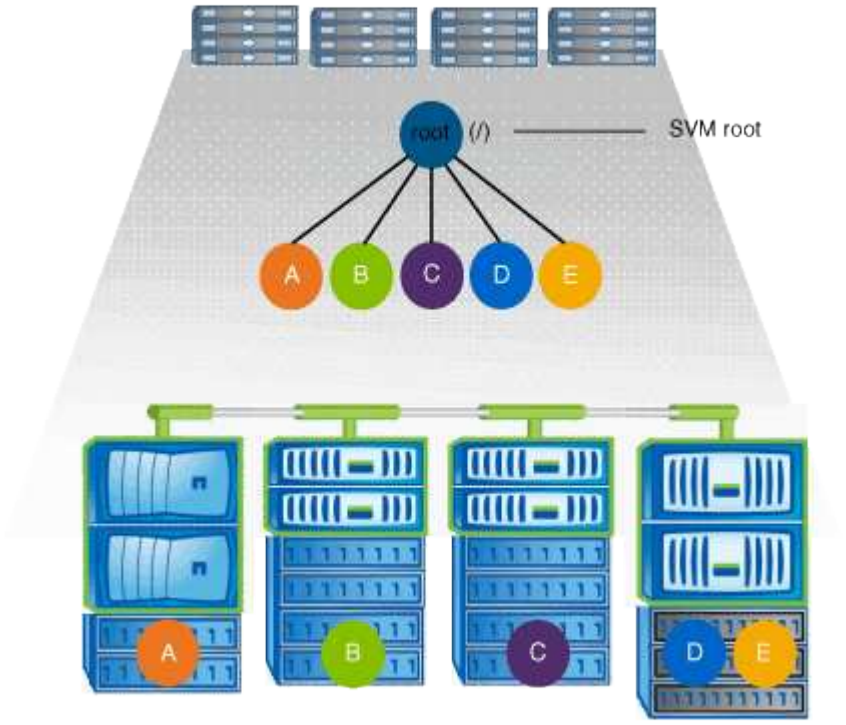


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há três pontos de inserção para o volume raiz do SVM. Dois pontos de inserção são diretórios denominados "data" e "projetos". Um ponto de inserção é um volume juntado chamado "audit":

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     audit       true     /audit                 RW_volume
vs1     audit_logs1 true     /audit/logs1           RW_volume
vs1     audit_logs2 true     /audit/logs2           RW_volume
vs1     audit_logs3 true     /audit/logs3           RW_volume
vs1     eng         true     /data/eng              RW_volume
vs1     mktg1       true     /data/mktg1            RW_volume
vs1     mktg2       true     /data/mktg2            RW_volume
vs1     project1    true     /projects/project1     RW_volume
vs1     project2    true     /projects/project2     RW_volume
vs1     vs1_root    -        /                      -
```

Namespace com vários volumes autônomos

Em uma arquitetura com volumes autônomos, cada volume tem um ponto de inserção para a raiz do namespace SVM. No entanto, o volume não é juntado abaixo de outro volume. Cada volume tem um caminho exclusivo e é juntado diretamente abaixo da raiz ou é juntado sob um diretório abaixo da raiz.



Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há cinco pontos de inserção para o volume raiz do SVM, com cada ponto de inserção representando um caminho para um volume.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

Como o ONTAP controla o acesso aos arquivos

Como o ONTAP controla o acesso aos arquivos

O ONTAP controla o acesso aos arquivos de acordo com as restrições baseadas em autenticação e em arquivo especificadas.

Quando um cliente se coneta ao sistema de armazenamento para acessar arquivos, o ONTAP tem que executar duas tarefas:

- Autenticação

  O ONTAP tem que autenticar o cliente verificando a identidade com uma fonte confiável. Além disso, o tipo de autenticação do cliente é um método que pode ser usado para determinar se um cliente pode acessar dados ao configurar políticas de exportação (opcional para CIFS).

- Autorização

  O ONTAP tem que autorizar o usuário comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório e determinando que tipo de acesso, se houver, a fornecer.

Para gerenciar adequadamente o controle de acesso a arquivos, o ONTAP deve se comunicar com serviços externos, como NIS, LDAP e servidores do ative Directory. A configuração de um sistema de storage para acesso a arquivos usando CIFS ou NFS requer a configuração dos serviços apropriados, dependendo do seu ambiente no ONTAP.

Restrições baseadas em autenticação

Com restrições baseadas em autenticação, você pode especificar quais máquinas cliente e quais usuários podem se conetar à máquina virtual de armazenamento (SVM).

O ONTAP suporta autenticação Kerberos de servidores UNIX e Windows.

Restrições baseadas em arquivos

O ONTAP avalia três níveis de segurança para determinar se uma entidade está autorizada a executar uma ação solicitada em arquivos e diretórios localizados em um SVM. O acesso é determinado pelas permissões efetivas após a avaliação dos três níveis de segurança.

Qualquer objeto de armazenamento pode conter até três tipos de camadas de segurança:

- Segurança de exportação (NFS) e compartilhamento (SMB)

  A segurança de exportação e compartilhamento se aplica ao acesso do cliente a uma determinada exportação NFS ou compartilhamento SMB. Os usuários com Privileges administrativo podem gerenciar a segurança de exportação e compartilhamento a partir de clientes SMB e NFS.

- Segurança de arquivo e diretório do Access Guard no nível de armazenamento

  A segurança do Access Guard no nível de storage se aplica ao acesso de clientes SMB e NFS aos volumes SVM. Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

  > Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança do Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

- Segurança nativa em nível de arquivo NTFS, UNIX e NFSv4

  A segurança de nível de arquivo nativo existe no arquivo ou diretório que representa o objeto de storage. Você pode definir a segurança no nível do arquivo de um cliente. As permissões de arquivo são efetivas independentemente de SMB ou NFS serem usados para acessar os dados.

Como o ONTAP lida com a autenticação de cliente NFS

Como o ONTAP lida com a visão geral da autenticação do cliente NFS

Os clientes NFS devem ser devidamente autenticados antes de poderem acessar os dados no SVM. O ONTAP autentica os clientes verificando suas credenciais UNIX em relação aos serviços de nome que você configura.

Quando um cliente NFS se coneta ao SVM, o ONTAP obtém as credenciais UNIX para o usuário verificando diferentes serviços de nome, dependendo da configuração dos serviços de nome do SVM. O ONTAP pode verificar credenciais para contas UNIX locais, domínios NIS e domínios LDAP. Pelo menos um deles deve ser configurado para que o ONTAP possa autenticar com êxito o usuário. Você pode especificar vários serviços de nomes e a ordem em que o ONTAP os procura.

Em um ambiente NFS puro com estilos de segurança de volume UNIX, essa configuração é suficiente para autenticar e fornecer o acesso de arquivo adequado para um usuário conetado a partir de um cliente NFS.

Se você estiver usando estilos de segurança de volume misto, NTFS ou unificado, o ONTAP deve obter um nome de usuário SMB para o usuário UNIX para autenticação com um controlador de domínio do Windows. Isso pode acontecer mapeando usuários individuais usando contas UNIX locais ou domínios LDAP, ou usando um usuário SMB padrão em vez disso. Você pode especificar quais serviços de nome o ONTAP pesquisa em qual ordem ou especificar um usuário SMB padrão.

Como o ONTAP usa os serviços de nomes

O ONTAP usa serviços de nome para obter informações sobre usuários e clientes. O

ONTAP usa essas informações para autenticar usuários acessando dados ou administrando o sistema de storage e mapear credenciais de usuário em um ambiente misto.

Ao configurar o sistema de storage, você deve especificar quais serviços de nome deseja que o ONTAP use para obter credenciais de usuário para autenticação. O ONTAP oferece suporte aos seguintes serviços de nomes:

- Utilizadores locais (ficheiro)
- Domínios NIS externos (NIS)
- Domínios LDAP externos (LDAP)

Você usa a `vserver services name-service ns-switch` família de comandos para configurar SVMs com as fontes para procurar informações de rede e a ordem na qual pesquisá-las. Esses comandos fornecem a funcionalidade equivalente do `/etc/nsswitch.conf` arquivo em sistemas UNIX.

Quando um cliente NFS se coneta ao SVM, o ONTAP verifica os serviços de nome especificados para obter as credenciais UNIX do usuário. Se os serviços de nome estiverem configurados corretamente e o ONTAP puder obter as credenciais UNIX, o ONTAP autentica o usuário com êxito.

Em um ambiente com estilos de segurança mistos, o ONTAP pode ter que mapear as credenciais do usuário. Você deve configurar os serviços de nome adequadamente para o seu ambiente para permitir que o ONTAP mapeie corretamente as credenciais do usuário.

O ONTAP também usa serviços de nomes para autenticar contas de administrador da SVM. Você deve ter isso em mente ao configurar ou modificar o switch do serviço de nomes para evitar desabilitar acidentalmente a autenticação para contas de administrador SVM. Para obter mais informações sobre usuários de administração do SVM, "Autenticação de administrador e RBAC"consulte .

Como o ONTAP concede acesso a arquivos SMB de clientes NFS

O ONTAP usa a semântica de segurança do sistema de arquivos do Windows NT (NTFS) para determinar se um usuário UNIX, em um cliente NFS, tem acesso a um arquivo com permissões NTFS.

O ONTAP faz isso convertendo o ID de usuário UNIX do usuário (UID) em uma credencial SMB e, em seguida, usando a credencial SMB para verificar se o usuário tem direitos de acesso ao arquivo. Uma credencial SMB consiste em um SID (Identificador de Segurança primário), geralmente o nome de usuário do Windows do usuário e um ou mais SIDs de grupo que correspondem aos grupos do Windows dos quais o usuário é membro.

O Time ONTAP leva a conversão do UID UNIX em uma credencial SMB pode ser de dezenas de milissegundos a centenas de milissegundos, porque o processo envolve entrar em Contato com um controlador de domínio. O ONTAP mapeia o UID para a credencial SMB e insere o mapeamento em um cache de credenciais para reduzir o tempo de verificação causado pela conversão.

Como funciona o cache de credenciais NFS

Quando um usuário NFS solicita acesso às exportações de NFS no sistema de storage, o ONTAP deve recuperar as credenciais de usuário de servidores de nomes externos ou de arquivos locais para autenticar o usuário. Em seguida, o ONTAP armazena essas credenciais em um cache interno de credenciais para referência posterior. Entender

como os caches de credenciais NFS funcionam permite que você lide com possíveis problemas de desempenho e acesso.

Sem o cache de credenciais, o ONTAP teria que consultar serviços de nomes sempre que um usuário NFS solicitou acesso. Em um sistema de armazenamento ocupado que é acessado por muitos usuários, isso pode rapidamente levar a sérios problemas de desempenho, causando atrasos indesejados ou até mesmo negações ao acesso do cliente NFS.

Com o cache de credenciais, o ONTAP recupera as credenciais do usuário e as armazena por um período predeterminado de tempo para acesso rápido e fácil caso o cliente NFS envie outra solicitação. Este método oferece as seguintes vantagens:

- Ele facilita a carga no sistema de armazenamento, manipulando menos solicitações para servidores de nomes externos (como NIS ou LDAP).
- Ele facilita a carga em servidores de nomes externos, enviando menos solicitações para eles.
- Ele acelera o acesso do usuário eliminando o tempo de espera para obter credenciais de fontes externas antes que o usuário possa ser autenticado.

O ONTAP armazena credenciais positivas e negativas no cache de credenciais. Credenciais positivas significa que o usuário foi autenticado e recebeu acesso. Credenciais negativas significa que o usuário não foi autenticado e foi negado o acesso.

Por padrão, o ONTAP armazena credenciais positivas por 24 horas; ou seja, após a autenticação inicial de um usuário, o ONTAP usa as credenciais em cache para quaisquer solicitações de acesso por esse usuário por 24 horas. Se o usuário solicitar acesso após 24 horas, o ciclo será iniciado novamente: O ONTAP descarta as credenciais armazenadas em cache e obtém as credenciais novamente a partir da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as 24 horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas 24 horas.

Por padrão, o ONTAP armazena credenciais negativas por duas horas; ou seja, depois de inicialmente negar acesso a um usuário, o ONTAP continua negando quaisquer solicitações de acesso por esse usuário por duas horas. Se o usuário solicitar acesso após 2 horas, o ciclo será iniciado novamente: O ONTAP obtém as credenciais novamente da fonte de serviço de nome apropriada. Se as credenciais tiverem sido alteradas no servidor de nomes durante as duas horas anteriores, o ONTAP armazena em cache as credenciais atualizadas para uso nas próximas duas horas.

Crie e gerencie volumes de dados em namespaces nas

Crie volumes de dados com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Os seguintes carateres não podem ser usados no caminho de junção: * *

Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed} -junction-path junction_path
   ```

   O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   O caminho de junção é insensível a maiúsculas e minúsculas; `/ENG` é o mesmo que `/eng`. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for `/ENG`, o caminho de um compartilhamento SMB deve começar com `/ENG`, não `/eng`.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home`:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Crie volumes de dados sem especificar pontos de junção

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

- O agregado no qual você deseja criar o volume já deve existir.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando:

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado sem um ponto de junção:

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

Montar ou desmontar volumes existentes no namespace nas

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você pode montar um volume em um ponto de junção se ele não estiver montado no momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.

> Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento:
>
> "Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"

Quando você desmontar e off-line um volume, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser…	Digite os comandos…
Monte um volume	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*

Se você quiser…	Digite os comandos…

Desmontar um volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Verifique se o volume está no estado de montagem desejado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

O exemplo a seguir desmonta e fica offline um volume chamado "data" localizado na SVM ""VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Apresentar informações sobre a montagem do volume e o ponto de junção

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados.

Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passo

1. Execute a ação desejada:

Se você quiser exibir…	Digite o comando…
Informações resumidas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -volume volume_name -instance`
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Apresentar a informação pretendida utilizando o `-fields` parâmetro: `volume show -vserver vserver_name -fields fieldname,…`

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, Visão geral do gerenciamento do FlexGroup volumesconsulte .

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.

> O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Onde e quando definir estilos de segurança

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema

de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se…
UNIX	• O sistema de arquivos é gerenciado por um administrador UNIX. • A maioria dos usuários são clientes NFS. • Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	• O sistema de arquivos é gerenciado por um administrador do Windows. • A maioria dos usuários são clientes SMB. • Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	• O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

  Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz do SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

   As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado:

   `vserver show -vserver` *`vserver_name`*

Configurar estilos de segurança no FlexVol volumes

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume…	Use o comando…
Ainda não existe	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

   Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

   Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte comando:

   ```
   volume show -volume volume_name -instance
   ```

Configurar estilos de segurança no qtrees

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree…	Use o comando…
Ainda não existe	`volume qtree create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume qtree modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

   Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será

`mixed`.

Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Configurar o acesso a arquivos usando NFS

Configure o acesso a arquivos usando a visão geral do NFS

Você deve concluir várias etapas para permitir que os clientes acessem arquivos em máquinas virtuais de armazenamento (SVMs) usando NFS. Existem algumas etapas adicionais que são opcionais, dependendo da configuração atual do seu ambiente.

Para que os clientes possam acessar arquivos em SVMs usando NFS, você deve concluir as seguintes tarefas:

1. Habilite o protocolo NFS na SVM.

   Você precisa configurar o SVM para permitir acesso a dados de clientes em NFS.

2. Criar um servidor NFS no SVM.

   Um servidor NFS é uma entidade lógica no SVM que permite que o SVM forneça arquivos em NFS. Você deve criar o servidor NFS e especificar as versões do protocolo NFS que deseja permitir.

3. Configurar políticas de exportação no SVM.

   Você deve configurar políticas de exportação para tornar os volumes e qtrees disponíveis para os clientes.

4. Configure o servidor NFS com a segurança adequada e outras configurações, dependendo da rede e do ambiente de armazenamento.

   Esta etapa pode incluir a configuração Kerberos, "NFS em TLS", LDAP, NIS, mapeamentos de nomes e usuários locais.

Proteja o acesso NFS usando políticas de exportação

Como as políticas de exportação controlam o acesso do cliente a volumes ou qtrees

As políticas de exportação contêm uma ou mais *regras de exportação* que processam cada solicitação de acesso de cliente. O resultado do processo determina se o cliente é negado ou concedido acesso e que nível de acesso. Uma política de exportação com regras de exportação deve existir na máquina virtual de storage (SVM) para que os clientes acessem os dados.

Você associa exatamente uma política de exportação a cada volume ou qtree para configurar o acesso do cliente ao volume ou qtree. O SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes ou qtrees:

- Atribua diferentes políticas de exportação a cada volume ou qtree do SVM para controle de acesso de cliente individual a cada volume ou qtree no SVM.
- Atribua a mesma política de exportação a vários volumes ou qtrees do SVM para controle de acesso de cliente idêntico sem ter que criar uma nova política de exportação para cada volume ou qtree.

Se um cliente fizer uma solicitação de acesso que não é permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados.

Você pode modificar uma política de exportação dinamicamente em um sistema executando o ONTAP.

Política de exportação padrão para SVMs

Cada SVM tem uma política de exportação padrão que não contém regras. Uma política de exportação com regras deve existir antes que os clientes possam acessar os dados no SVM. Cada FlexVol volume contido no SVM deve estar associado a uma política de exportação.

Ao criar um SVM, o sistema de storage cria automaticamente uma política de exportação padrão chamada `default` volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM. Como alternativa, você pode criar uma política de exportação personalizada com regras. Você pode modificar e renomear a política de exportação padrão, mas não pode excluir a política de exportação padrão.

Quando você cria um FlexVol volume que contém o SVM, o sistema de storage cria o volume e associa o volume à política de exportação padrão para o volume raiz do SVM. Por padrão, cada volume criado no SVM está associado à política de exportação padrão do volume raiz. Você pode usar a política de exportação padrão para todos os volumes contidos no SVM ou criar uma política de exportação exclusiva para cada volume. Você pode associar vários volumes à mesma política de exportação.

Como funcionam as regras de exportação

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

  O tamanho máximo para o `-clientmatch` campo é de 4096 carateres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

> A partir do ONTAP 9.3, você pode habilitar a verificação de configuração de política de exportação como uma tarefa em segundo plano que Registra quaisquer violações de regras em uma lista de regras de erro. Os `vserver export-policy config-checker` comandos invocam o verificador e exibem resultados, que podem ser usados para verificar sua configuração e excluir regras errôneas da política.
>
> Os comandos apenas validam a configuração de exportação para nomes de host, netgroups e usuários anônimos.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Gerencie clientes com um tipo de segurança não listado

Quando um cliente se apresenta com um tipo de segurança que não está listado em um parâmetro de acesso de uma regra de exportação, você tem a opção de negar acesso ao cliente ou mapeá-lo para o ID de usuário anônimo usando a opção `none` no parâmetro de acesso.

Um cliente pode apresentar-se com um tipo de segurança que não está listado em um parâmetro de acesso porque foi autenticado com um tipo de segurança diferente ou não foi autenticado de todo (tipo de segurança AUTH_NONE). Por padrão, o cliente é automaticamente negado o acesso a esse nível. No entanto, você pode adicionar a opção `none` ao parâmetro Access. Como resultado, os clientes com um estilo de segurança não listado são mapeados para o ID de usuário anônimo. O `-anon` parâmetro determina qual ID de usuário é atribuído a esses clientes. O ID de usuário especificado para o `-anon` parâmetro deve ser um usuário válido que esteja configurado com permissões que você considere apropriadas para o usuário anônimo.

Valores válidos para o `-anon` intervalo de parâmetros `0` de a `65535`.

ID de utilizador atribuída a `-anon`	**Processamento resultante de solicitações de acesso do cliente**
`0 - 65533`	A solicitação de acesso do cliente é mapeada para o ID de usuário anônimo e obtém acesso dependendo das permissões configuradas para esse usuário.
`65534`	A solicitação de acesso do cliente é mapeada para o usuário ninguém e obtém acesso dependendo das permissões configuradas para esse usuário. Este é o padrão.
`65535`	A solicitação de acesso de qualquer cliente é negada quando mapeada para essa ID e o cliente se apresenta com o tipo de segurança AUTH_NONE. A solicitação de acesso de clientes com ID de usuário 0 é negada quando mapeada para essa ID e o cliente se apresenta com qualquer outro tipo de segurança.

Ao usar a opção `none`, é importante lembrar que o parâmetro somente leitura é processado primeiro. Considere as seguintes diretrizes ao configurar regras de exportação para clientes com tipos de segurança não listados:

Somente leitura inclui `none`	**A leitura-gravação inclui** `none`	**Acesso resultante para clientes com tipos de segurança não listados**
Não	Não	Negado
Não	Sim	Negado porque somente leitura é processada primeiro
Sim	Não	Somente leitura como anônima
Sim	Sim	Leia-escreva como anônimo

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a qualquer tipo de segurança, mas neste caso só se aplica a clientes já filtrados pela regra somente leitura.

Portanto, os clientes nº 1 e nº 3 recebem acesso de leitura e gravação apenas como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso de leitura e gravação com seu próprio ID de usuário.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (ou seja, o tipo de segurança AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a clientes com seu próprio ID de usuário autenticado com AUTH_SYS. O parâmetro somente leitura permite o acesso somente leitura como usuário anônimo com ID de usuário 70 para clientes autenticados usando qualquer outro tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação somente como usuário anônimo.

Portanto, o cliente nº 1 e o cliente nº 3 recebem acesso de leitura e gravação somente como usuário anônimo com ID de usuário 70. O cliente nº 2 obtém acesso somente leitura com seu próprio ID de usuário, mas é negado o acesso de leitura e gravação.

Como os tipos de segurança determinam os níveis de acesso do cliente

O tipo de segurança com o qual o cliente autenticou desempenha um papel especial nas regras de exportação. Você deve entender como o tipo de segurança determina os níveis de acesso que o cliente obtém a um volume ou qtree.

Os três níveis de acesso possíveis são os seguintes:

1. Somente leitura
2. Leitura-gravação
3. Superusuário (para clientes com ID de usuário 0)

Como o nível de acesso por tipo de segurança é avaliado nesta ordem, você deve observar as seguintes regras ao construir parâmetros de nível de acesso em regras de exportação:

Para um cliente obter nível de acesso…	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente…
Apenas de leitura normal do utilizador	Somente leitura (`-rorule`)
Leitura-escrita normal do utilizador	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`)
Somente leitura do superusuário	Apenas leitura (`-rorule`) e. `-superuser`

Para um cliente obter nível de acesso…	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente…
Leitura-gravação do superusuário	Somente leitura (`-rorule`) e leitura-gravação (`-rwrule`) e. `-superuser`

Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- `any`
- `none`
- `never`

  Este tipo de segurança não é válido para utilização com o `-superuser` parâmetro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Ao combinar o tipo de segurança de um cliente com cada um dos três parâmetros de acesso, há três resultados possíveis:

Se o tipo de segurança do cliente…	Então o cliente…
Corresponde ao especificado no parâmetro Access.	Obtém acesso para esse nível com seu próprio ID de usuário.
Não corresponde ao especificado, mas o parâmetro Access inclui a opção `none`.	Obtém acesso para esse nível, mas como o usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro.
Não corresponde ao especificado e o parâmetro Access não inclui a opção `none`.	Não obtém acesso para esse nível. Isso não se aplica ao `-superuser` parâmetro porque ele sempre inclui `none` mesmo quando não especificado.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys,krb5`
- `-superuser krb5`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O cliente nº 3 tem o endereço IP 10,1.16,234, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e não autenticou (AUTH_NONE).

O protocolo de acesso do cliente e o endereço IP correspondem aos três clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança. O parâmetro read-write permite o acesso de leitura-gravação a clientes com sua própria ID de usuário autenticado com AUTH_SYS ou Kerberos v5. O parâmetro superuser permite o acesso do superusuário a clientes com ID de usuário 0 autenticado com Kerberos v5.

Portanto, o cliente nº 1 obtém acesso de leitura e gravação do superusuário porque ele corresponde aos três parâmetros de acesso. O cliente nº 2 obtém acesso de leitura e gravação, mas não acesso ao superusuário. O cliente nº 3 obtém acesso somente leitura, mas não acesso ao superusuário.

Gerenciar solicitações de acesso de superusuário

Ao configurar políticas de exportação, você precisa considerar o que deseja acontecer se o sistema de armazenamento receber uma solicitação de acesso de cliente com ID de usuário 0, ou seja, como superusuário, e configurar suas regras de exportação de acordo.

No mundo UNIX, um usuário com o ID de usuário 0 é conhecido como superusuário, normalmente chamado de root, que tem direitos de acesso ilimitados em um sistema. O uso do superusuário Privileges pode ser perigoso por várias razões, incluindo a violação do sistema e da segurança de dados.

Por padrão, o ONTAP mapeia os clientes que apresentam com ID de usuário 0 para o usuário anônimo. No entanto, você pode especificar o `- superuser` parâmetro em regras de exportação para determinar como lidar com clientes que apresentam com ID de usuário 0, dependendo do seu tipo de segurança. A seguir estão as opções válidas para o `-superuser` parâmetro:

- `any`
- `none`

  Esta é a configuração padrão se você não especificar o `-superuser` parâmetro.

- `krb5`
- `ntlm`
- `sys`

Há duas maneiras diferentes de como os clientes que apresentam com ID de usuário 0 são manipulados, dependendo da `-superuser` configuração do parâmetro:

Se o `-superuser` parâmetro e o tipo de segurança do cliente…	**Então o cliente…**
Correspondência	Obtém acesso de superusuário com ID de usuário 0.

Se o `-superuser` parâmetro e o tipo de segurança do cliente…	Então o cliente…
Não corresponder	Obtém acesso como usuário anônimo com o ID de usuário especificado pelo `-anon` parâmetro e suas permissões atribuídas. Isso é independentemente de o parâmetro somente leitura ou leitura-gravação especificar a opção `none`.

Se um cliente apresentar com ID de usuário 0 para acessar um volume com estilo de segurança NTFS e o `-superuser` parâmetro estiver definido como `none`, o ONTAP usará o mapeamento de nomes para o usuário anônimo obter as credenciais adequadas.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 746, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar.

O cliente nº 2 não obtém acesso ao superusuário. Em vez disso, ele é mapeado para anônimo porque o `-superuser` parâmetro não é especificado. Isto significa que o padrão é `none` e mapeia automaticamente a ID do usuário 0 para anônimo. O cliente nº 2 também só obtém acesso somente leitura porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

O cliente nº 1 tem o endereço IP 10,1.16,207, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, tem ID de usuário 0, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

A regra de exportação permite o acesso do superusuário para clientes com ID de usuário 0. O cliente nº 1 obtém acesso ao superusuário porque corresponde ao ID do usuário e ao tipo de segurança para somente leitura e `-superuser` parâmetros. O cliente nº 2 não obtém acesso de leitura-escrita ou superusuário porque seu tipo de segurança não corresponde ao parâmetro de leitura-gravação ou ao `-superuser` parâmetro. Em vez disso, o cliente nº 2 é mapeado para o usuário anônimo, que neste caso tem o ID de usuário 0.

Como o ONTAP usa caches de política de exportação

Para melhorar o desempenho do sistema, o ONTAP usa caches locais para armazenar informações como nomes de host e grupos de rede. Isso permite que o ONTAP processe regras de política de exportação mais rapidamente do que recuperar as informações de fontes externas. Entender o que são os caches e o que eles fazem pode ajudá-lo a solucionar problemas de acesso ao cliente.

Você configura políticas de exportação para controlar o acesso do cliente às exportações NFS. Cada política de exportação contém regras e cada regra contém parâmetros que correspondem à regra aos clientes que solicitam acesso. Alguns desses parâmetros exigem que o ONTAP entre em Contato com uma fonte externa, como servidores DNS ou NIS, para resolver objetos como nomes de domínio, nomes de host ou netgroups.

Essas comunicações com fontes externas levam um pouco de tempo. Para aumentar o desempenho, o ONTAP reduz o tempo necessário para resolver objetos de regra de política de exportação armazenando informações localmente em cada nó em vários caches.

Nome do cache	Tipo de informação armazenada
Acesso	Mapeamentos de clientes para políticas de exportação correspondentes
Nome	Mapeamentos de nomes de usuário UNIX para IDs de usuário UNIX correspondentes
ID	Mapeamentos de IDs de usuário UNIX para IDs de usuário UNIX correspondentes e IDs de grupo UNIX estendidos
Host	Mapeamentos de nomes de host para endereços IP correspondentes

Nome do cache	Tipo de informação armazenada
Grupo de rede	Mapeamentos de netgroups para endereços IP correspondentes de membros
Showmount	Lista de diretórios exportados do namespace SVM

Se você alterar as informações nos servidores de nomes externos em seu ambiente depois que o ONTAP as recuperou e armazenou localmente, os caches agora podem conter informações desatualizadas. Embora o ONTAP atualize caches automaticamente após determinados períodos de tempo, os caches diferentes têm tempos e algoritmos diferentes de expiração e atualização.

Outro motivo possível para que os caches contenham informações desatualizadas é quando o ONTAP tenta atualizar informações em cache, mas encontra uma falha ao tentar se comunicar com servidores de nomes. Se isso acontecer, o ONTAP continuará a usar as informações atualmente armazenadas nos caches locais para evitar a interrupção do cliente.

Como resultado, as solicitações de acesso ao cliente que devem ser bem-sucedidas podem falhar e as solicitações de acesso ao cliente que devem falhar podem ser bem-sucedidas. Você pode exibir e lavar manualmente alguns dos caches de política de exportação ao solucionar problemas de acesso ao cliente.

Como o cache de acesso funciona

O ONTAP usa um cache de acesso para armazenar os resultados da avaliação de regras de política de exportação para operações de acesso do cliente para um volume ou qtree. Isso resulta em melhorias de desempenho porque as informações podem ser recuperadas muito mais rapidamente do cache de acesso do que passar pelo processo de avaliação de regras de política de exportação sempre que um cliente envia uma solicitação de e/S.

Sempre que um cliente NFS enviar uma solicitação de e/S para acessar dados em um volume ou qtree, o ONTAP deve avaliar cada solicitação de e/S para determinar se deve conceder ou negar a solicitação de e/S. Essa avaliação envolve verificar todas as regras de política de exportação da política de exportação associada ao volume ou qtree. Se o caminho para o volume ou qtree envolver cruzar um ou mais pontos de junção, isso pode exigir a realização desta verificação para várias políticas de exportação ao longo do caminho.

Observe que essa avaliação ocorre para cada solicitação de e/S enviada de um cliente NFS, como leitura, gravação, lista, cópia e outras operações, não apenas para solicitações de montagem inicial.

Depois que o ONTAP identificou as regras de política de exportação aplicáveis e decidiu se deseja permitir ou negar a solicitação, o ONTAP cria uma entrada no cache de acesso para armazenar essas informações.

Quando um cliente NFS envia uma solicitação de e/S, o ONTAP observa o endereço IP do cliente, a ID do SVM e a política de exportação associada ao volume ou qtree de destino e verifica primeiro a entrada correspondente no cache de acesso. Se existir uma entrada correspondente no cache de acesso, o ONTAP usará as informações armazenadas para permitir ou negar a solicitação de e/S. Se uma entrada correspondente não existir, o ONTAP passa pelo processo normal de avaliação de todas as regras de política aplicáveis, conforme explicado acima.

As entradas de cache de acesso que não são usadas ativamente não são atualizadas. Isso reduz a comunicação desnecessária e desperdiçada com o nome externo serve.

Recuperar as informações do cache de acesso é muito mais rápido do que passar por todo o processo de avaliação de regras de política de exportação para cada solicitação de e/S. Portanto, o uso do cache de acesso melhora significativamente o desempenho reduzindo a sobrecarga das verificações de acesso do cliente.

Como funcionam os parâmetros de cache de acesso

Vários parâmetros controlam os períodos de atualização para entradas no cache de acesso. Entender como esses parâmetros funcionam permite modificá-los para ajustar o cache de acesso e equilibrar o desempenho com o quão recente é a informação armazenada.

O cache de acesso armazena entradas que consistem em uma ou mais regras de exportação que se aplicam a clientes que tentam acessar volumes ou qtrees. Essas entradas são armazenadas por um determinado período de tempo antes de serem atualizadas. O tempo de atualização é determinado pelos parâmetros de cache de acesso e depende do tipo de entrada de cache de acesso.

Você pode especificar parâmetros de cache de acesso para SVMs individuais. Isso permite que os parâmetros sejam diferentes de acordo com os requisitos de acesso à SVM. As entradas de cache de acesso que não são usadas ativamente não são atualizadas, o que reduz a comunicação desnecessária e desperdiçada com servidores de nomes externos.

Acesse o tipo de entrada de cache	Descrição	Período de atualização em segundos
Entradas positivas	Acesse entradas de cache que não resultaram na negação de acesso aos clientes.	Mínimo: 300 Máximo: 86.400 Padrão: 3.600
Entradas negativas	Acesse entradas de cache que resultaram na negação de acesso aos clientes.	Mínimo: 60 Máximo: 86.400 Padrão: 3.600

Exemplo

Um cliente NFS tenta acessar um volume em um cluster. O ONTAP corresponde o cliente a uma regra de política de exportação e determina que o cliente obtém acesso com base na configuração da regra de política de exportação. O ONTAP armazena a regra de política de exportação no cache de acesso como uma entrada positiva. Por padrão, o ONTAP mantém a entrada positiva no cache de acesso por uma hora (3.600 segundos) e, em seguida, atualiza automaticamente a entrada para manter as informações atualizadas.

Para evitar que o cache de acesso seja preenchido desnecessariamente, há um parâmetro adicional para limpar entradas de cache de acesso existentes que não foram usadas por um determinado período de tempo para decidir o acesso do cliente. `-harvest-timeout`Este parâmetro tem um intervalo permitido de 60 a 2.592.000 segundos e uma predefinição de 86.400 segundos.

Remova uma política de exportação de uma qtree

Se você decidir que não deseja que uma política de exportação específica seja atribuída

a uma qtree por mais tempo, poderá remover a política de exportação modificando a qtree para herdar a política de exportação do volume que contém. Você pode fazer isso usando o `volume qtree modify` comando com o `-export-policy` parâmetro e uma string de nome vazia ("").

Passos

1. Para remover uma política de exportação de uma qtree, digite o seguinte comando:

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. Verifique se a qtree foi modificada em conformidade:

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

Valide as IDs de qtree para operações de arquivos de qtree

O ONTAP pode executar uma validação adicional opcional de IDs de qtree. Essa validação garante que as solicitações de operação de arquivo cliente usem um ID de qtree válido e que os clientes só possam mover arquivos dentro da mesma qtree. Pode ativar ou desativar esta validação modificando o `-validate-qtree-export` parâmetro. Este parâmetro está ativado por predefinição.

Sobre esta tarefa

Esse parâmetro só é efetivo quando você atribuiu uma política de exportação diretamente a um ou mais qtrees na máquina virtual de armazenamento (SVM).

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se pretender que a validação da ID de qtree seja…	Digite o seguinte comando…
Ativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
Desativado	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Restrições de política de exportação e junções aninhadas para volumes FlexVol

Se você configurou políticas de exportação para definir uma política menos restritiva em uma junção aninhada, mas uma política mais restritiva em uma junção de nível mais alto, o acesso à junção de nível inferior pode falhar.

Você deve garantir que as junções de nível mais alto tenham políticas de exportação menos restritivas do que as junções de nível mais baixo.

Usando Kerberos com NFS para segurança forte

Suporte ONTAP para Kerberos

O Kerberos fornece autenticação segura forte para aplicativos cliente/servidor. A autenticação fornece a verificação de identidades de usuário e processo para um servidor. No ambiente ONTAP, o Kerberos fornece autenticação entre máquinas virtuais de armazenamento (SVMs) e clientes NFS.

No ONTAP 9, a seguinte funcionalidade Kerberos é suportada:

- Autenticação Kerberos 5 com verificação de integridade (krb5i)

  O Krb5i usa checksums para verificar a integridade de cada mensagem NFS transferida entre cliente e servidor. Isso é útil tanto por motivos de segurança (por exemplo, para garantir que os dados não foram adulterados) quanto por motivos de integridade de dados (por exemplo, para evitar a corrupção de dados ao usar NFS em redes não confiáveis).

- Autenticação Kerberos 5 com verificação de privacidade (krb5p)

  Krb5p usa checksums para criptografar todo o tráfego entre o cliente e o servidor. Isto é mais seguro e também incorre mais carga.

- Criptografia AES de 128 bits e 256 bits

  O Advanced Encryption Standard (AES) é um algoritmo de encriptação para proteger dados eletrónicos. O ONTAP suporta AES com chaves de 128 bits (AES-128) e AES com criptografia de chaves de 256 bits (AES-256) para Kerberos para maior segurança.

- Configurações de realm Kerberos no nível da SVM

  Os administradores do SVM agora podem criar configurações do Kerberos Realm no nível SVM. Isso significa que os administradores do SVM não precisam mais confiar no administrador do cluster para a configuração do Kerberos Realm e podem criar configurações individuais do Kerberos Realm em um ambiente de alocação a vários clientes.

Requisitos para configurar Kerberos com NFS

Antes de configurar o Kerberos com NFS no sistema, você deve verificar se determinados itens no ambiente de rede e armazenamento estão configurados corretamente.

As etapas para configurar seu ambiente dependem de qual versão e tipo de sistema operacional cliente, controlador de domínio, Kerberos, DNS, etc. que você está usando. Documentar todas essas variáveis está além do escopo deste documento. Para obter mais informações, consulte a respetiva documentação para cada componente.

Para um exemplo detalhado de como configurar o ONTAP e o Kerberos 5 com NFSv3 e NFSv4 em um ambiente usando o ative Directory do Windows Server 2008 R2 e hosts Linux, consulte o relatório técnico 4073.

Os seguintes itens devem ser configurados primeiro:

Requisitos de ambiente de rede

- Kerberos

  Você deve ter uma configuração Kerberos funcionando com um centro de distribuição de chaves (KDC), como Kerberos baseados no ative Directory do Windows ou MIT Kerberos.

  Os servidores NFS devem usar `nfs` como o componente principal de sua máquina principal.

- Serviço de diretório

  Você deve usar um serviço de diretório seguro em seu ambiente, como ative Directory ou OpenLDAP, que esteja configurado para usar LDAP em SSL/TLS.

- NTP

  Você deve ter um servidor de tempo de trabalho executando NTP. Isso é necessário para evitar a falha de autenticação Kerberos devido ao desvio de tempo.

- Resolução de nome de domínio (DNS)

  Cada cliente UNIX e cada SVM LIF devem ter um Registro de serviço (SRV) adequado registrado no KDC em zonas de pesquisa direta e inversa. Todos os participantes devem ser solucionáveis corretamente via DNS.

- Contas de utilizador

  Cada cliente deve ter uma conta de usuário no Reino Kerberos. Os servidores NFS devem usar "nfs" como o componente principal de sua máquina principal.

Requisitos do cliente NFS

- NFS

  Cada cliente deve ser configurado corretamente para se comunicar através da rede usando NFSv3 ou NFSv4.

  Os clientes devem suportar RFC1964 e RFC2203.

- Kerberos

  Cada cliente deve ser configurado corretamente para usar a autenticação Kerberos, incluindo os seguintes detalhes:

- A encriptação para comunicação TGS está ativada.

  AES-256 para maior segurança.

- O tipo de encriptação mais seguro para comunicação TGT está ativado.
- O domínio e o domínio Kerberos estão configurados corretamente.
- O GSS está ativado.

  Ao usar credenciais de máquina:

- Não execute `gssd` com o `-n` parâmetro.
- Não execute `kinit` como usuário raiz.

- Cada cliente deve usar a versão mais recente e atualizada do sistema operacional.

  Isso fornece a melhor compatibilidade e confiabilidade para criptografia AES com Kerberos.

- DNS

  Cada cliente deve ser configurado corretamente para usar o DNS para a resolução correta do nome.

- NTP

  Cada cliente deve estar sincronizando com o servidor NTP.

- Informações de host e domínio

  Cada cliente `/etc/hosts` e `/etc/resolv.conf` arquivos devem conter o nome de host correto e as informações de DNS, respetivamente.

- Ficheiros keytab

  Cada cliente deve ter um arquivo keytab do KDC. O Reino deve estar em letras maiúsculas. O tipo de criptografia deve ser AES-256 para maior segurança.

- Opcional: Para obter o melhor desempenho, os clientes se beneficiam de ter pelo menos duas interfaces de rede: Uma para comunicação com a rede local e outra para comunicação com a rede de armazenamento.

Requisitos do sistema de storage

- Licença NFS

  O sistema de storage deve ter uma licença NFS válida instalada.

- Licença CIFS

  A licença CIFS é opcional. Só é necessário para verificar credenciais do Windows ao usar mapeamento de nomes multiprotocolo. Não é necessário em um ambiente restrito somente para UNIX.

- SVM

  Você precisa ter pelo menos um SVM configurado no sistema.

- DNS na SVM

  Você deve ter DNS configurado em cada SVM.

- Servidor NFS

  Você precisa ter o NFS configurado na SVM.

- Criptografia AES

  Para uma segurança mais forte, você deve configurar o servidor NFS para permitir apenas criptografia AES-256 para Kerberos.

- Servidor SMB

  Se você estiver executando um ambiente multiprotocolo, deverá ter o SMB configurado na SVM. O servidor SMB é necessário para o mapeamento de nomes multiprotocolo.

- Volumes

  Você precisa ter um volume raiz e pelo menos um volume de dados configurados para uso pelo SVM.

- Volume raiz

  O volume raiz do SVM precisa ter a seguinte configuração:

Nome	Definição
Estilo de segurança	UNIX
UID	Raiz ou ID 0
GID	Raiz ou ID 0
Permissões da UNIX	777

  Em contraste com o volume raiz, os volumes de dados podem ter um estilo de segurança.

- Grupos UNIX

  O SVM deve ter os seguintes grupos UNIX configurados:

Nome do grupo	ID do grupo
daemon	1
raiz	0
pcuser	65534 (criado automaticamente pelo ONTAP ao criar o SVM)

- Utilizadores UNIX

  O SVM deve ter os seguintes usuários UNIX configurados:

Nome de utilizador	ID de utilizador	ID do grupo principal	Comentário
nfs	500	0	Necessário para a fase INIT do GSS O primeiro componente do usuário cliente NFS SPN é usado como usuário.
pcuser	65534	65534	Necessário para uso multiprotocolo NFS e CIFS Criado e adicionado ao grupo pcuser automaticamente pelo ONTAP ao criar o SVM.
raiz	0	0	Necessário para a montagem

  O usuário nfs não é necessário se existir um mapeamento de nomes Kerberos-UNIX para o SPN do usuário cliente NFS.

- Políticas e regras de exportação

  Você deve ter configurado políticas de exportação com as regras de exportação necessárias para os volumes raiz e de dados e qtrees. Se todos os volumes da SVM forem acessados por Kerberos, você poderá definir as opções de regra de exportação `-rorule` , `-rwrule` e `-superuser` para o volume raiz como `krb5` , `krb5i` ou `krb5p`.

- Mapeamento de nomes Kerberos-UNIX

  Se você quiser que o usuário identificado pelo usuário cliente NFS SPN tenha permissões de raiz, você deve criar um mapeamento de nome para root.

Informações relacionadas

"Relatório técnico da NetApp 4073: Autenticação unificada segura"

"Ferramenta de Matriz de interoperabilidade do NetApp"

"Administração do sistema"

"Gerenciamento de storage lógico"

Especifique o domínio de ID de usuário para NFSv4

Para especificar o domínio de ID de usuário, você pode definir a `-v4-id-domain` opção.

Sobre esta tarefa

Por padrão, o ONTAP usa o domínio NIS para o mapeamento de ID de usuário NFSv4, se um estiver definido. Se um domínio NIS não estiver definido, o domínio DNS será usado. Talvez seja necessário definir o domínio de ID de usuário se, por exemplo, você tiver vários domínios de ID de usuário. O nome de domínio deve corresponder à configuração de domínio no controlador de domínio. Não é necessário para NFSv3.

Passo

1. Introduza o seguinte comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

Uso do TLS com NFS para uma segurança forte

Visão geral do uso do TLS com NFS para uma segurança forte

O TLS permite comunicações de rede criptografadas com segurança equivalente e menos complexidade do que o Kerberos e o IPsec. Como administrador, você pode habilitar, configurar e desabilitar o TLS para segurança forte com conexões NFSv3 e NFSv4.x usando o Gerenciador de sistema, a CLI do ONTAP ou a API REST do ONTAP.

> O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

O ONTAP usa o TLS 1,3 para conexões NFS em TLS.

Requisitos

O NFS em TLS requer certificados X,509. Você pode criar e instalar um certificado de servidor assinado pela CA no cluster do ONTAP ou instalar um certificado que o serviço NFS usa diretamente. Seus certificados devem atender às seguintes diretrizes:

- O nome comum (CN) de cada certificado deve ser configurado com o nome de domínio totalmente qualificado (FQDN) do LIF de dados no qual o TLS será ativado.
- O nome alternativo do assunto (SAN) de cada certificado deve ser configurado com o endereço IP do LIF de dados no qual o TLS será ativado. Opcionalmente, você também pode adicionar FQDN do LIF de dados. Se o endereço IP e o FQDN estiverem configurados, os clientes NFS podem se conetar usando o endereço IP ou o FQDN.
- Você pode instalar vários certificados de serviço NFS para o mesmo LIF, mas apenas um deles pode ser usado de cada vez como parte da configuração TLS NFS.

Ativar ou desativar TLS para clientes NFS no ONTAP

Você pode melhorar a segurança das conexões NFS configurando o NFS em TLS para criptografar todos os dados enviados pela rede entre o cliente NFS e o ONTAP. Isso aumenta a segurança das conexões NFS. Você pode configurar isso em uma VM de

storage existente habilitada para NFS.

O NFS em TLS está disponível no ONTAP 9.15,1 como prévia pública. Como oferta de prévia, o NFS em TLS não é compatível com workloads de produção no ONTAP 9.15,1.

Ativar TLS

Você pode habilitar a criptografia TLS para clientes NFS para aumentar a segurança dos dados em trânsito.

Antes de começar

- Consulte "requisitos"o para NFS sobre TLS antes de começar.
- Consulte as páginas do manual do ONTAP para obter mais informações sobre o comando neste procedimento.
- Saiba mais sobre `vserver nfs tls interface show` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) na qual ativar o TLS.
2. Habilite o TLS para conexões NFS nessa VM e interface de storage.

```
vserver nfs tls interface enable -vserver <STORAGE_VM> -lif <LIF_NAME>
-certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir habilita o NFS sobre TLS no `data1` LIF da `vs1` VM de storage:

```
vserver nfs tls interface enable -vserver vs1 -lif data1 -certificate-name
cert_vs1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        enabled    cert_vs1
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Desativar TLS

Você pode desativar o TLS para clientes NFS se não precisar mais da segurança aprimorada para dados em trânsito.

Antes de começar

Saiba mais sobre `vserver nfs tls interface disable` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de armazenamento e uma interface lógica (LIF) para desativar o TLS.
2. Desative TLS para conexões NFS nessa VM e interface de storage.

```
vserver nfs tls interface disable -vserver <STORAGE_VM> -lif <LIF_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir desativa NFS sobre TLS no `data1` LIF da `vs1` VM de armazenamento:

```
vserver nfs tls interface disable -vserver vs1 -lif data1
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        disabled   -
2 entries were displayed.
```

Editar uma configuração TLS

Você pode alterar as configurações de uma configuração NFS em TLS existente. Por exemplo, você pode usar este procedimento para atualizar o certificado TLS.

Antes de começar

Saiba mais sobre `vserver nfs tls interface modify` o "Referência do comando ONTAP"na .

Passos

1. Escolha uma VM de storage e uma interface lógica (LIF) para modificar a configuração TLS para clientes NFS.
2. Modificar a configuração. Se especificar um `status` de `enable`, também terá de especificar o `certificate-name` parâmetro. Substitua os valores entre parêntesis> por informações do seu ambiente:

```
vserver nfs tls interface modify -vserver <STORAGE_VM> -lif <LIF_NAME>
-status <STATUS> -certificate-name <CERTIFICATE_NAME>
```

3. Use o `vserver nfs tls interface show` comando para visualizar os resultados:

```
vserver nfs tls interface show
```

Exemplo

O comando a seguir modifica a configuração NFS sobre TLS no `data2` LIF da `vs2` VM de armazenamento:

```
vserver nfs tls interface modify -vserver vs2 -lif data2 -status enable
-certificate-name new_cert
```

```
vserver nfs tls interface show
```

```
               Logical
Vserver        Interface     Address         TLS Status TLS Certificate
Name
-------------- ------------- --------------- ----------
-----------------------
vs1            data1         10.0.1.1        disabled   -
vs2            data2         10.0.1.2        enabled    new_cert
2 entries were displayed.
```

Informações relacionadas

"Ative o storage nas para servidores Linux usando NFS".

Configurar serviços de nomes

Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para…	Fontes válidas são…
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem…	Para procurar informações em…	Gerenciado pelas famílias de comando…

ficheiros	Arquivos de origem local	`vserver services name-service unix-user vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	`vserver services name-service ldap`
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	`vserver services name-service dns`

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch do serviço de nomes para o SVM_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar endereços IP para hosts, o ONTAP primeiro consulta os arquivos de origem locais. Se a consulta não retornar nenhum resultado, os servidores DNS serão verificados em seguida.

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Utilize LDAP

Visão geral do LDAP

Um servidor LDAP (Lightweight Directory Access Protocol) permite manter centralmente as informações do usuário. Se você armazenar seu banco de dados de usuários em um servidor LDAP em seu ambiente, poderá configurar seu sistema de storage para procurar informações de usuário em seu banco de dados LDAP existente.

- Antes de configurar o LDAP para ONTAP, você deve verificar se a implantação do site atende às práticas recomendadas para configuração do servidor LDAP e do cliente. Em especial, devem ser satisfeitas as seguintes condições:
  - O nome de domínio do servidor LDAP deve corresponder à entrada no cliente LDAP.
  - Os tipos de hash de senha do usuário LDAP suportados pelo servidor LDAP devem incluir aqueles suportados pelo ONTAP:
    - CRYPT (todos os tipos) e SHA-1 (SHA, SSHA).
    - A partir do ONTAP 9.8, hashes SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, SSHA-384 e SSHA-512) também são suportados.
  - Se o servidor LDAP exigir medidas de segurança de sessão, você deve configurá-las no cliente LDAP.

    As seguintes opções de segurança de sessão estão disponíveis:

        - Assinatura LDAP (fornece verificação de integridade de dados) e assinatura e vedação LDAP (fornece verificação e criptografia de integridade de dados)
        - INICIE O TLS
        - LDAPS (LDAP sobre TLS ou SSL)
    - Para ativar consultas LDAP assinadas e seladas, os seguintes serviços devem ser configurados:
        - Os servidores LDAP devem suportar o mecanismo SASL GSSAPI (Kerberos).
        - Os servidores LDAP devem ter Registros DNS A/AAAA, bem como Registros PTR configurados no servidor DNS.
        - Os servidores Kerberos devem ter Registros SRV presentes no servidor DNS.
    - Para ativar o TLS ou LDAPS, os seguintes pontos devem ser considerados.
        - É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.
        - Se o LDAPS for usado, o servidor LDAP deve estar habilitado para TLS ou SSL no ONTAP 9.5 e posterior. O SSL não é suportado no ONTAP 9.0-9,4.
        - Um servidor de certificados já deve estar configurado no domínio.
    - Para ativar a perseguição de referência LDAP (no ONTAP 9.5 e posterior), as seguintes condições devem ser satisfeitas:
        - Ambos os domínios devem ser configurados com uma das seguintes relações de confiança:
            - Bidirecional
            - One-way, onde o primário confia no domínio de referência
            - Pai-filho
        - O DNS deve ser configurado para resolver todos os nomes de servidor referidos.
        - As senhas de domínio devem ser iguais para autenticar quando `--bind-as-cifs-server` definidas como verdadeiro.

        As configurações a seguir não são suportadas com a busca por referência LDAP.

        - Para todas as versões do ONTAP:
        - Clientes LDAP em um SVM admin
        - Para o ONTAP 9.8 e versões anteriores (eles são suportados em 9.9.1 e posteriores):
        - Assinatura e selagem LDAP (a `-session-security` opção)
        - Conexões TLS criptografadas (a `-use-start-tls` opção)
        - Comunicações através da porta LDAPS 636 (a `-use-ldaps-for-ad-ldap` opção)

- Começando com ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch."
- Você deve inserir um esquema LDAP ao configurar o cliente LDAP no SVM.

  Na maioria dos casos, um dos esquemas ONTAP padrão será apropriado. No entanto, se o esquema LDAP em seu ambiente for diferente desses, você deverá criar um novo esquema de cliente LDAP para o ONTAP antes de criar o cliente LDAP. Consulte o administrador LDAP sobre os requisitos para o seu ambiente.

- O uso do LDAP para resolução de nome de host não é suportado.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você deve configurar as configurações de segurança do servidor NFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`. teste

A assinatura LDAP e a vedação no tráfego SMB são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Conceitos LDAPS

Você deve entender certos termos e conceitos sobre como o ONTAP protege a comunicação LDAP. O ONTAP pode usar TLS ou LDAPS para configurar sessões autenticadas entre servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX.

Terminologia

Existem certos termos que você deve entender sobre como o ONTAP usa o LDAPS para proteger a comunicação LDAP.

- **LDAP**

  (Lightweight Directory Access Protocol) Um protocolo para acessar e gerenciar diretórios de informações. O LDAP é usado como um diretório de informações para armazenar objetos como usuários, grupos e grupos de rede. O LDAP também fornece serviços de diretório que gerenciam esses objetos e atendem solicitações LDAP de clientes LDAP.

- **SSL**

  (Secure Sockets Layer) Um protocolo desenvolvido para enviar informações de forma segura pela Internet. O SSL é suportado pelo ONTAP 9 e posterior, mas foi obsoleto em favor do TLS.

- **TLS**

  (Transport Layer Security) um protocolo de rastreamento de padrões IETF que é baseado nas especificações SSL anteriores. É o sucessor do SSL. O TLS é compatível com o ONTAP 9.5 e posterior.

- **LDAPS (LDAP sobre SSL ou TLS)**

  Um protocolo que usa TLS ou SSL para proteger a comunicação entre clientes LDAP e servidores LDAP. Os termos *LDAP sobre SSL* e *LDAP sobre TLS* às vezes são usados de forma intercambiável. O LDAPS é suportado pelo ONTAP 9.5 e posterior.

- No ONTAP 9.5-9,8, o LDAPS só pode ser ativado na porta 636. Para fazer isso, use o `-use-ldaps -for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.
- A partir do ONTAP 9.9,1, o LDAPS pode ser ativado em qualquer porta, embora a porta 636 permaneça a predefinição. Para fazer isso, defina o `-ldaps-enabled` parâmetro `true` e especifique o parâmetro desejado `-port`. Para obter mais informações, consulte a `vserver services name-service ldap client create` página de manual

É uma prática recomendada do NetApp usar Iniciar TLS em vez de LDAPS.

- * Iniciar TLS*

  (Também conhecido como *start_tls*, *STARTTLS* e *STARTTLS*) Um mecanismo para fornecer comunicação segura usando os protocolos TLS.

  O ONTAP usa o STARTTLS para proteger a comunicação LDAP e usa a porta LDAP padrão (389) para se comunicar com o servidor LDAP. O servidor LDAP deve ser configurado para permitir conexões pela porta LDAP 389; caso contrário, as conexões LDAP TLS do SVM ao servidor LDAP falharão.

Como o ONTAP usa o LDAPS

O ONTAP oferece suporte à autenticação de servidor TLS, o que permite que o cliente LDAP SVM confirme a identidade do servidor LDAP durante a operação de vinculação. Os clientes LDAP habilitados para TLS podem usar técnicas padrão de criptografia de chave pública para verificar se o certificado e a ID pública de um servidor são válidos e foram emitidos por uma autoridade de certificação (CA) listada na lista de CAs confiáveis do cliente.

O LDAP suporta STARTTLS para criptografar comunicações usando TLS. O STARTTLS começa como uma conexão de texto simples sobre a porta LDAP padrão (389), e essa conexão é então atualizada para TLS.

O ONTAP oferece suporte ao seguinte:

- LDAPS para tráfego relacionado a SMB entre os servidores LDAP integrados ao ative Directory e o SVM
- LDAPS para tráfego LDAP para mapeamento de nomes e outras informações do UNIX

  Servidores LDAP integrados ao ative Directory ou servidores LDAP baseados em UNIX podem ser usados para armazenar informações para mapeamento de nomes LDAP e outras informações do UNIX, como usuários, grupos e netgroups.

- Certificados CA raiz autoassinados

  Ao usar um LDAP integrado do ative-Directory, o certificado raiz autoassinado é gerado quando o Serviço de certificados do Windows Server é instalado no domínio. Ao usar um servidor LDAP baseado em UNIX para mapeamento de nomes LDAP, o certificado raiz autoassinado é gerado e salvo usando meios apropriados para esse aplicativo LDAP.

Por predefinição, o LDAPS está desativado.

Ative o suporte ao LDAP RFC2307bis

Se você quiser usar o LDAP e exigir a capacidade adicional de usar associações a grupos aninhados, você pode configurar o ONTAP para habilitar o suporte ao LDAP RFC2307bis.

O que você vai precisar

Você deve ter criado uma cópia de um dos esquemas de cliente LDAP padrão que você deseja usar.

Sobre esta tarefa

Em esquemas de cliente LDAP, os objetos de grupo usam o atributo memberUid. Esse atributo pode conter vários valores e lista os nomes dos usuários que pertencem a esse grupo. Em esquemas de cliente LDAP habilitados para RFC2307bis, os objetos de grupo usam o atributo uniqueMember. Este atributo pode conter o nome distinto completo (DN) de outro objeto no diretório LDAP. Isso permite que você use grupos aninhados porque os grupos podem ter outros grupos como membros.

O usuário não deve ser membro de mais de 256 grupos, incluindo grupos aninhados. O ONTAP ignora quaisquer grupos acima do limite de 256 grupos.

Por padrão, o suporte a RFC2307bis está desativado.

> O suporte a RFC2307bis é ativado automaticamente no ONTAP quando um cliente LDAP é criado com o esquema MS-AD-BIS.

Para obter informações adicionais, "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"consulte .

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Modifique o esquema de cliente LDAP RFC2307 copiado para ativar o suporte RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique o esquema para corresponder à classe de objeto suportada no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique o esquema para corresponder ao nome de atributo suportado no servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Opções de configuração para pesquisas de diretório LDAP

Você pode otimizar as pesquisas de diretório LDAP, incluindo informações de usuário, grupo e netgroup, configurando o cliente LDAP do ONTAP para se conetar a servidores LDAP da maneira mais apropriada para o seu ambiente. Você precisa entender quando os valores padrão de pesquisa base LDAP e escopo são suficientes e quais parâmetros

especificar quando os valores personalizados são mais apropriados.

As opções de pesquisa de cliente LDAP para informações de usuário, grupo e netgroup podem ajudar a evitar consultas LDAP com falha e, portanto, falha no acesso de cliente aos sistemas de armazenamento. Eles também ajudam a garantir que as pesquisas sejam o mais eficientes possível para evitar problemas de desempenho do cliente.

Valores de pesquisa padrão base e escopo

A base LDAP é o DN base padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o DN base. Essa opção é apropriada quando o diretório LDAP é relativamente pequeno e todas as entradas relevantes estão localizadas no mesmo DN.

Se você não especificar um DN base personalizado, o padrão será `root`. Isso significa que cada consulta pesquisa o diretório inteiro. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

O escopo base LDAP é o escopo de pesquisa padrão que o cliente LDAP usa para executar consultas LDAP. Todas as pesquisas, incluindo pesquisas de usuário, grupo e netgroup, são feitas usando o escopo base. Ele determina se a consulta LDAP pesquisa somente a entrada nomeada, as entradas um nível abaixo do DN ou toda a subárvore abaixo do DN.

Se você não especificar um escopo base personalizado, o padrão será `subtree`. Isso significa que cada consulta pesquisa a subárvore inteira abaixo do DN. Embora isso maximize as chances de sucesso da consulta LDAP, ela pode ser ineficiente e resultar em desempenho significativamente menor com grandes diretórios LDAP.

Valores de pesquisa de base e escopo personalizados

Opcionalmente, você pode especificar valores de base e escopo separados para pesquisas de usuário, grupo e netgroup. Limitar a base de pesquisa e o escopo das consultas dessa forma pode melhorar significativamente o desempenho, pois limita a pesquisa a uma subseção menor do diretório LDAP.

Se você especificar valores de base e escopo personalizados, eles substituirão a base de pesquisa padrão geral e o escopo para pesquisas de usuário, grupo e netgroup. Os parâmetros para especificar valores de base e escopo personalizados estão disponíveis no nível de privilégio avançado.

Parâmetro cliente LDAP…	Especifica personalizado…
`-base-dn`	DN base para todas as pesquisas LDAP os valores múltiplos podem ser inseridos se necessário (por exemplo, se a busca por referência LDAP estiver ativada no ONTAP 9.5 e versões posteriores).
`-base-scope`	Escopo base para todas as pesquisas LDAP
`-user-dn`	DNS base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.
`-user-scope`	Escopo base para todas as pesquisas de usuário LDAP este parâmetro também se aplica a pesquisas de mapeamento de nome de usuário.

`-group-dn`	DNS base para todas as pesquisas de grupo LDAP
`-group-scope`	Escopo base para todas as pesquisas de grupo LDAP
`-netgroup-dn`	DNS base para todas as pesquisas de netgroup LDAP
`-netgroup-scope`	Escopo base para todas as pesquisas de netgroup LDAP

Vários valores DN base personalizados

Se a estrutura de diretórios LDAP for mais complexa, poderá ser necessário especificar vários DNS base para procurar determinadas informações em várias partes do diretório LDAP. Você pode especificar vários DNS para os parâmetros DN de usuário, grupo e netgroup separando-os com um ponto e vírgula (;) e anexando toda a lista de pesquisa DN com aspas duplas ("). Se um DN contiver um ponto-e-vírgula, você deve adicionar um caractere de escape imediatamente antes do ponto-e-vírgula no DN.

Observe que o escopo se aplica a toda a lista de DNS especificada para o parâmetro correspondente. Por exemplo, se você especificar uma lista de três DNS de usuário e subárvore diferentes para o escopo do usuário, o usuário LDAP pesquisará toda a subárvore para cada um dos três DNS especificados.

A partir do ONTAP 9.5, você também pode especificar LDAP *referral chasing*, o que permite que o cliente LDAP ONTAP consulte solicitações de pesquisa para outros servidores LDAP se uma resposta de referência LDAP não for retornada pelo servidor LDAP primário. O cliente usa esses dados de referência para recuperar o objeto de destino do servidor descrito nos dados de referência. Para procurar objetos presentes nos servidores LDAP referidos, o base-DN dos objetos referidos pode ser adicionado ao base-DN como parte da configuração do cliente LDAP. No entanto, os objetos referidos só são procurados quando a busca por referência está ativada (usando a `-referral-enabled true` opção) durante a criação ou modificação do cliente LDAP.

Melhore o desempenho das pesquisas de diretório LDAP netgroup-by-host

Se o seu ambiente LDAP estiver configurado para permitir pesquisas netgroup-by-host, você poderá configurar o ONTAP para aproveitar isso e realizar pesquisas netgroup-by-host. Isso pode acelerar significativamente as pesquisas do netgroup e reduzir possíveis problemas de acesso ao cliente NFS devido à latência durante as pesquisas do netgroup.

O que você vai precisar

Seu diretório LDAP deve conter um `netgroup.byhost` mapa.

Seus servidores DNS devem conter Registros de pesquisa direta (A) e reversa (PTR) para clientes NFS.

Quando você especifica endereços IPv6 em netgroups, você deve sempre encurtar e compactar cada endereço conforme especificado no RFC 5952.

Sobre esta tarefa

Os servidores NIS armazenam informações do netgroup em três mapas separados chamados `netgroup` `netgroup.byuser` , e `netgroup.byhost`. O objetivo dos `netgroup.byuser` mapas e `netgroup.byhost` é acelerar as pesquisas de netgroup. O ONTAP pode realizar pesquisas netgroup-by-host

em servidores NIS para melhorar os tempos de resposta de montagem.

Por padrão, os diretórios LDAP não têm um `netgroup.byhost` mapa como os servidores NIS. No entanto, é possível, com a ajuda de ferramentas de terceiros, importar um mapa NIS `netgroup.byhost` para diretórios LDAP para permitir pesquisas rápidas netgroup-by-host. Se você tiver configurado seu ambiente LDAP para permitir pesquisas netgroup-by-host, poderá configurar o cliente LDAP do ONTAP com o `netgroup.byhost` nome do mapa, DN e o escopo de pesquisa para pesquisas mais rápidas netgroup-by-host.

Receber os resultados das pesquisas netgroup-by-host com mais rapidez permite que o ONTAP processe regras de exportação com mais rapidez quando os clientes NFS solicitam acesso às exportações. Isso reduz a chance de atraso no acesso devido a problemas de latência de pesquisa do netgroup.

Passos

1. Obtenha o nome distinto completo exato do mapa NIS `netgroup.byhost` importado para o diretório LDAP.

   O DN do mapa pode variar dependendo da ferramenta de terceiros usada para importação. Para obter o melhor desempenho, você deve especificar o DN exato do mapa.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Ative as pesquisas netgroup-by-host na configuração de cliente LDAP da máquina virtual de armazenamento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false`Ativar ou desativar a pesquisa netgroup-by-host para diretórios LDAP. A predefinição é `false`.

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` Especifica o nome distinto do `netgroup.byhost` mapa no diretório LDAP. Ele substitui o DN base para pesquisas netgroup-by-host. Se você não especificar esse parâmetro, o ONTAP usará o DN base.

   `-netgroup-byhost-scope {base|onelevel subtree`especifica o escopo de pesquisa para pesquisas netgroup-by-host. Se não especificar este parâmetro, a predefinição é `subtree`.

   Se a configuração do cliente LDAP ainda não existir, você pode habilitar pesquisas netgroup-by-host especificando esses parâmetros ao criar uma nova configuração de cliente LDAP usando o `vserver services name-service ldap client create` comando.

   > ⓘ A partir de ONTAP 9.2, o campo `-ldap-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor LDAP.

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O comando a seguir modifica a configuração de cliente LDAP existente chamada "ldap_corp" para habilitar pesquisas netgroup-by-host usando o mapa chamado netgroup `netgroup.byhost`.byhost", dc `subtree`

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Depois de terminar

Os `netgroup.byhost` mapas e `netgroup` no diretório devem ser mantidos sempre sincronizados para evitar problemas de acesso do cliente.

Informações relacionadas

"IETF RFC 5952: Uma recomendação para representação de texto de endereço IPv6"

Use LDAP fast bind para autenticação nsswitch

A partir do ONTAP 9.11,1, você pode aproveitar a funcionalidade LDAP *fast bind* (também conhecida como *concurrent bind*) para solicitações de autenticação de cliente mais rápidas e simples. Para utilizar esta funcionalidade, o servidor LDAP tem de suportar a funcionalidade de ligação rápida.

Sobre esta tarefa

Sem vinculação rápida, o ONTAP usa o LDAP Simple BIND para autenticar usuários administrativos com o servidor LDAP. Com esse método de autenticação, o ONTAP envia um nome de usuário ou grupo para o servidor LDAP, recebe a senha de hash armazenada e compara o código de hash do servidor com o código de hash gerado localmente a partir da senha do usuário. Se forem idênticos, o ONTAP concede permissão de login.

Com a funcionalidade de vinculação rápida, o ONTAP envia apenas credenciais de usuário (nome de usuário e senha) para o servidor LDAP por meio de uma conexão segura. Em seguida, o servidor LDAP valida essas credenciais e instrui o ONTAP a conceder permissões de login.

Uma vantagem do fast bind é que não há necessidade de o ONTAP suportar cada novo algoritmo de hash suportado por servidores LDAP, porque o hash de senha é executado pelo servidor LDAP.

"Saiba mais sobre como usar o fast bind."

Você pode usar configurações de cliente LDAP existentes para o LDAP fast bind. No entanto, é altamente recomendável que o cliente LDAP seja configurado para TLS ou LDAPS; caso contrário, a senha é enviada por fio em texto simples.

Para ativar o LDAP fast bind em um ambiente ONTAP, você precisa atender a estes requisitos:

- Os usuários de administração do ONTAP devem ser configurados em um servidor LDAP que suporte a vinculação rápida.
- O SVM do ONTAP deve ser configurado para LDAP no banco de dados de switch de serviços de nome (nsswitch).
- As contas de usuário e grupo de administrador do ONTAP devem ser configuradas para autenticação nsswitch usando vinculação rápida.

Passos

1. Confirme com o administrador LDAP que o LDAP FAST BIND é suportado no servidor LDAP.

2. Certifique-se de que as credenciais de utilizador admin do ONTAP estão configuradas no servidor LDAP.
3. Verifique se o administrador ou SVM de dados está configurado corretamente para o LDAP fast bind.

   a. Para confirmar se o servidor LDAP FAST BIND está listado na configuração do cliente LDAP, introduza:

      `vserver services name-service ldap client show`

      "Saiba mais sobre a configuração do cliente LDAP."

   b. Para confirmar `ldap` que é uma das fontes configuradas para o banco de dados nsswitch `passwd`, digite:

      `vserver services name-service ns-switch show`

   "Saiba mais sobre a configuração do nsswitch."

4. Certifique-se de que os usuários de administração estejam autenticando com o nsswitch e que a autenticação LDAP de vinculação rápida esteja habilitada em suas contas.

   ◦ Para usuários existentes, insira `security login modify` e verifique as seguintes configurações de parâmetro:

      `-authentication-method nsswitch`

`-is-ldap-fastbind true`

   ◦ Para novos utilizadores de administração, consulte "Ative o acesso a contas LDAP ou NIS."

Apresentar estatísticas LDAP

A partir do ONTAP 9.2, você pode exibir estatísticas LDAP para máquinas virtuais de armazenamento (SVMs) em um sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

O que você vai precisar

- Você deve ter configurado um cliente LDAP no SVM.
- Você deve ter objetos LDAP identificados a partir dos quais você pode exibir dados.

Passo

1. Veja os dados de desempenho para objetos de contador:

   `statistics show`

Exemplos

O exemplo a seguir exibe estatísticas para a amostra chamada **smpl_1** para contadores: avg_processor_busy e CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades SMB para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades SMB. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conetando a partir de um cliente NFS ou de um cliente SMB.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso SMB ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

  Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um

mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

  Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

  Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário SMB padrão não estiver configurado e o ONTAP não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

  Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ative Directory com o domínio home do servidor SMB podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor SMB no SVM.

- *Confiança bidirecional*

  Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor SMB tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

  Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

  Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*

  Com uma confiança de entrada, o outro domínio confia no domínio home do servidor SMB. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

  Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	o administrador do servidor não está habilitado a usar a barra de ferramentas	O usuário UNIX "'root'" é mapeado para o usuário chamado "'administrador'". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.
*	clique no botão "ok"	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado.  O asterisco é válido apenas para o mapeamento de nomes de UNIX para Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de carateres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula `" "` (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Configure o usuário UNIX padrão	`vserver cifs options modify -default-unix-user user_name`
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user user_name`

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`
Troque a posição de dois mapeamentos de nomes NOTA: Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`
Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Ative o acesso para clientes Windows NFS

O ONTAP suporta acesso a arquivos de clientes Windows NFSv3. Isso significa que os clientes que executam sistemas operacionais Windows com suporte a NFSv3 podem

acessar arquivos em exportações NFSv3 no cluster. Para usar essa funcionalidade com êxito, você deve configurar corretamente a máquina virtual de storage (SVM) e estar ciente de certos requisitos e limitações.

Sobre esta tarefa

Por padrão, o suporte ao cliente do Windows NFSv3 está desativado.

Antes de começar

O NFSv3 precisa estar habilitado no SVM.

Passos

1. Ativar o suporte ao cliente do Windows NFSv3:

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly
   disabled
   ```

2. Em todos os SVMs que suportam clientes Windows NFSv3, desative os `-enable-ejukebox` parâmetros e `-v3-connection-drop`:

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection
   -drop disabled
   ```

   Os clientes do Windows NFSv3 agora podem montar exportações no sistema de armazenamento.

3. Certifique-se de que cada cliente do Windows NFSv3 utiliza suportes rígidos especificando a `-o mtype=hard` opção.

   Isso é necessário para garantir montagens confiáveis.

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

Ative a exibição de exportações NFS em clientes NFS

Os clientes NFS podem usar o `showmount -e` comando para ver uma lista de exportações disponíveis a partir de um servidor ONTAP NFS. Isso pode ajudar os usuários a identificar o sistema de arquivos que eles querem montar.

A partir do ONTAP 9.2, o ONTAP permite que os clientes NFS visualizem a lista de exportação por padrão. Em versões anteriores, a `showmount` opção `vserver nfs modify` do comando deve ser ativada explicitamente. Para visualizar a lista de exportação, o NFSv3 deve estar habilitado no SVM.

Exemplo

O comando a seguir mostra o recurso showmount no SVM chamado VS1:

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

O comando a seguir executado em um cliente NFS exibe a lista de exportações em um servidor NFS com o endereço IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

Gerenciar o acesso a arquivos usando NFS

Ativar ou desativar NFSv3

Pode ativar ou desativar o NFSv3 modificando a `-v3` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv3. Por padrão, NFSv3 está ativado.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
Desativar NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

Ativar ou desativar NFSv4,0

Pode ativar ou desativar o NFSv4,0 modificando a `-v4.0` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,0. No ONTAP 9.9,1, o NFSv4,0 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	**Digite o seguinte comando…**
Ativar NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
Desativar NFSv4,0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

Ativar ou desativar NFSv4,1

Pode ativar ou desativar o NFSv4,1 modificando a `-v4.1` opção. Isto permite o acesso a ficheiros para clientes que utilizam o protocolo NFSv4,1. No ONTAP 9.9,1, o NFSv4,1 é ativado por padrão; em versões anteriores, ele é desativado por padrão.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
Desativar NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

Gerenciar NFSv4 limites de storepool

A partir do ONTAP 9.13, os administradores podem habilitar seus servidores NFSv4 para negar recursos a clientes NFSv4 quando eles tiverem atingido os limites de recursos do storepool de clientes. Quando os clientes consomem muitos recursos do storepool de NFSv4 isso pode levar a outros clientes NFSv4 serem bloqueados devido à indisponibilidade de recursos do storepool de NFSv4.

Ativar esse recurso também permite que os clientes visualizem o consumo de recursos do storepool ativo por cada cliente. Isso facilita a identificação de clientes que esgotam os recursos do sistema e possibilita impor limites de recursos por cliente.

Veja os recursos do storepool consumidos

O `vserver nfs storepool show` comando mostra o número de recursos do storepool consumidos. Um storepool é um pool de recursos usado por clientes NFSv4.

Passo

1. Como administrador, execute o `vserver nfs storepool show` comando para exibir as informações do storepool de clientes NFSv4.

Exemplo

Este exemplo exibe as informações do storepool de clientes NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

Ative ou desative os controles de limite do storepool

Os administradores podem usar os seguintes comandos para ativar ou desativar os controles de limite do storepool.

Passo

1. Como administrador, execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce enabled`
Desative os controles de limite do storepool	`vserver nfs storepool config modify -limit-enforce disabled`

Exibir uma lista de clientes bloqueados

Se o limite storepool estiver ativado, os administradores poderão ver quais clientes foram bloqueados ao atingir o limite de recursos por cliente. Os administradores podem usar o seguinte comando para ver quais clientes foram marcados como clientes bloqueados.

Passos

1. Use o `vserver nfs storepool blocked-client show` comando para exibir a lista de clientes bloqueados do NFSv4.

Remova um cliente da lista de clientes bloqueados

Os clientes que atingirem seu limite por cliente serão desconetados e adicionados ao cache block-client. Os administradores podem usar o seguinte comando para remover o cliente do cache de cliente de bloco. Isso permitirá que o cliente se conete ao servidor ONTAP NFSv4.

Passos

1. Use o `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando para lavar o cache de cliente bloqueado storepool.
2. Use o `vserver nfs storepool blocked-client show` comando para verificar se o cliente foi removido do cache de cliente de bloco.

Exemplo

Este exemplo exibe um cliente bloqueado com o endereço IP "10,2.1,1" sendo lavado de todos os nós.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

Ative ou desative o pNFS

O pNFS melhora o desempenho permitindo que os clientes NFS executem operações de leitura/gravação em dispositivos de storage diretamente e em paralelo, ignorando o servidor NFS como um potencial gargalo. Para ativar ou desativar pNFS (NFS paralelo), pode modificar a `-v4.1-pnfs` opção.

Se a versão ONTAP for…	O padrão pNFS é…
9,8 ou posterior	desativado
9,7 ou anterior	ativado

O que você vai precisar

O suporte NFSv4,1 é necessário para poder usar o pNFS.

Se você quiser ativar o pNFS, primeiro você deve desativar as referências NFS. Ambos não podem ser ativados ao mesmo tempo.

Se você usar pNFS com Kerberos em SVMs, você deverá habilitar o Kerberos em cada LIF na SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
Desativar pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

Informações relacionadas

- Visão geral do trunking NFS

Controle o acesso NFS por TCP e UDP

Você pode ativar ou desativar o acesso NFS a máquinas virtuais de armazenamento (SVMs) em TCP e UDP, modificando os `-tcp` parâmetros e `-udp`, respetivamente. Isso permite que você controle se os clientes NFS podem acessar dados via TCP ou UDP em seu ambiente.

Sobre esta tarefa

Estes parâmetros aplicam-se apenas ao NFS. Não afetam protocolos auxiliares. Por exemplo, se o NFS sobre TCP estiver desativado, as operações de montagem sobre TCP ainda terão êxito. Para bloquear completamente o tráfego TCP ou UDP, você pode usar regras de política de exportação.

> Você deve desativar o SnapDiff RPC Server antes de desativar o TCP para NFS para evitar um erro de falha de comando. Você pode desativar o TCP usando o comando `vserver snapdiff-rpc-server off -vserver vserver name`.

Passo

1. Execute uma das seguintes ações:

Se você quiser que o acesso NFS seja…	Digite o comando…
Ativado em TCP	`vserver nfs modify -vserver vserver_name -tcp enabled`
Desativado por TCP	`vserver nfs modify -vserver vserver_name -tcp disabled`
Ativado em UDP	`vserver nfs modify -vserver vserver_name -udp enabled`
Desativado por UDP	`vserver nfs modify -vserver vserver_name -udp disabled`

Controle solicitações NFS de portas não reservadas

Você pode rejeitar solicitações de montagem NFS de portas não reservadas habilitando

a `-mount-rootonly` opção. Para rejeitar todas as solicitações NFS de portas não reservadas, você pode ativar a `-nfs-rootonly` opção.

Sobre esta tarefa

Por padrão, a opção `-mount-rootonly` é `enabled`.

Por padrão, a opção `-nfs-rootonly` é `disabled`.

Estas opções não se aplicam ao procedimento NULL.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Permitir solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
Rejeitar solicitações de montagem NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
Permitir todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
Rejeitar todas as solicitações NFS de portas não reservadas	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

Lidar com o acesso NFS a volumes NTFS ou qtrees para usuários UNIX desconhecidos

Se o ONTAP não conseguir identificar usuários UNIX tentando se conetar a volumes ou qtrees com estilo de segurança NTFS, ele não poderá mapear explicitamente o usuário para um usuário do Windows. Você pode configurar o ONTAP para negar acesso a esses usuários para segurança mais rigorosa ou mapeá-los para um usuário padrão do Windows para garantir um nível mínimo de acesso para todos os usuários.

O que você vai precisar

Um usuário padrão do Windows deve ser configurado se você quiser habilitar essa opção.

Sobre esta tarefa

Se um usuário UNIX tentar acessar volumes ou qtrees com estilo de segurança NTFS, o usuário UNIX deve primeiro ser mapeado para um usuário do Windows para que o ONTAP possa avaliar adequadamente as permissões NTFS. No entanto, se o ONTAP não conseguir procurar o nome do usuário UNIX nas fontes de serviço de nome de informações de usuário configuradas, ele não poderá mapear explicitamente o usuário UNIX para um usuário específico do Windows. Você pode decidir como lidar com esses usuários UNIX desconhecidos das seguintes maneiras:

- Negar acesso a usuários UNIX desconhecidos.

  Isso impõe segurança mais rigorosa, exigindo mapeamento explícito para todos os usuários UNIX para

obter acesso a volumes NTFS ou qtrees.

- Mapeie usuários UNIX desconhecidos para um usuário padrão do Windows.

  Isso fornece menos segurança, mas mais conveniência, garantindo que todos os usuários obtenham um nível mínimo de acesso a volumes NTFS ou qtrees por meio de um usuário padrão do Windows.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser o usuário padrão do Windows para usuários UNIX desconhecidos…	Digite o comando…
Ativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
Desativado	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Considerações para clientes que montam exportações NFS usando uma porta não reservada

A `-mount-rootonly` opção deve ser desativada em um sistema de armazenamento que deve suportar clientes que montam exportações NFS usando uma porta não reservada mesmo quando o usuário está conetado como raiz. Tais clientes incluem clientes Hummingbird e clientes Solaris NFS/IPv6.

Se a `-mount-rootonly` opção estiver ativada, o ONTAP não permitirá que clientes NFS que usam portas não reservadas, ou seja, portas com números superiores a 1.023, montem exportações NFS.

Execute uma verificação de acesso mais rigorosa para netgroups verificando domínios

Por padrão, o ONTAP executa uma verificação adicional ao avaliar o acesso do cliente para um netgroup. A verificação adicional garante que o domínio do cliente corresponda à configuração do domínio da máquina virtual de armazenamento (SVM). Caso contrário, o ONTAP nega acesso ao cliente.

Sobre esta tarefa

Quando o ONTAP avalia regras de política de exportação para acesso de cliente e uma regra de política de exportação contém um netgroup, o ONTAP deve determinar se o endereço IP de um cliente pertence ao netgroup. Para isso, o ONTAP converte o endereço IP do cliente para um nome de host usando DNS e obtém um nome de domínio totalmente qualificado (FQDN).

Se o arquivo netgroup apenas listar um nome curto para o host e o nome curto para o host existir em vários domínios, é possível que um cliente de um domínio diferente obtenha acesso sem essa verificação.

Para evitar isso, o ONTAP compara o domínio retornado do DNS para o host com a lista de nomes de domínio DNS configurados para o SVM. Se corresponder, o acesso é permitido. Se não corresponder, o acesso é negado.

Esta verificação está ativada por predefinição. Você pode gerenciá-lo modificando o `-netgroup-dns -domain-search` parâmetro, que está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você deseja que a verificação de domínio para netgroups seja…	Digite…
Ativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
Desativado	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. Defina o nível de privilégio como admin:

   ```
   set -privilege admin
   ```

Modifique as portas usadas para serviços NFSv3

O servidor NFS no sistema de armazenamento usa serviços como o daemon de montagem e o Gerenciador de bloqueio de rede para se comunicar com clientes NFS através de portas de rede padrão específicas. Na maioria dos ambientes NFS, as portas padrão funcionam corretamente e não exigem modificação, mas se você quiser usar diferentes portas de rede NFS em seu ambiente NFSv3, você pode fazer isso.

O que você vai precisar

A alteração das portas NFS no sistema de storage exige que todos os clientes NFS se reconetem ao sistema. Portanto, você deve comunicar essas informações aos usuários antes de fazer a alteração.

Sobre esta tarefa

Você pode definir as portas usadas pelos serviços de daemon de montagem NFS, Network Lock Manager, Network Status Monitor e NFS quota daemon para cada máquina virtual de armazenamento (SVM). A alteração do número da porta afeta os clientes NFS que acessam dados por TCP e UDP.

As portas para NFSv4 e NFSv4,1 não podem ser alteradas.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Desativar o acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access false
   ```

3. Defina a porta NFS para o serviço NFS específico:

   ```
   vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
   ```

Parâmetro da porta NFS	Descrição	Porta predefinida
`-mountd-port`	Daemon de montagem NFS	635
`-nlm-port`	Gerenciador de bloqueio de rede	4045
`-nsm-port`	Monitor de estado da rede	4046
`-rquotad-port`	Daemon de cota NFS	4049

   Além da porta padrão, o intervalo permitido de números de porta é de 1024 a 65535. Cada serviço NFS precisa usar uma porta única.

4. Ativar acesso ao NFS:

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. Use o `network connections listening show` comando para verificar as alterações no número da porta.
6. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

Os comandos a seguir definem a porta NFS Mount Daemon como 1113 no SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

Comandos para gerenciar servidores NFS

Existem comandos ONTAP específicos para gerenciar servidores NFS.

Se você quiser…	Use este comando…
Crie um servidor NFS	`vserver nfs create`
Exibir servidores NFS	`vserver nfs show`
Modificar um servidor NFS	`vserver nfs modify`
Excluir um servidor NFS	`vserver nfs delete`

Oculte a `.snapshot` lista de diretórios em NFSv3 pontos de montagem O acesso explícito ao `.snapshot` diretório ainda será permitido mesmo que a opção esteja ativada.	`vserver nfs` comandos com a `-v3-hide-snapshot` opção ativada

Consulte a página de manual de cada comando para obter mais informações.

Solucionar problemas do serviço de nomes

Quando os clientes experimentam falhas de acesso devido a problemas de serviço de nome, você pode usar a `vserver services name-service getxxbyyy` família de comandos para executar manualmente várias pesquisas de serviço de nome e examinar os detalhes e resultados da pesquisa para ajudar na solução de problemas.

Sobre esta tarefa

- Para cada comando, você pode especificar o seguinte:
  - Nome do nó ou da máquina virtual de storage (SVM) para realizar a pesquisa.

    Isso permite testar pesquisas de serviços de nomes para um nó específico ou SVM para restringir a pesquisa de um possível problema de configuração de serviço de nomes.
  - Se deve mostrar a fonte usada para a pesquisa.

    Isso permite verificar se a fonte correta foi usada.
- O ONTAP seleciona o serviço para realizar a pesquisa com base na ordem configurada do switch do serviço de nomes.
- Esses comandos estão disponíveis no nível avançado de privilégio.

Passos

1. Execute uma das seguintes ações:

Para recuperar…	Use o comando…
Endereço IP de um nome de host	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (Apenas endereços IPv4)
Membros de um grupo por ID de grupo	`vserver services name-service getxxbyyy getgrbygid`

Membros de um grupo por nome de grupo	`vserver services name-service getxxbyyy getgrbyname`
Lista de grupos aos quais um usuário pertence	`vserver services name-service getxxbyyy getgrlist`
Nome do host de um endereço IP	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (Apenas endereços IPv4)
Informações do usuário por nome de usuário	`vserver services name-service getxxbyyy getpwbyname` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
Informações do usuário por ID do usuário	`vserver services name-service getxxbyyy getpwbyuid` É possível testar a resolução de nomes de usuários do RBAC especificando o `-use-rbac` parâmetro como `true`.
A associação netgroup de um cliente	`vserver services name-service getxxbyyy netgrp`
A associação netgroup de um cliente usando a pesquisa netgroup-by-host	`vserver services name-service getxxbyyy netgrpbyhost`

O exemplo a seguir mostra um teste de pesquisa de DNS para o SVM VS1 ao tentar obter o endereço IP do host acast1.eng.example.com:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

O exemplo a seguir mostra um teste de pesquisa NIS para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

O exemplo a seguir mostra um teste de pesquisa LDAP para o SVM VS1 ao tentar recuperar informações de usuário para um usuário com o nome ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

O exemplo a seguir mostra um teste de pesquisa de netgroup para o SVM VS1 ao tentar descobrir se o cliente dnshost0 é membro do netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analise os resultados do teste realizado e tome a ação necessária.

Se o…	Veja o…
A pesquisa de nome de host ou endereço IP falhou ou gerou resultados incorretos	Configuração DNS
A pesquisa consultou uma fonte incorreta	Configuração do switch do serviço de nomes

Se o…	Veja o…
A pesquisa de usuário ou grupo falhou ou produziu resultados incorretos	• Configuração do switch do serviço de nomes • Configuração de origem (arquivos locais, domínio NIS, cliente LDAP) • Configuração de rede (por exemplo, LIFs e rotas)
A pesquisa de nomes de host falhou ou expirou, e o servidor DNS não resolve nomes curtos de DNS (por exemplo, host1)	Configuração de DNS para consultas de domínio de topo (TLD). Você pode desabilitar consultas TLD usando a `-is-tld-query-enabled false` opção para o `vserver services name-service dns modify` comando.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Verifique as conexões do serviço de nomes

A partir do ONTAP 9.2, pode verificar os servidores de nomes DNS e LDAP para verificar se estão ligados ao ONTAP. Esses comandos estão disponíveis no nível de privilégios de administrador.

Sobre esta tarefa

Você pode verificar se há uma configuração válida do serviço de nomes DNS ou LDAP conforme necessário usando o verificador de configuração do serviço de nomes. Esta verificação de validação pode ser iniciada na linha de comando ou no System Manager.

Para configurações de DNS, todos os servidores são testados e precisam estar funcionando para que a configuração seja considerada válida. Para configurações LDAP, desde que qualquer servidor esteja ativo, a configuração é válida. Os comandos do serviço de nomes aplicam o verificador de configuração a menos que o `skip-config-validation` campo seja verdadeiro (o padrão é falso).

Passo

1. Use o comando apropriado para verificar uma configuração do serviço de nomes. A IU exibe o status dos servidores configurados.

Para verificar…	Use este comando…
Estado da configuração DNS	`vserver services name-service dns check`
Estado da configuração LDAP	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

A validação da configuração é bem-sucedida se pelo menos um dos servidores configurados (name-serviders/ldap-serviders) estiver acessível e fornecendo o serviço. É apresentado um aviso se alguns dos servidores não estiverem acessíveis.

Comandos para gerenciar entradas do switch do serviço de nomes

Você pode gerenciar entradas de switch de serviço de nomes criando, exibindo, modificando e excluindo-as.

Se você quiser…	Use este comando…
Crie uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch create`
Exibir entradas do switch de serviço de nomes	`vserver services name-service ns-switch show`
Modificar uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch modify`
Excluir uma entrada de switch de serviço de nomes	`vserver services name-service ns-switch delete`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

"Relatório técnico da NetApp 4668: Guia de práticas recomendadas para serviços de nomes"

Comandos para gerenciar o cache do serviço de nomes

Você pode gerenciar o cache do serviço de nomes modificando o valor time to live (TTL). O valor TTL determina quanto tempo as informações do serviço de nome são persistentes no cache.

Se você quiser modificar o valor TTL para…	Use este comando…
Usuários UNIX	`vserver services name-service cache unix-user settings`
Grupos UNIX	`vserver services name-service cache unix-group settings`
Netgroups UNIX	`vserver services name-service cache netgroups settings`
Hosts	`vserver services name-service cache hosts settings`
Associação ao grupo	`vserver services name-service cache group-membership settings`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`
Troque a posição de dois mapeamentos de nomes NOTA: Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`

Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar usuários UNIX locais

Existem comandos ONTAP específicos para gerenciar usuários UNIX locais.

Se você quiser…	Use este comando…
Crie um usuário local do UNIX	`vserver services name-service unix-user create`
Carregue usuários UNIX locais a partir de um URI	`vserver services name-service unix-user load-from-uri`
Exibir usuários locais do UNIX	`vserver services name-service unix-user show`
Modifique um usuário local UNIX	`vserver services name-service unix-user modify`
Excluir um usuário local UNIX	`vserver services name-service unix-user delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar grupos UNIX locais.

Se você quiser…	Use este comando…
Crie um grupo UNIX local	`vserver services name-service unix-group create`
Adicione um usuário a um grupo UNIX local	`vserver services name-service unix-group adduser`
Carregue grupos UNIX locais a partir de um URI	`vserver services name-service unix-group load-from-uri`
Exibir grupos UNIX locais	`vserver services name-service unix-group show`
Modifique um grupo UNIX local	`vserver services name-service unix-group modify`

Excluir um usuário de um grupo UNIX local	`vserver services name-service unix-group deluser`
Exclua um grupo UNIX local	`vserver services name-service unix-group delete`

Consulte a página de manual de cada comando para obter mais informações.

Limites para usuários, grupos e membros do grupo UNIX locais

O ONTAP introduziu limites para o número máximo de usuários e grupos UNIX no cluster e comandos para gerenciar esses limites. Esses limites podem ajudar a evitar problemas de desempenho, impedindo que os administradores criem muitos usuários e grupos UNIX locais no cluster.

Há um limite para o número combinado de grupos de usuários UNIX locais e membros de grupo. Há um limite separado para usuários UNIX locais. Os limites são em todo o cluster. Cada um desses novos limites é definido como um valor padrão que você pode modificar até um limite rígido pré-atribuído.

Banco de dados	Limite padrão	Limite rígido
Usuários locais do UNIX	32.768	65.536
Grupos UNIX locais e membros do grupo	32.768	65.536

Gerenciar limites para usuários e grupos UNIX locais

Existem comandos ONTAP específicos para gerenciar limites para usuários e grupos UNIX locais. Os administradores de cluster podem usar esses comandos para solucionar problemas de desempenho no cluster que se acredita estar relacionado a um número excessivo de usuários e grupos UNIX locais.

Sobre esta tarefa

Esses comandos estão disponíveis para o administrador do cluster no nível avançado de privilégio.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Use o comando…
Exibir informações sobre os limites de usuários UNIX locais	`vserver services unix-user max-limit show`
Exibir informações sobre os limites de grupos UNIX locais	`vserver services unix-group max-limit show`

Se você quiser…	Use o comando…
Modifique os limites de usuários UNIX locais	`vserver services unix-user max-limit modify`
Modificar limites de grupo UNIX local	`vserver services unix-group max-limit modify`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar netgroups locais

É possível gerenciar grupos de redes locais carregando-os a partir de um URI, verificando seu status entre nós, exibindo-os e excluindo-os.

Se você quiser…	Use o comando…
Carregue netgroups de um URI	`vserver services name-service netgroup load`
Verifique o status dos grupos de redes entre nós	`vserver services name-service netgroup status` Disponível no nível de privilégio avançado e superior.
Exibir grupos de redes locais	`vserver services name-service netgroup file show`
Exclua um netgroup local	`vserver services name-service netgroup file delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de domínio NIS

Existem comandos ONTAP específicos para gerenciar configurações de domínio NIS.

Se você quiser…	Use este comando…
Crie uma configuração de domínio NIS	`vserver services name-service nis-domain create`
Exibir configurações de domínio NIS	`vserver services name-service nis-domain show`
Exibir status de vinculação de uma configuração de domínio NIS	`vserver services name-service nis-domain show-bound`
Apresentar estatísticas NIS	`vserver services name-service nis-domain show-statistics` Disponível no nível de privilégio avançado e superior.

Limpar estatísticas NIS	`vserver services name-service nis-domain clear-statistics` Disponível no nível de privilégio avançado e superior.
Modificar uma configuração de domínio NIS	`vserver services name-service nis-domain modify`
Excluir uma configuração de domínio NIS	`vserver services name-service nis-domain delete`
Ative o armazenamento em cache para pesquisas netgroup-by-host	`vserver services name-service nis-domain netgroup-database config modify` Disponível no nível de privilégio avançado e superior.

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de cliente LDAP

Existem comandos ONTAP específicos para gerenciar configurações de cliente LDAP.

Os administradores do SVM não podem modificar ou excluir configurações de cliente LDAP criadas pelos administradores de cluster.

Se você quiser…	Use este comando…
Crie uma configuração de cliente LDAP	`vserver services name-service ldap client create`
Exibir configurações de cliente LDAP	`vserver services name-service ldap client show`
Modificar uma configuração de cliente LDAP	`vserver services name-service ldap client modify`
Altere a senha DE VINCULAÇÃO do cliente LDAP	`vserver services name-service ldap client modify-bind-password`
Eliminar uma configuração de cliente LDAP	`vserver services name-service ldap client delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações LDAP

Existem comandos ONTAP específicos para gerenciar configurações LDAP.

Se você quiser…	Use este comando…
Crie uma configuração LDAP	`vserver services name-service ldap create`

Exibir configurações LDAP	`vserver services name-service ldap show`
Modificar uma configuração LDAP	`vserver services name-service ldap modify`
Eliminar uma configuração LDAP	`vserver services name-service ldap delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar modelos de esquema de cliente LDAP

Existem comandos ONTAP específicos para gerenciar modelos de esquema de cliente LDAP.

Os administradores do SVM não podem modificar ou excluir esquemas de cliente LDAP criados por administradores de cluster.

Se você quiser…	Use este comando…
Copie um modelo de esquema LDAP existente	`vserver services name-service ldap client schema copy` Disponível no nível de privilégio avançado e superior.
Exibir modelos de esquema LDAP	`vserver services name-service ldap client schema show`
Modifique um modelo de esquema LDAP	`vserver services name-service ldap client schema modify` Disponível no nível de privilégio avançado e superior.
Excluir um modelo de esquema LDAP	`vserver services name-service ldap client schema delete` Disponível no nível de privilégio avançado e superior.

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações de interface NFS Kerberos

Existem comandos ONTAP específicos para gerenciar configurações de interface do NFS Kerberos.

Se você quiser…	Use este comando…
Ative o NFS Kerberos em um LIF	`vserver nfs kerberos interface enable`
Exibir configurações de interface NFS Kerberos	`vserver nfs kerberos interface show`
Modificar uma configuração de interface NFS Kerberos	`vserver nfs kerberos interface modify`

Desative o NFS Kerberos em um LIF	`vserver nfs kerberos interface disable`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar configurações NFS Kerberos Realm

Existem comandos ONTAP específicos para gerenciar configurações de realm Kerberos NFS.

Se você quiser…	Use este comando…
Crie uma configuração NFS Kerberos realm	`vserver nfs kerberos realm create`
Exibir configurações do NFS Kerberos Realm	`vserver nfs kerberos realm show`
Modifique uma configuração de realm do Kerberos NFS	`vserver nfs kerberos realm modify`
Excluir uma configuração NFS Kerberos realm	`vserver nfs kerberos realm delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar políticas de exportação

Existem comandos ONTAP específicos para gerenciar políticas de exportação.

Se você quiser…	Use este comando…
Exibir informações sobre políticas de exportação	`vserver export-policy show`
Renomeie uma política de exportação	`vserver export-policy rename`
Copiar uma política de exportação	`vserver export-policy copy`
Eliminar uma política de exportação	`vserver export-policy delete`

Consulte a página de manual de cada comando para obter mais informações.

Comandos para gerenciar regras de exportação

Existem comandos ONTAP específicos para gerenciar regras de exportação.

Se você quiser…	Use este comando…
Crie uma regra de exportação	`vserver export-policy rule create`
Exibir informações sobre regras de exportação	`vserver export-policy rule show`
Modificar uma regra de exportação	`vserver export-policy rule modify`
Excluir uma regra de exportação	`vserver export-policy rule delete`

Se você tiver configurado várias regras de exportação idênticas que correspondam a diferentes clientes, certifique-se de mantê-las sincronizadas ao gerenciar regras de exportação.

Consulte a página de manual de cada comando para obter mais informações.

Configurar o cache de credenciais NFS

Motivos para modificar o tempo de funcionamento do cache de credenciais NFS

O ONTAP usa um cache de credenciais para armazenar as informações necessárias para autenticação de usuário para acesso de exportação NFS para fornecer acesso mais rápido e melhorar o desempenho. Você pode configurar por quanto tempo as informações são armazenadas no cache de credenciais para personalizá-las para o seu ambiente.

Há vários cenários ao modificar o cache de credenciais NFS Time-to-live (TTL) pode ajudar a resolver problemas. Você deve entender quais são esses cenários, bem como as consequências de fazer essas modificações.

Razões

Considere alterar o TTL padrão nas seguintes circunstâncias:

Problema	Medidas corretivas
Os servidores de nomes no seu ambiente estão sofrendo degradação no desempenho devido a uma alta carga de solicitações do ONTAP.	Aumente o TTL para credenciais positivas e negativas armazenadas em cache para reduzir o número de solicitações do ONTAP para servidores de nomes.
O administrador do servidor de nomes fez alterações para permitir o acesso a usuários NFS que foram negados anteriormente.	Diminua o TTL para credenciais negativas armazenadas em cache para reduzir o tempo que os usuários NFS precisam esperar que o ONTAP solicite novas credenciais de servidores de nomes externos para que eles possam obter acesso.

Problema	Medidas corretivas
O administrador do servidor de nomes fez alterações para negar acesso a usuários NFS que anteriormente eram permitidos.	Reduza o TTL para credenciais positivas armazenadas em cache para reduzir o tempo antes que o ONTAP solicite novas credenciais de servidores de nomes externos para que os usuários NFS agora tenham acesso negado.

Consequências

Você pode modificar o tempo individualmente para armazenar credenciais positivas e negativas em cache. No entanto, você deve estar ciente das vantagens e desvantagens de fazê-lo.

Se você…	A vantagem é…	A desvantagem é…
Aumente o tempo de cache de credenciais positivas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.
Diminua o tempo de cache positivo de credenciais	Leva menos tempo para negar acesso a usuários NFS que anteriormente eram permitidos acesso, mas não são mais.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.
Aumente o tempo de cache de credenciais negativas	O ONTAP envia solicitações de credenciais para nomear servidores com menos frequência, reduzindo a carga nos servidores de nomes.	Leva mais tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.
Diminua o tempo de cache de credenciais negativas	Leva menos tempo para conceder acesso a usuários NFS que anteriormente não tinham acesso permitido, mas agora.	O ONTAP envia solicitações de credenciais para nomear servidores com mais frequência, aumentando a carga nos servidores de nomes.

Configure o tempo de ativação para credenciais de usuário NFS armazenadas em cache

Você pode configurar o período de tempo que o ONTAP armazena credenciais para usuários NFS em seu cache interno (time-to-live ou TTL) modificando o servidor NFS da máquina virtual de armazenamento (SVM). Isso permite que você solucione certos problemas relacionados à alta carga nos servidores de nomes ou alterações nas credenciais que afetam o acesso do usuário NFS.

Sobre esta tarefa

Estes parâmetros estão disponíveis no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser modificar o TTL para cache…	Use o comando…
Credenciais positivas	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` O TTL é medido em milissegundos. A partir do ONTAP 9.10,1 e posterior, o padrão é de 1 hora (3.600.000 milissegundos). No ONTAP 9.9,1 e anterior, o padrão é 24 horas (86.400.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).
Credenciais negativas	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` O TTL é medido em milissegundos. O padrão é 2 horas (7.200.000 milissegundos). O intervalo permitido para este valor é de 1 minuto (60000 milissegundos) a 7 dias (604.800.000 milissegundos).

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar caches de política de exportação

Lavar caches de política de exportação

O ONTAP usa vários caches de política de exportação para armazenar informações relacionadas a políticas de exportação para acesso mais rápido. A eliminação de caches de política de exportação manualmente (`vserver export-policy cache flush`) remove informações potencialmente desatualizadas e força o ONTAP a recuperar informações atuais dos recursos externos apropriados. Isso pode ajudar a resolver uma variedade de problemas relacionados ao acesso do cliente às exportações NFS.

Sobre esta tarefa

As informações de cache de política de exportação podem estar desatualizadas devido aos seguintes motivos:

- Uma alteração recente às regras de política de exportação
- Uma alteração recente nos registos de nome de anfitrião nos servidores de nomes
- Uma alteração recente para entradas de netgroup em servidores de nomes
- Recuperando-se de uma interrupção de rede que impedia que os netgroups fossem totalmente

carregados

Passos

1. Se você não tiver o cache do serviço de nomes habilitado, execute uma das seguintes ações no modo de privilégio avançado:

Se você quiser flush…	Digite o comando…
Todos os caches de política de exportação (exceto showmount)	`vserver export-policy cache flush -vserver vserver_name`
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver export-policy cache flush -vserver vserver_name -cache host`
O cache netgroup	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. Se o cache do serviço de nomes estiver ativado, execute uma das seguintes ações:

Se você quiser flush…	Digite o comando…
As regras de política de exportação acedem à cache	`vserver export-policy cache flush -vserver vserver_name -cache access` Você pode incluir o parâmetro opcional `-node` para especificar o nó no qual deseja limpar o cache de acesso.
O cache do nome do host	`vserver services name-service cache hosts forward-lookup delete-all`

Se você quiser flush…	Digite o comando…
O cache netgroup	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` O processamento de netgroups é intensivo em recursos. Você só deve limpar o cache do netgroup se estiver tentando resolver um problema de acesso de cliente causado por um netgroup obsoleto.
O cache showmount	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

Exiba a fila e o cache do netgroup da política de exportação

O ONTAP usa a fila netgroup ao importar e resolver netgroups e usa o cache netgroup para armazenar as informações resultantes. Ao solucionar problemas relacionados ao netgroup da política de exportação, você pode usar os `vserver export-policy netgroup queue show` comandos e `vserver export-policy netgroup cache show` para exibir o status da fila do netgroup e o conteúdo do cache do netgroup.

Passo

1. Execute uma das seguintes ações:

Para exibir o netgroup da política de exportação…	Digite o comando…
Fila de espera	`vserver export-policy netgroup queue show`
Cache	`vserver export-policy netgroup cache show -vserver vserver_name`

Consulte a página de manual de cada comando para obter mais informações.

Verifique se um endereço IP de cliente é membro de um netgroup

Ao solucionar problemas de acesso de cliente NFS relacionados a netgroups, você pode usar o `vserver export-policy netgroup check-membership` comando para ajudar a determinar se um IP de cliente é membro de um determinado netgroup.

Sobre esta tarefa

Verificar a associação ao netgroup permite determinar se o ONTAP está ciente de que um cliente é ou não membro de um netgroup. Ele também permite que você saiba se o cache do ONTAP netgroup está em um estado transitório enquanto atualiza informações do netgroup. Essas informações podem ajudá-lo a entender por que um cliente pode ter acesso inesperadamente concedido ou negado.

Passo

1. Verifique a associação do netgroup de um endereço IP de cliente: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   O comando pode retornar os seguintes resultados:

   - O cliente é um membro do netgroup.

     Isso foi confirmado por meio de uma pesquisa de pesquisa reversa ou de uma pesquisa netgroup-by-host.

   - O cliente é um membro do netgroup.

     Ele foi encontrado no cache do ONTAP netgroup.

   - O cliente não é membro do netgroup.
   - A associação ao cliente ainda não pode ser determinada porque o ONTAP está atualizando o cache do netgroup.

     Até que isso seja feito, a associação não pode ser explicitamente descartada dentro ou fora. Use o `vserver export-policy netgroup queue show` comando para monitorar o carregamento do netgroup e tentar novamente a verificação depois que ela estiver concluída.

Exemplo

O exemplo a seguir verifica se um cliente com o endereço IP 172.17.16.72 é membro do netgroup Mercury no SVM VS1:

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

Otimizar o desempenho do cache de acesso

Você pode configurar vários parâmetros para otimizar o cache de acesso e encontrar o equilíbrio certo entre o desempenho e a corrente das informações armazenadas no cache de acesso.

Sobre esta tarefa

Quando configurar os períodos de atualização do cache de acesso, tenha em mente o seguinte:

- Valores mais altos significam que as entradas permanecem mais longas no cache de acesso.

  A vantagem é o melhor desempenho porque o ONTAP gasta menos recursos na atualização de entradas de cache de acesso. A desvantagem é que se as regras de política de exportação mudarem e as entradas de cache de acesso ficarem obsoletas como resultado, leva mais tempo para atualizá-las. Como resultado, os clientes que devem obter acesso podem ser negados e os clientes que devem ser negados podem obter acesso.

- Valores mais baixos significam que o ONTAP atualiza as entradas do cache de acesso com mais frequência.

A vantagem é que as entradas são mais atuais e os clientes são mais propensos a ter acesso correto ou negado. A desvantagem é uma diminuição no desempenho porque o ONTAP gasta mais recursos atualizando entradas de cache de acesso.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Para modificar o…	Digite…
Período de atualização para entradas positivas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
Período de atualização para entradas negativas	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
Período de tempo limite para entradas antigas	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. Verifique as novas configurações de parâmetros:

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem

causar falha no aplicativo NFS.

- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança da Lista de Controle de Acesso (ACL) do Windows que impedem que usuários ou aplicativos renomeem diretórios críticos.

Saiba mais "Como impedir que diretórios sejam renomeados enquanto os clientes os acessam"sobre o .

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
```

```
                    Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Travas de quebra

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador:

   `set -privilege admin`

Como os filtros de primeira leitura e primeira gravação do FPolicy funcionam com o NFS

Os clientes NFS experimentam um alto tempo de resposta durante o alto tráfego de solicitações de leitura/gravação quando o FPolicy é habilitado usando um servidor FPolicy externo com operações de leitura/gravação como eventos monitorados. Para clientes NFS, o uso de filtros de primeira leitura e primeira gravação no FPolicy reduz o número de notificações do FPolicy e melhora o desempenho.

No NFS, o cliente faz a e/S em um arquivo, buscando sua alça. Esse identificador pode permanecer válido nas reinicializações do servidor e do cliente. Portanto, o cliente está livre para armazenar em cache o identificador e enviar solicitações nele sem recuperar alças novamente. Em uma sessão regular, muitas solicitações de leitura/gravação são enviadas para o servidor de arquivos. Se as notificações forem geradas para todas essas solicitações, isso pode resultar nos seguintes problemas:

- Uma carga maior devido ao processamento de notificação adicional e maior tempo de resposta.
- Um grande número de notificações sendo enviadas para o servidor FPolicy, mesmo que o servidor não seja afetado por todas as notificações.

Depois de receber a primeira solicitação de leitura/gravação de um cliente para um arquivo específico, uma entrada de cache é criada e a contagem de leitura/gravação é incrementada. Essa solicitação é marcada como a operação de primeira leitura/gravação e um evento FPolicy é gerado. Antes de Planejar e criar seus filtros FPolicy para um cliente NFS, você deve entender os conceitos básicos de como os filtros FPolicy funcionam.

- Primeira leitura: Filtra as solicitações de leitura do cliente para primeira leitura.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira leitura para a qual o FPolicy é processado.

- Primeira gravação: Filtra as solicitações de gravação do cliente para a primeira gravação.

  Quando esse filtro é usado para eventos NFS, as `-file-session-io-grouping-count` configurações e `-file-session-io-grouping-duration` determinam a solicitação de primeira gravação para a qual o FPolicy foi processado.

As seguintes opções são adicionadas no banco de dados de servidores NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

Modifique a ID de implementação do servidor NFSv4,1

O protocolo NFSv4,1 inclui uma ID de implementação de servidor que documenta o domínio, o nome e a data do servidor. Você pode modificar os valores padrão da ID de implementação do servidor. Alterar os valores padrão pode ser útil, por exemplo, ao coletar estatísticas de uso ou solucionar problemas de interoperabilidade. Para obter mais informações, consulte RFC 5661.

Sobre esta tarefa

Os valores padrão para as três opções são os seguintes:

Opção	Nome da opção	Valor padrão
Domínio ID de implementação NFSv4,1	`-v4.1-implementation -domain`	NetApp.com
NFSv4,1 Nome ID implementação	`-v4.1-implementation-name`	Nome da versão do cluster
NFSv4,1 Data ID implementação	`-v4.1-implementation-date`	Data da versão do cluster

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser modificar o ID de implementação do NFSv4,1…	Digite o comando…
Domínio	`vserver nfs modify -v4.1 -implementation-domain domain`
Nome	`vserver nfs modify -v4.1 -implementation-name name`
Data	`vserver nfs modify -v4.1 -implementation-date date`

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar ACLs NFSv4

Benefícios de habilitar ACLs NFSv4

Há muitos benefícios em habilitar ACLs NFSv4.

Os benefícios de habilitar ACLs NFSv4 incluem o seguinte:

- Controle mais refinado do acesso do usuário para arquivos e diretórios
- Melhor segurança NFS
- Interoperabilidade aprimorada com CIFS
- Remoção da limitação NFS de 16 grupos por usuário

Como as ACLs NFSv4 funcionam

Um cliente que usa ACLs NFSv4 pode definir e exibir ACLs em arquivos e diretórios no sistema. Quando um novo arquivo ou subdiretório é criado em um diretório que tem uma ACL, o novo arquivo ou subdiretório herda todas as entradas de controle de acesso (ACEs) na ACL que foram marcadas com os sinalizadores de herança apropriados.

Quando um arquivo ou diretório é criado como resultado de uma solicitação NFSv4, a ACL no arquivo ou diretório resultante depende se a solicitação de criação de arquivo inclui uma ACL ou apenas permissões de acesso de arquivo UNIX padrão e se o diretório pai tem uma ACL:

- Se a solicitação incluir uma ACL, essa ACL é usada.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão, mas o diretório pai tiver uma ACL, os ACEs na ACL do diretório pai serão herdados pelo novo arquivo ou diretório, desde que os ACEs tenham sido marcados com os sinalizadores de herança apropriados.

  Uma ACL pai é herdada mesmo se `-v4.0-acl` estiver definida como `off`.

- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão e o diretório pai não tiver uma ACL, o modo de arquivo cliente será usado para definir permissões de acesso a arquivos UNIX padrão.
- Se a solicitação incluir apenas permissões de acesso de arquivo UNIX padrão e o diretório pai tiver uma ACL não herdável, o novo objeto será criado apenas com bits de modo.

Se o `-chown-mode` parâmetro tiver sido definido como `restricted` com comandos nas `vserver nfs` famílias ou `vserver export-policy rule`, a propriedade do arquivo só pode ser alterada pelo superusuário, mesmo que as permissões no disco definidas com ACLs NFSv4 permitam que um usuário não-root altere a propriedade do arquivo. Para obter mais informações, consulte as páginas de manual relevantes.

Ativar ou desativar a modificação das ACLs NFSv4

Quando o ONTAP recebe um `chmod` comando para um arquivo ou diretório com uma ACL, por padrão a ACL é mantida e modificada para refletir a alteração de bit de modo. Você pode desativar o `-v4-acl-preserve` parâmetro para alterar o comportamento se quiser que a ACL seja descartada.

Sobre esta tarefa

Ao usar estilo de segurança unificado, esse parâmetro também especifica se as permissões de arquivo NTFS são preservadas ou descartadas quando um cliente envia um comando chmod, chgroup ou chown para um arquivo ou diretório.

A predefinição para este parâmetro está ativada.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Ativar retenção e modificação de ACLs NFSv4 existentes (padrão)	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
Desative a retenção e solte as ACLs NFSv4 ao alterar os bits de modo	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como o ONTAP usa ACLs NFSv4 para determinar se ele pode excluir um arquivo

Para determinar se ele pode excluir um arquivo, o ONTAP usa uma combinação do bit DE EXCLUSÃO do arquivo e o bit DELETE_CHILD do diretório que contém. Para obter mais informações, consulte o NFS 4,1 RFC 5661.

Ativar ou desativar ACLs NFSv4

Para ativar ou desativar as ACLs NFSv4, pode modificar as `-v4.0-acl` opções e. `-v4.1-acl` Estas opções estão desativadas por predefinição.

Sobre esta tarefa

A `-v4.0-acl` opção ou `-v4.1-acl` controla a configuração e visualização de ACLs NFSv4; ela não controla a aplicação dessas ACLs para verificação de acesso.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
Desativar ACLs NFSv4,0	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
Ativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`
Desativar ACLs NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

Modifique o limite máximo de ACE para ACLs NFSv4

É possível modificar o número máximo de ACEs permitidos para cada ACL NFSv4 modificando o parâmetro `-v4-acl-max-aces`. Por padrão, o limite é definido como 400 ACEs para cada ACL. Aumentar esse limite pode ajudar a garantir a migração bem-sucedida de dados com ACLs que contêm mais de 400 ACEs para sistemas de storage que executam ONTAP.

Sobre esta tarefa

Aumentar esse limite pode afetar o desempenho dos clientes que acessam arquivos com ACLs NFSv4.

Passos

1. Defina o nível de privilégio como avançado:

   `set -privilege advanced`

2. Modifique o limite máximo de ACE para ACLs NFSv4:

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   O intervalo válido de

   `max_ace_limit` é a. `192` `1024`.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Gerenciar delegações de arquivos do NFSv4

Ativar ou desativar as delegações de ficheiros de leitura do NFSv4

Para ativar ou desativar as delegações de ficheiros de leitura do NFSv4, pode modificar a `-v4.0-read-delegation`opção ou . Ao ativar as delegações de arquivos de leitura, você pode eliminar grande parte da sobrecarga de mensagens associada à abertura e fechamento de arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de leitura são desativadas.

A desvantagem de habilitar delegações de arquivos de leitura é que o servidor e seus clientes devem recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar, ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
Ativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: E `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
Desativar as delegações de ficheiros de leitura NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
Desativar as delegações de ficheiros de leitura NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Ativar ou desativar as delegações de ficheiros de gravação NFSv4

Para ativar ou desativar as delegações de ficheiros de gravação, pode modificar a `-v4.0-write-delegation`opção ou . Ao ativar as delegações de arquivos de gravação, você pode eliminar grande parte da sobrecarga de mensagens associada ao bloqueio de arquivos e Registros, além de abrir e fechar arquivos.

Sobre esta tarefa

Por padrão, as delegações de arquivos de gravação são desativadas.

A desvantagem de habilitar delegações de arquivos de gravação é que o servidor e seus clientes devem executar tarefas adicionais para recuperar delegações após o servidor reiniciar ou reiniciar, um cliente reiniciar ou reiniciar ou uma partição de rede ocorrer.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Então…
Ativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled`
Ativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled`
Desativar as delegações de ficheiros de gravação NFSv4	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled`
Desativar as delegações de ficheiros de gravação NFSv4,1	Introduza o seguinte comando: `vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled`

Resultado

As opções de delegação de arquivos entram em vigor assim que são alteradas. Não há necessidade de reinicializar ou reiniciar o NFS.

Configure o bloqueio de arquivos NFSv4 e Registro

Cerca de NFSv4 arquivo e Registro de bloqueio

Para clientes NFSv4, o ONTAP suporta o mecanismo de bloqueio de arquivos NFSv4, mantendo o estado de todos os bloqueios de arquivos em um modelo baseado em leasing.

"Relatório técnico da NetApp 3580: NFSv4 melhorias e melhores práticas Guia de implementação do Data ONTAP"

Especifique o período de locação de bloqueio NFSv4

Para especificar o período de locação de bloqueio NFSv4 (ou seja, o período de tempo em que o ONTAP concede irrevogavelmente um bloqueio a um cliente), você pode modificar a `-v4-lease-seconds` opção. Períodos de leasing mais curtos aceleram a recuperação do servidor, enquanto períodos de leasing mais longos são benéficos para servidores que lidam com uma grande quantidade de clientes.

Sobre esta tarefa

Por padrão, essa opção está definida como `30`. O valor mínimo para esta opção é `10`. O valor máximo para esta opção é o período de tolerância de bloqueio, que pode ser definido com a `locking.lease_seconds` opção.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Especifique o período de tolerância de bloqueio NFSv4

Para especificar o período de carência de bloqueio NFSv4 (ou seja, o período de tempo em que os clientes tentam recuperar seu estado de bloqueio do ONTAP durante a recuperação do servidor), você pode modificar a `-v4-grace-seconds` opção.

Sobre esta tarefa

Por padrão, essa opção está definida como `45`.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Como NFSv4 referências funcionam

Quando você ativa referências NFSv4, o ONTAP fornece referências "intra-SVM" para clientes NFSv4. A referência intra-SVM ocorre quando um nó de cluster que recebe a solicitação NFSv4 refere o cliente NFSv4 a outra interface lógica (LIF) na máquina virtual de storage (SVM).

O cliente NFSv4 deve acessar o caminho que recebeu a referência no LIF de destino a partir desse ponto. O nó do cluster original fornece tal referência quando determina que existe um LIF no SVM que reside no nó do cluster no qual o volume de dados reside, permitindo assim aos clientes acesso mais rápido aos dados e evitando comunicação extra do cluster.

Ativar ou desativar referências NFSv4

Você pode habilitar referências NFSv4D em máquinas virtuais de armazenamento (SVMs) habilitando as opções `-v4-fsid-change` e `-v4.0-referrals`ou. Habilitar referências NFSv4 pode resultar em acesso mais rápido aos dados para clientes NFSv4 que suportam esse recurso.

O que você vai precisar

Se você quiser ativar as referências NFS, primeiro desative o NFS paralelo. Não é possível ativar ambos ao mesmo tempo.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar NFSv4 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
Desative as referências NFSv4	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
Ativar NFSv4,1 referências	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
Desative as referências NFSv4,1	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exibir estatísticas NFS

É possível exibir estatísticas NFS para máquinas virtuais de storage (SVMs) no sistema de storage para monitorar a performance e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NFS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object nfs*
   ```

2. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Exemplo: Monitorando o desempenho do NFSv3

O exemplo a seguir mostra os dados de desempenho do protocolo NFSv3.

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

O comando a seguir mostra os dados da amostra especificando contadores que mostram o número de solicitações de leitura e gravação bem-sucedidas versus o número total de solicitações de leitura e gravação:

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ---------------------------
    read_success                                40042
    read_total                                  40042
    write_success                             1492052
    write_total                               1492052
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Exibir estatísticas de DNS

Você pode exibir estatísticas de DNS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos DNS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas de DNS

Os exemplos a seguir mostram dados de desempenho para consultas DNS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de consultas DNS enviadas versus o número de consultas DNS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que exibem o número de vezes que um erro específico foi recebido para uma consulta DNS no servidor específico:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Apresentar estatísticas NIS

Você pode exibir estatísticas NIS para máquinas virtuais de armazenamento (SVMs) no sistema de armazenamento para monitorar o desempenho e diagnosticar problemas.

Passos

1. Use o `statistics catalog object show` comando para identificar os objetos NIS a partir dos quais você pode exibir dados.

   ```
   statistics catalog object show -object external_service_op*
   ```

2. Use os `statistics start` comandos e `statistics stop` para coletar uma amostra de dados de um ou mais objetos.
3. Use o `statistics show` comando para exibir os dados de amostra.

Monitoramento de estatísticas NIS

Os exemplos a seguir exibem dados de desempenho para consultas NIS. Os seguintes comandos iniciam a coleta de dados para uma nova amostra:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de consultas NIS enviadas versus o número de consultas NIS recebidas, com falha ou com tempo limite:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

O comando a seguir exibe dados da amostra especificando contadores que mostram o número de vezes que um erro específico foi recebido para uma consulta NIS no servidor específico:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                    10.227.13.221
3 entries were displayed.
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Suporte para VMware vStorage sobre NFS

O ONTAP dá suporte a determinados recursos de APIs de storage do VMware vStorage para integração de array (VAAI) em um ambiente NFS.

Recursos suportados

Os seguintes recursos são suportados:

- Descarga de cópia

  Permite que um host ESXi copie máquinas virtuais ou discos de máquinas virtuais (VMDKs) diretamente entre o local de armazenamento de dados de origem e destino sem envolver o host. Isso conserva os ciclos de CPU do host ESXi e a largura de banda da rede. A descarga de cópia preserva a eficiência de espaço se o volume de origem for esparso.

- Reserva de espaço

  Garante espaço de armazenamento para um arquivo VMDK reservando espaço para ele.

Limitações

O VMware vStorage sobre NFS tem as seguintes limitações:

- As operações de descarga de cópia podem falhar nos seguintes cenários:
  - Ao executar o wafliron no volume de origem ou destino, porque ele temporariamente coloca o volume off-line
  - Ao mover o volume de origem ou destino
  - Ao mover o LIF de origem ou destino
  - Durante a realização de operações de takeover ou giveback
  - Durante a execução de operações de comutação ou switchback
- A cópia do lado do servidor pode falhar devido a diferenças de formato de identificador de arquivo no seguinte cenário:

  Você tenta copiar dados de SVMs que exportaram qtrees atualmente ou anteriormente para SVMs que nunca exportaram qtrees. Para contornar essa limitação, você pode exportar pelo menos uma qtree no SVM de destino.

Informações relacionadas

"Quais operações descarregadas da VAAI são suportadas pelo Data ONTAP?"

Ative ou desative o VMware vStorage em NFS

Você pode ativar ou desativar o suporte para VMware vStorage sobre NFS em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, o suporte ao VMware vStorage sobre NFS está desativado.

Passos

1. Exibir o status atual de suporte do vStorage para SVMs:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage enabled`
Desative o suporte ao VMware vStorage	`vserver nfs modify -vserver vserver_name -vstorage disabled`

Depois de terminar

Você deve instalar o plug-in NFS para VMware VAAI antes de usar essa funcionalidade. Para obter mais informações, consulte *Instalando o plug-in NFS do NetApp para VMware VAAI*.

Informações relacionadas

"Documentação do NetApp: Plug-in NFS do NetApp para VMware VAAI"

Ativar ou desativar o suporte rquota

O ONTAP suporta o protocolo de cota remota versão 1 (rquota v1). O protocolo rquota permite que os clientes NFS obtenham informações de quota para os utilizadores a partir de uma máquina remota. Você pode ativar o rquota em máquinas virtuais de armazenamento (SVMs) usando o `vserver nfs modify` comando.

Sobre esta tarefa

Por padrão, rquota está desativada.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Habilite o suporte a rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota enable`
Desative o suporte rquota para SVMs	`vserver nfs modify -vserver vserver_name -rquota disable`

   Para obter mais informações sobre cotas, "Gerenciamento de storage lógico"consulte .

Melhoria do desempenho NFSv3 e NFSv4 modificando o tamanho da transferência TCP

Você pode melhorar o desempenho de clientes NFSv3 e NFSv4 conetados a sistemas de armazenamento em uma rede de alta latência, modificando o tamanho máximo de

transferência TCP.

Quando os clientes acessam sistemas de armazenamento em uma rede de alta latência, como uma rede de área ampla (WAN) ou uma rede de área metropolitana (MAN) com latência superior a 10 milissegundos, talvez você consiga melhorar o desempenho da conexão modificando o tamanho máximo da transferência TCP. Os clientes que acessam sistemas de storage em uma rede de baixa latência, como uma rede de área local (LAN), podem esperar pouco ou nenhum benefício ao modificar esses parâmetros. Se a melhoria da taxa de transferência não exceder o impactos da latência, você não deve usar esses parâmetros.

Para determinar se o ambiente de storage se beneficiaria da modificação desses parâmetros, primeiro você deve realizar uma avaliação abrangente de desempenho de um cliente NFS com baixa performance. Analise se o baixo desempenho é devido à latência excessiva da viagem de ida e volta e à pequena solicitação no cliente. Nestas condições, o cliente e o servidor não podem utilizar totalmente a largura de banda disponível porque gastam a maioria dos seus ciclos de serviço esperando que pequenas solicitações e respostas sejam transmitidas através da conexão.

Ao aumentar o tamanho da solicitação NFSv3 e NFSv4, o cliente e o servidor podem usar a largura de banda disponível de forma mais eficaz para mover mais dados por unidade de tempo; portanto, aumentando a eficiência geral da conexão.

Tenha em mente que a configuração entre o sistema de armazenamento e o cliente pode variar. O sistema de armazenamento e o cliente suportam o tamanho máximo de 1 MB para operações de transferência. No entanto, se você configurar o sistema de armazenamento para suportar o tamanho máximo de transferência de 1 MB, mas o cliente só suporta 64 KB, então o tamanho de transferência de montagem é limitado a 64 KB ou menos.

Antes de modificar esses parâmetros, você deve estar ciente de que isso resulta em consumo de memória adicional no sistema de armazenamento pelo período de tempo necessário para montar e transmitir uma grande resposta. Quanto mais conexões de alta latência para o sistema de armazenamento, maior o consumo de memória adicional. Sistemas de armazenamento com alta capacidade de memória podem ter muito pouco efeito com essa mudança. Os sistemas de armazenamento com baixa capacidade de memória podem sofrer uma degradação notável do desempenho.

O uso bem-sucedido desses parâmetros depende da capacidade de recuperar dados de vários nós de um cluster. A latência inerente da rede do cluster pode aumentar a latência geral da resposta. A latência geral tende a aumentar ao usar esses parâmetros. Como resultado, workloads sensíveis à latência podem mostrar impacto negativo.

Modifique o tamanho máximo de transferência do TCP NFSv3 e NFSv4

Você pode modificar a `-tcp-max-xfer-size` opção para configurar tamanhos máximos de transferência para todas as conexões TCP usando os protocolos NFSv3 e NFSv4.x.

Sobre esta tarefa

Você pode modificar essas opções individualmente para cada máquina virtual de storage (SVM).

A partir do ONTAP 9, as `v3-tcp-max-read-size` opções e `v3-tcp-max-write-size` são obsoletas. Você deve usar a `-tcp-max-xfer-size` opção em vez disso.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Modifique o tamanho máximo de transferência do TCP NFSv3 ou NFSv4	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

Opção	Alcance	Padrão
`-tcp-max-xfer-size`	8192 a 1048576 bytes	65536 bytes

> O tamanho máximo de transferência que você inserir deve ser um múltiplo de 4 KB (4096 bytes). As solicitações que não estão alinhadas corretamente afetam negativamente o desempenho.

3. Use o `vserver nfs show -fields tcp-max-xfer-size` comando para verificar as alterações.
4. Se algum cliente usar montagens estáticas, desmonte e remonte para que o novo tamanho de parâmetro entre em vigor.

Exemplo

O comando a seguir define o tamanho máximo de transferência TCP NFSv3 e NFSv4.x para 1048576 bytes no SVM chamado VS1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

Configure o número de IDs de grupo permitidas para usuários NFS

Por padrão, o ONTAP suporta até 32 IDs de grupo ao lidar com credenciais de usuário NFS usando autenticação Kerberos (RPCSEC_GSS). Ao usar a autenticação AUTH_SYS, o número máximo padrão de IDs de grupo é 16, conforme definido na RFC 5531. Você pode aumentar o máximo até 1.024 se tiver usuários que são membros de mais do que o número padrão de grupos.

Sobre esta tarefa

Se um usuário tiver mais do que o número padrão de IDs de grupo em suas credenciais, os IDs de grupo restantes serão truncados e o usuário poderá receber erros ao tentar acessar arquivos do sistema de armazenamento. Você deve definir o número máximo de grupos, por SVM, para um número que represente o máximo de grupos no ambiente.

> Para entender os pré-requisitos de autenticação AUTH_SYS para ativar grupos estendidos (`-auth-sys-extended-groups`) que usam IDs de grupo além do máximo padrão de 16, consulte este artigo da base de dados de Conhecimento: "AUTH_SYS grupos estendidos alterações para autenticação NFS para ONTAP 9".

A tabela a seguir mostra os dois parâmetros `vserver nfs modify` do comando que determinam o número máximo de IDs de grupo em três configurações de amostra:

Parâmetros	Definições	Limite de IDs de grupo resultantes

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	Estas são as predefinições.
		RPCSEC_GSS: 32
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS: 256
		
		AUTH_SYS: 16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS: 512
		
		AUTH_SYS: 512

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se pretender definir o número máximo de grupos auxiliares permitidos…	Digite o comando…
Apenas para RPCSEC_GSS e deixar AUTH_SYS definido para o valor padrão 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
Para RPCSEC_GSS e AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. Verifique o `-extended-groups-limit` valor e verifique se AUTH_SYS está usando grupos estendidos: `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

O exemplo a seguir habilita grupos estendidos para autenticação AUTH_SYS e define o número máximo de

grupos estendidos para 512 para autenticação AUTH_SYS e RPCSEC_GSS. Essas alterações são feitas apenas para clientes que acessam o SVM chamado VS1:

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ --------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

Controle o acesso do usuário raiz aos dados de estilo de segurança NTFS

Você pode configurar o ONTAP para permitir que clientes NFS acessem dados de estilo de segurança NTFS e clientes NTFS para acessar dados de estilo de segurança NFS. Ao usar o estilo de segurança NTFS em um armazenamento de dados NFS, você deve decidir como tratar o acesso pelo usuário raiz e configurar a máquina virtual de armazenamento (SVM) de acordo.

Sobre esta tarefa

Quando um usuário raiz acessa dados de estilo de segurança NTFS, você tem duas opções:

- Mapeie o usuário raiz para um usuário do Windows como qualquer outro usuário NFS e gerencie o acesso de acordo com ACLs NTFS.
- Ignore as ACLs NTFS e forneça acesso total à raiz.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute a ação desejada:

Se você quiser que o usuário root…	Digite o comando…
Ser mapeado para um usuário do Windows	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`

Ignorar a verificação da ACL NT	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

Por predefinição, este parâmetro está desativado.

Se este parâmetro estiver ativado, mas não houver mapeamento de nomes para o usuário raiz, o ONTAP usará uma credencial de administrador SMB padrão para auditoria.

3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Versões e clientes de NFS compatíveis

Visão geral das versões e clientes NFS compatíveis

Antes de poder usar o NFS na rede, você precisa saber quais versões e clientes do ONTAP são compatíveis.

Esta tabela observa quando versões maiores e menores do protocolo NFS são suportadas por padrão no ONTAP. O suporte por padrão não indica que esta é a versão mais antiga do ONTAP que suporta esse protocolo NFS.

Versão	Suportado	Introduzido
NFSv3	Sim	Todos os lançamentos do ONTAP
NFSv4.0	Sim	ONTAP 8
NFSv4.1	Sim	ONTAP 8,1
NFSv4.2	Sim	ONTAP 9,8
PNFS	Sim	ONTAP 8,1

Para obter as informações mais recentes sobre quais clientes NFS ONTAP suportam, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

NFSv4,0 funcionalidade suportada pelo ONTAP

O ONTAP suporta todas as funcionalidades obrigatórias no NFSv4,0, exceto os mecanismos de segurança SPKM3 e LIPKEY.

A seguinte funcionalidade NFSv4 é suportada:

- **COMPOSTO**

Permite que um cliente solicite várias operações de arquivo em uma única solicitação RPC (chamada de procedimento remoto).

- * Delegação de arquivos*

  Permite que o servidor delege o controle de arquivos a alguns tipos de clientes para acesso de leitura e gravação.

- **Pseudo-fs**

  Usado por servidores NFSv4 para determinar pontos de montagem no sistema de armazenamento. Não existe nenhum protocolo de montagem no NFSv4.

- **Bloqueio**

  Baseado em leasing. Não existem protocolos NLM (Network Lock Manager) ou NSM (Network Status Monitor) separados no NFSv4.

Para obter mais informações sobre o protocolo NFSv4,0, consulte RFC 3530.

Limitações do suporte do ONTAP para NFSv4

Você deve estar ciente de várias limitações do suporte do ONTAP para NFSv4.

- O recurso de delegação não é suportado por todos os tipos de cliente.
- No ONTAP 9.4 e versões anteriores, nomes com carateres não-ASCII em volumes diferentes de UTF8 volumes são rejeitados pelo sistema de armazenamento.

  No ONTAP 9.5 e versões posteriores, os volumes criados com a configuração de linguagem utf8mb4 e montados usando NFS v4 não estão mais sujeitos a essa restrição.

- Todos os identificadores de arquivo são persistentes; o servidor não fornece alças de arquivo voláteis.
- Migração e replicação não são compatíveis.
- Os clientes NFSv4 não são suportados com espelhos de compartilhamento de carga somente leitura.

  O ONTAP encaminha clientes NFSv4 para a fonte do espelho de compartilhamento de carga para acesso direto de leitura e gravação.

- Atributos nomeados não são suportados.
- Todos os atributos recomendados são suportados, exceto para o seguinte:
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`

- time_backup

> Embora não ofereça suporte aos `quota*` atributos, o ONTAP oferece suporte a cotas de usuário e grupo por meio do protocolo RQUOTA de banda lateral.

Suporte ONTAP para NFSv4,1

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por predefinição quando o NFSv4,1 está ativado.

Implementações anteriores de clientes NFS usam apenas uma única conexão TCP com uma montagem. No ONTAP, uma única conexão TCP pode se tornar um gargalo com o aumento de IOPS. No entanto, um cliente habilitado para nconnect pode ter várias conexões TCP (até 16) associadas a uma única montagem NFS. Tal cliente NFS multiplexa operações de arquivos em várias conexões TCP de forma round-robin e, assim, obtém maior throughput da largura de banda de rede disponível. O nConnect é recomendado apenas para montagens NFSv3 e NFSv4,1.

Consulte a documentação do cliente NFS para confirmar se o nconnect é suportado na versão do cliente.

NFSv4,1 é ativado por padrão no ONTAP 9.9,1 e posterior. Em versões anteriores, você pode habilitá-la especificando a `-v4.1` opção e definindo-a para `enabled` quando criar um servidor NFS na máquina virtual de armazenamento (SVM).

O ONTAP não suporta delegações de nível de diretório e arquivo NFSv4,1.

Suporte ONTAP para NFSv4,2

A partir do ONTAP 9.8, o ONTAP suporta o protocolo NFSv4,2 para permitir acesso a clientes habilitados para NFSv4,2.

NFSv4,2 é ativado por padrão no ONTAP 9.9,1 e posterior. No ONTAP 9.8, é necessário habilitar manualmente o v4,2 especificando a `-v4.1` opção e definindo-a para `enabled` quando criar um servidor NFS na máquina virtual de armazenamento (SVM). Ativar o NFSv4,1 também permite que os clientes usem os recursos do NFSv4,1 enquanto montados como v4,2.

Versões sucessivas do ONTAP expandem o suporte para NFSv4,2 recursos opcionais.

Começando com…	NFSv4,2 recursos opcionais incluem …
ONTAP 9.12,1	• Atributos estendidos do NFS • Ficheiros esparsos • Reservas de espaço
ONTAP 9.9,1	Controlo de Acesso obrigatório (MAC) identificado como NFS

Etiquetas de segurança NFS v4,2

A partir do ONTAP 9.9,1, os rótulos de segurança NFS podem ser ativados. Eles são desativados por padrão.

Com os rótulos de segurança NFS v4,2, os servidores ONTAP NFS são cientes do Controle de Acesso

obrigatório (MAC), armazenando e recuperando atributos SEC_label enviados pelos clientes.

Para obter mais informações, "RFC 7240"consulte .

A partir do ONTAP 9.12,1, as etiquetas de segurança NFS v4,2 são compatíveis com operações de despejo NDMP. Se rótulos de segurança forem encontrados em arquivos ou diretórios em versões anteriores, o despejo falhará.

Passos

1. Altere a configuração de privilégios para avançado:

```
set -privilege advanced
```

2. Ativar etiquetas de segurança:

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

Atributos estendidos do NFS

A partir do ONTAP 9.12,1, os atributos estendidos NFS (xattrs) são ativados por padrão.

Atributos estendidos são atributos NFS padrão definidos "RFC 8276" e habilitados em clientes NFS modernos. Eles podem ser usados para anexar metadados definidos pelo usuário a objetos do sistema de arquivos, e são de interesse em implantações de segurança avançadas.

Atributos estendidos NFS não são atualmente suportados para operações de despejo NDMP. Se atributos estendidos forem encontrados em arquivos ou diretórios, o despejo prossegue, mas não faz backup dos atributos estendidos nesses arquivos ou diretórios.

Se você precisar desativar atributos estendidos, use o `vserver nfs modify -v4.2-xattrs disabled` comando.

Suporte ONTAP para NFS paralelo

O ONTAP dá suporte a NFS paralelo (pNFS). O protocolo pNFS oferece melhorias de desempenho ao proporcionar aos clientes acesso direto aos dados de um conjunto de arquivos distribuídos por vários nós de um cluster. Ele ajuda os clientes a localizar o caminho ideal para um volume.

Utilização de suportes rígidos

Ao solucionar problemas de montagem, você precisa ter certeza de que está usando o tipo de montagem correto. O NFS suporta dois tipos de montagem: Suportes macios e suportes rígidos. Você deve usar apenas suportes rígidos por razões de confiabilidade.

Você não deve usar montagens virtuais, especialmente quando houver possibilidade de tempos limite frequentes de NFS. As condições de corrida podem ocorrer como resultado desses tempos limite, o que pode levar à corrupção de dados.

Dependências de nomes de arquivos e diretórios NFS e SMB

Visão geral das dependências de nomes de arquivos e diretórios NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta carateres multibyte em nomes de arquivo, diretório e qtree, dependendo da versão do ONTAP.

Carateres que um nome de arquivo ou diretório pode usar

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (:) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
  - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
  - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

    Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt` , porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
  - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
  - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.

> Se um mapeamento de carateres tiver sido criado usando os comandos SVM CIFS de mapeamento de carateres, uma pesquisa do Windows que normalmente seria insensível a maiúsculas e minúsculas pode se tornar sensível a maiúsculas e minúsculas. Isso significa que as pesquisas de nome de arquivo só serão sensíveis a maiúsculas e minúsculas se o mapeamento de carateres tiver sido criado e o nome de arquivo estiver usando esse mapeamento de carateres.

Como o ONTAP cria nomes de arquivo e diretório

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito carateres ou o limite de extensão de três carateres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis carateres, se o nome exceder seis carateres.
- Ele adiciona um til (…) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

  Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três carateres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Como o ONTAP lida com nomes de arquivos, diretórios e qtree de vários bytes

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem carateres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses carateres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem *utf8mb4* está disponível para as `vserver` famílias de comandos e `volume` .

- Você deve criar um novo volume de uma das seguintes maneiras:
- Definir a opção de volume `-language` explicitamente:

  ```
  volume create -language utf8mb4 {…}
  ```

- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção:

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- Se você estiver usando o ONTAP 9.6 e anteriores, não será possível modificar volumes existentes para suporte a utf8mb4; você deve criar um novo volume pronto para utf8mb4 e migrar os dados usando ferramentas de cópia baseadas em cliente.

  Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o utf8mb4 com uma solicitação de suporte. Para obter mais informações, "O idioma do volume pode ser alterado após a criação no ONTAP?"consulte .

Você pode atualizar SVMs para suporte a utf8mb4, mas os volumes existentes mantêm seus códigos de idioma originais.

E

Nomes LUN com carateres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de carateres Unicode são normalmente representados em aplicações de sistemas de ficheiros Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

  Em versões anteriores ao ONTAP 9.5, nomes incluindo carateres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com carateres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm carateres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

  Para evitar esse problema, use apenas carateres BMP em nomes de arquivo e evite usar carateres suplementares ou atualize para o ONTAP 9.5 ou posterior.

Carateres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir carateres de vários bytes no formato Unicode, como carateres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os carateres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.

Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com carateres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os carateres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para utf8mb4.

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Os clientes NFS podem criar nomes de arquivos que contêm carateres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de carateres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos "':'" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar carateres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo carateres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os carateres NFS inválidos em carateres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de carateres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de carateres em um volume:

- O mapeamento de carateres não é aplicado em pontos de junção.

  Você deve configurar explicitamente o mapeamento de carateres para cada volume de junção.

- Você deve certificar-se de que os carateres Unicode que são usados para representar carateres inválidos ou ilegais são carateres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

  Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "'a-b'" teria sua solicitação mapeada para o nome NFS de "'a:b'" (não o resultado desejado).

- Depois de aplicar o mapeamento de carateres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.

- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de carateres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver carateres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de carateres:

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   O mapeamento consiste em uma lista de pares de carateres fonte-alvo separados por "':'". Os carateres são carateres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C.

   O primeiro valor de cada `mapping_text` par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

   - Mapeamento de origem

     A tabela a seguir mostra o conjunto de carateres Unicode permissível para mapeamento de fontes:

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C	*	Barra invertida
0x3A	:	Cólon
0x2A	*	Asterisco
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	*	Menos de
0x3E	>	Superior a.

0x7C		
Linha vertical	0xB1	±

◦ Mapeamento de alvos

Você pode especificar carateres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000…U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de carateres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Comandos para gerenciar mapeamentos de carateres para a tradução de nome de arquivo SMB

É possível gerenciar o mapeamento de carateres criando, modificando, exibindo informações ou excluindo mapeamentos de carateres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser…	Use este comando…
Criar novos mapeamentos de carateres de arquivo	`vserver cifs character-mapping create`
Exibir informações sobre mapeamentos de carateres de arquivo	`vserver cifs character-mapping show`
Modificar mapeamentos de carateres de arquivo existentes	`vserver cifs character-mapping modify`
Excluir mapeamentos de carateres de arquivo	`vserver cifs character-mapping delete`

Para obter mais informações, consulte a página man para cada comando.

Gerenciar trunking NFS

Saiba mais sobre o entroncamento do ONTAP NFS

A partir do ONTAP 9.14,1, os clientes NFSv4,1 podem aproveitar o entroncamento de sessão para abrir várias conexões a diferentes LIFs no servidor NFS, aumentando assim a velocidade de transferência de dados e fornecendo resiliência por meio de multipathing.

O entroncamento é vantajoso para exportar volumes FlexVol para clientes com capacidade de entroncamento, em particular clientes VMware e Linux, ou para NFS sobre RDMA, TCP ou pNFS.

No ONTAP 9.14,1, o entroncamento é restrito a LIFs em um único nó; o entroncamento não pode abranger LIFs em vários nós.

Os volumes FlexGroup são compatíveis com o entroncamento. Embora isso possa proporcionar melhor desempenho, o acesso multipath a um volume FlexGroup só pode ser configurado em um único nó.

Somente o entroncamento de sessão é suportado para multipathing nesta versão.

Como usar o entroncamento

Para aproveitar os benefícios de vários pathing oferecidos pelo entroncamento, você precisa de um conjunto de LIFs – conhecido como *entroncamento group* – que esteja associado ao SVM que contém um servidor NFS habilitado para entroncamento. Os LIFs em um grupo de entroncamento devem ter portas home no mesmo nó do cluster e devem residir nessas portas home. É uma prática recomendada que todos os LIFs de um grupo de entroncamento sejam membros do mesmo grupo de failover.

O ONTAP suporta até 16 conexões truncadas por nó de um determinado cliente.

Quando um cliente monta exportações de um servidor habilitado para entroncamento, ele especifica um número de endereços IP para LIFs em um grupo de entroncamento. Depois que o cliente se coneta ao primeiro LIF, LIFs adicionais só são adicionados à sessão NFSv4,1 e usados para entroncamento se eles estiverem em conformidade com os requisitos do grupo de entroncamento. Em seguida, o cliente distribui operações NFS pelas várias conexões com base em seu próprio algoritmo (como round-robin).

Para obter a melhor performance, configure o entroncamento em uma SVM dedicada a fornecer exportações de multipath, e não exportações de caminho único. Ou seja, você só deve habilitar o entroncamento em um servidor NFS em um SVM cujas exportações são fornecidas apenas para clientes habilitados para entroncamento.

Clientes suportados

O servidor ONTAP NFSv4,1 suporta entroncamento com qualquer cliente capaz de entroncamento de sessão NFSv4,1.

Os seguintes clientes foram testados com o ONTAP 9.14,1:

- VMware - ESXi 7.0U3F e posterior
- Linux - Red Hat Enterprise Linux (RHEL) 8,8 e 9,3

Quando o entroncamento é ativado em um servidor NFS, os usuários que acessam compartilhamentos exportados em clientes NFS que não suportam entroncamento podem ver uma queda de desempenho. Isso ocorre porque apenas uma única conexão TCP é usada para várias montagens nos LIFs de dados da SVM.

Diferença entre o entroncamento NFS e o nconnect

A partir do ONTAP 9.8, a funcionalidade nconnect está disponível por predefinição quando o NFSv4,1 está ativado. Em clientes compatíveis com nconnect, uma única montagem NFS pode ter várias conexões TCP (até 16) em um único LIF.

Em contraste, o entroncamento é a funcionalidade *multipathing*, que fornece várias conexões TCP sobre vários LIFs. Se você tiver a capacidade de empregar NICs adicionais em seu ambiente, o entroncamento fornece maior paralelismo e desempenho além da capacidade do nconnect.

Saiba mais sobre "nligar."

Configurar um novo servidor NFS e exportar para entroncamento

Criar um servidor NFS habilitado para trunking em um SVM do ONTAP

A partir do ONTAP 9.14,1, o entroncamento pode ser ativado em servidores NFS. O NFSv4,1 é ativado por padrão quando os servidores NFS são criados.

Antes de começar

A criação de um servidor NFS habilitado para trunking requer uma SVM. O SVM precisa ser:

- apoiado por armazenamento suficiente para os requisitos de dados do cliente.
- Habilitado para NFS.

Você pode usar uma SVM existente. No entanto, a ativação do entroncamento requer que todos os clientes NFSv4.x sejam remontados, o que pode ser disruptivo. Se não for possível montar novamente, crie um novo SVM para o servidor NFS.

Passos

1. Se não houver um SVM adequado, crie um:

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. Verifique a configuração e o status do SVM recém-criado:

   ```
   vserver show -vserver svm_name
   ```

   Saiba mais "Criação de um SVM"sobre o .

3. Crie o servidor NFS:

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. Verifique se o NFS está em execução:

```
vserver nfs status -vserver svm_name
```

5. Verifique se o NFS está configurado conforme desejado:

```
vserver nfs show -vserver svm_name
```

Saiba mais sobre "Configuração do servidor NFS."

Depois de terminar

Configure os seguintes serviços conforme necessário:

- "DNS"
- "LDAP"
- "Kerberos"

Prepare sua rede para o entroncamento de NFS do ONTAP

Para aproveitar o entroncamento NFSv4,1, os LIFs em um grupo de entroncamento devem residir no mesmo nó e ter portas iniciais no mesmo nó. As LIFs devem ser configuradas em um grupo de failover no mesmo nó.

Sobre esta tarefa

Um mapeamento individual de LIFs e NICs produz o maior ganho de desempenho, mas não é necessário para habilitar o entroncamento. Ter pelo menos duas NICs instaladas pode oferecer um benefício de desempenho, mas não é necessário.

Você pode ter vários grupos de failover, mas o grupo de failover para o entroncamento deve incluir apenas os LIFS no grupo de entroncamento.

Você deve ajustar o grupo de failover do entroncamento sempre que adicionar ou remover conexões (e NICs subjacentes) de um grupo de failover.

Antes de começar

- Você deve saber os nomes das portas associadas às placas de rede se quiser criar um grupo de failover.
- Todas as portas devem estar no mesmo nó.

Passos

1. Verifique os nomes e o status das portas de rede que você planeja usar:

```
network port status
```

2. Crie o grupo failover:

```
network interface failover-groups create -vserver svm_name -failover-group
failover_group_name -targets ports_list
```

> Não é um requisito ter um grupo de failover, mas é altamente recomendável.

   - *svm_name* É o nome do SVM que contém o servidor NFS.
   - *ports_list* é a lista de portas que serão adicionadas ao grupo failover.

As portas são adicionadas no formato *node_name:port_number*, por exemplo, node1:e0c.

O comando a seguir cria o grupo de failover FG3 para SVM VS1 e adiciona três portas:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Saiba mais sobre "grupos de failover."

3. Se necessário, crie LIFs para membros do grupo de entroncamento:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

   - `-home-node` - O nó para o qual o LIF retorna quando o comando de reversão de interface de rede é executado no LIF.

     Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

   - `-home-port` É a porta física ou lógica à qual o LIF retorna quando o comando de reversão da interface de rede é executado no LIF.
   - Pode especificar um endereço IP com `-address` as opções e `-netmask`, não com a `-subnet` opção.
   - Quando você atribui endereços IP, talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
   - `-service-policy` - A política de serviços para o LIF. Se nenhuma política for especificada, uma política padrão será atribuída automaticamente. Use o `network interface service-policy show` comando para revisar as políticas de serviço disponíveis.
   - `-auto-revert` - Especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é falsa, mas você pode configurá-la como verdadeira dependendo das políticas de gerenciamento de rede em seu ambiente.

     Repita esta etapa para cada LIF no grupo de entroncamento.

     O comando a seguir cria `lif-A` para o SVM `vs1`, na porta `e0c` do nó `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Saiba mais sobre "Criação de LIF."

4. Verifique se os LIFs foram criados:

```
network interface show
```

5. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Crie uma política de exportação de volume ONTAP

Para fornecer acesso de cliente a compartilhamentos de dados, você deve criar um ou mais volumes e o volume deve ter políticas de exportação com pelo menos uma regra.

Requisitos de exportação do cliente:

- Os clientes Linux devem ter uma montagem separada e um ponto de montagem separado para cada conexão de entroncamento (ou seja, para cada LIF).
- Os clientes VMware exigem apenas um único ponto de montagem para um volume exportado, com várias LIFs especificadas.

  Os clientes VMware exigem acesso root na política de exportação.

Passos

1. Criar uma política de exportação:

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   O nome da política pode ter até 256 carateres.

2. Verifique se a política de exportação foi criada:

   ```
   vserver export-policy show -policyname policy_name
   ```

   Exemplo

   Os comandos a seguir criam e verificam a criação de uma política de exportação chamada exp1 no SVM chamado VS1:

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. Crie uma regra de exportação e adicione-a a uma política de exportação existente:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   O `-clientmatch` parâmetro deve identificar os clientes Linux ou VMware compatíveis com entroncamento que montarão a exportação.

   Saiba mais sobre "criando regras de exportação."

4. Crie o volume com um ponto de junção:

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   ```

```
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Saiba mais "criando volumes."

5. Verifique se o volume foi criado com o ponto de junção desejado:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

Montar volumes ONTAP ou compartilhamentos de dados para trunking NFS

Os clientes Linux e VMware que oferecem suporte ao entroncamento podem montar volumes ou compartilhamentos de dados de um servidor ONTAP NFSv4,1 habilitado para entroncamento.

Ao inserir comandos de montagem nos clientes, você deve inserir endereços IP para cada LIF no grupo de entroncamento.

Saiba mais "clientes suportados"sobre .

Requisitos do cliente Linux

Um ponto de montagem separado é necessário para cada conexão no grupo de entroncamento.

Monte os volumes exportados com comandos semelhantes aos seguintes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

O (`vers`valor da versão) deve ser `4.1` ou posterior.

O `max_connect` valor corresponde ao número de conexões no grupo de entroncamento.

Requisitos do cliente VMware

É necessário um comando mount que inclua um endereço IP para cada conexão no grupo de entroncamento.

Monte o datastore exportado com um comando semelhante ao seguinte:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Os `-H` valores correspondem às conexões no grupo entroncamento.

Adaptar as exportações de NFS existentes para o trunking

Adaptar exportações de caminho único para o entroncamento de NFS da ONTAP

Você pode adaptar uma exportação NFSv4,1 de caminho único existente (não truncado) para usar o entroncamento. Os clientes com capacidade para entroncamento podem

aproveitar o desempenho melhorado assim que o entroncamento é ativado no servidor, desde que os pré-requisitos do servidor e do cliente tenham sido satisfeitos.

Adaptar uma exportação de caminho único para o entroncamento permite manter conjuntos de dados exportados em seus volumes e SVMs existentes. Para fazer isso, você deve habilitar o entroncamento no servidor NFS, atualizar a configuração de rede e exportar e remontar o compartilhamento exportado nos clientes.

Ativar o entroncamento tem o efeito de reiniciar o servidor. Os clientes VMware devem remontar os datastores exportados; os clientes Linux devem remontar os volumes exportados com a `max_connect` opção.

Ativar o entroncamento em um servidor ONTAP NFS

O entroncamento deve ser explicitamente ativado em servidores NFS. O NFSv4,1 é ativado por padrão quando os servidores NFS são criados.

Depois de ativar o entroncamento, verifique se os seguintes serviços estão configurados conforme necessário.

- "DNS"
- "LDAP"
- "Kerberos"

Passos

1. Ative o entroncamento e certifique-se de que o NFSv4,1 está ativado:

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. Verifique se o NFS está em execução:
   ```
   vserver nfs status -vserver svm_name
   ```
3. Verifique se o NFS está configurado conforme desejado:

   ```
   vserver nfs show -vserver svm_name
   ```

   Saiba mais sobre "Configuração do servidor NFS.".. Se você estiver atendendo a clientes Windows a partir deste SVM, mova os compartilhamentos e exclua o servidor.
   ```
   vserver cifs show -vserver svm_name
   ```

   E
   ```
   vserver cifs delete -vserver svm_name
   ```

Atualize sua rede para o entroncamento de NFS do ONTAP

O entroncamento NFSv4,1 exige que os LIFs em um grupo de entroncamento residam no mesmo nó e tenham portas iniciais no mesmo nó. Todas as LIFs devem ser configuradas em um grupo de failover no mesmo nó.

Sobre esta tarefa

Um mapeamento individual de LIFs e NICs produz o maior ganho de desempenho, mas não é necessário para habilitar o entroncamento.

Você pode ter vários grupos de failover, mas o grupo de failover para o entroncamento deve incluir apenas os LIFS no grupo de entroncamento.

Você deve ajustar o grupo de failover do entroncamento sempre que adicionar ou remover conexões (e NICs subjacentes) de um grupo de failover.

Antes de começar

- Você deve saber os nomes das portas associadas às placas de rede para criar um grupo de failover.
- Todas as portas devem estar no mesmo nó.

Passos

1. Verifique os nomes e o status das portas de rede que você planeja usar:

   ```
   network port show
   ```

2. Crie um grupo de failover de entroncamento ou modifique um grupo existente para entroncamento:

   ```
   network interface failover-groups create -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   ```
   network interface failover-groups modify -vserver svm_name -failover-group
   failover_group_name -targets ports_list
   ```

   Não é um requisito ter um grupo de failover, mas é altamente recomendável.

   - *svm_name* É o nome do SVM que contém o servidor NFS.
   - *ports_list* é a lista de portas que serão adicionadas ao grupo failover.

     As portas são adicionadas no formato *node_name:port_number*, por exemplo `node1:e0c`, .

     O comando a seguir cria um grupo de failover `fg3` para o SVM VS1 e adiciona três portas:

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   Saiba mais sobre "grupos de failover."

3. Crie LIFs adicionais para membros do grupo de entroncamento conforme necessário:

   ```
   network interface create -vserver svm_name -lif lif_name -home-node node_name
   -home-port port_name -address IP_address -netmask IP_address [-service-policy
   policy] [-auto-revert {true|false}]
   ```

   - `-home-node` - O nó para o qual o LIF retorna quando o comando de reversão de interface de rede é executado no LIF.

     Você pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

   - `-home-port` É a porta física ou lógica à qual o LIF retorna quando o comando de reversão da interface de rede é executado no LIF.

- Pode especificar um endereço IP com `-address` as opções e. `-netmask`
- Quando você atribui endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A página de manual de criação de rota de rede contém informações sobre a criação de uma rota estática em um SVM.
- `-service-policy` - A política de serviços para o LIF. Se nenhuma política for especificada, uma política padrão será atribuída automaticamente. Use o `network interface service-policy show` comando para revisar as políticas de serviço disponíveis.
- `-auto-revert` - Especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. **A configuração padrão é FALSE**, mas você pode configurá-la como verdadeira dependendo das políticas de gerenciamento de rede em seu ambiente.

  Repita esta etapa para cada LIF adicional necessário no grupo de entroncamento.

  O comando a seguir cria lif-A para o SVM VS1, na porta e0c do nó cluster1_01:

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

Saiba mais sobre "Criação de LIF."

4. Verifique se os LIFs foram criados:

   ```
   network interface show
   ```

5. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Modificar políticas de exportação de volume ONTAP

Para permitir que os clientes aproveitem o entroncamento para compartilhamentos de dados existentes, talvez seja necessário modificar políticas e regras de exportação e os volumes aos quais estão anexados. Existem diferentes requisitos de exportação para clientes Linux e datastores VMware.

Requisitos de exportação do cliente:

- Os clientes Linux devem ter uma montagem separada e um ponto de montagem separado para cada conexão de entroncamento (ou seja, para cada LIF).

  Se você estiver atualizando para o ONTAP 9.14,1 e já tiver exportado um volume, poderá continuar a usar esse volume em um grupo de entroncamento.

- Os clientes VMware exigem apenas um único ponto de montagem para um volume exportado, com várias LIFs especificadas.

Os clientes VMware exigem acesso root na política de exportação.

Passos

1. Verifique se uma política de exportação existente está em vigor:

   ```
   vserver export-policy show
   ```

2. Verifique se as regras de política de exportação existentes são apropriadas para a configuração do entroncamento:

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   Em particular, verifique se o `-clientmatch` parâmetro identifica corretamente os clientes Linux ou VMware compatíveis com entroncamento que montarão a exportação.

   Se forem necessários ajustes, modifique a regra usando o `vserver export-policy rule modify` comando ou crie uma nova regra:

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   Saiba mais sobre "criando regras de exportação."

3. Verifique se os volumes exportados existentes estão online:

   ```
   volume show -vserver svm_name
   ```

Remontagem de volumes de ONTAP ou compartilhamentos de dados para trunking NFS

Para converter conexões de cliente não truncadas em conexões truncadas, as montagens existentes nos clientes Linux e VMware devem ser desmontadas e remontadas usando informações sobre LIFs.

Ao inserir comandos de montagem nos clientes, você deve inserir endereços IP para cada LIF no grupo de entroncamento.

Saiba mais "clientes suportados"sobre .

> A desinstalação de clientes VMware causa interrupções em todas as VMs no datastore. Uma alternativa seria criar um novo datastore habilitado para entroncamento e usar **Storage vmotion** para mover suas VMs do datastore antigo para o novo. Consulte a documentação da VMware para obter detalhes.

Requisitos do cliente Linux

Um ponto de montagem separado é necessário para cada conexão no grupo de entroncamento.

Monte os volumes exportados com comandos semelhantes aos seguintes:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2

mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

O `vers` valor deve ser `4.1` ou posterior.

O `max_connect` valor deve corresponder ao número de conexões no grupo de entroncamento.

Requisitos do cliente VMware

É necessário um comando mount que inclua um endereço IP para cada conexão no grupo de entroncamento.

Monte o datastore exportado com um comando semelhante ao seguinte:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Os `-H` valores devem corresponder às conexões no grupo de entroncamento.

Gerenciar NFS em RDMA

Visão geral de NFS sobre RDMA

O NFS sobre RDMA utiliza adaptadores de rede compatíveis com RDMA, permitindo que os dados sejam copiados diretamente entre a memória do sistema de armazenamento e a memória do sistema host, contornando as interrupções da CPU e a sobrecarga.

As configurações NFS sobre RDMA são projetadas para clientes com workloads sensíveis à latência ou com alta largura de banda, como machine learning e análises. O ONTAP NFS em RDMA pode ser usado para quaisquer workloads baseados em NFS. Além disso, a NVIDIA estendeu o NFS por RDMA para habilitar o armazenamento direto da GPU (GDS). O GDS acelera ainda mais as cargas de trabalho com GPU, ignorando completamente a CPU e a memória principal, usando RDMA para transferir dados entre o sistema de armazenamento e a memória GPU diretamente.

A partir do ONTAP 9.10.1, as configurações NFS sobre RDMA são compatíveis com o protocolo NFSv4,0. Versões subsequentes do ONTAP introduziram suporte para versões adicionais de NFS.

Requisitos

- Certifique-se de que está a executar a versão correta do ONTAP para a versão NFS que pretende utilizar.

Versão de NFS	Suporte à ONTAP
NFSv4.0	ONTAP 9.10,1 e posterior
NFSv4.1	ONTAP 9.14,1 e posterior
NFSv3	ONTAP 9.15,1 e posterior

    - Você pode configurar o NFS através do RDMA com o Gerenciador de sistemas a partir do ONTAP 9.12,1. No ONTAP 9.10,1 e 9.11.1, você precisa usar a CLI para configurar o NFS em RDMA.
- Ambos os nós no par de alta disponibilidade (HA) precisam ter a mesma versão.
- Os controladores do sistema de storage devem suportar RDMA:

Começando em ONTAP…	Os seguintes controladores suportam RDMA…
9.10.1 e mais tarde	• AFF A400 • AFF A700 • AFF A800
ONTAP 9.14,1 e posterior	• Série C da AFF • AFF A900
ONTAP 9.15,1 e posterior	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16,1 e posterior	• AFF A50 • AFF A30 • AFF A20

- As LIFs de dados devem ser configuradas para suportar RDMA.
- Para obter informações sobre o suporte RNIC de destino, consulte o "NetApp Hardware Universe".
- Para obter informações sobre sistemas operacionais cliente compatíveis para NFS sobre RDMA, consulte o "Matriz de interoperabilidade NetApp (IMT)". Para RNICs compatíveis com RoCE v2, consulte a respetiva documentação do fornecedor RNIC.

Os grupos de interfaces não são compatíveis com NFS em RDMA.

Próximas etapas

- Configurar NICs para NFS em RDMA
- Configurar LIFs para NFS em RDMA
- Configurações de NFS para NFS em RDMA

Informações relacionadas

- "RDMA"
- Visão geral do trunking NFS
- "RFC 7530: Protocolo NFS versão 4"
- "RFC 8166: Transporte remoto de acesso direto à memória para chamada de procedimento remoto versão 1"
- "RFC 8167: Chamada de procedimento remoto bidirecional em transportes RPC-over-RDMA"
- "RFC 8267: Vinculação de camada superior NFS para RPC-over-RDMA versão 1"

Configurar NICs para NFS em RDMA

O NFS sobre RDMA requer configuração de NIC para o sistema cliente e plataforma de armazenamento.

Configuração da plataforma de storage

Para obter informações sobre o suporte RNIC de destino, consulte o "NetApp Hardware Universe".

Se você estiver usando uma configuração de alta disponibilidade (HA), ambos os nós devem usar o mesmo RNIC para suportar failover RDMA. A NIC deve ser compatível com RoCE.

- A partir do ONTAP 9.10.1, você pode visualizar uma lista de protocolos de descarga RDMA com o comando:

```
network port show -rdma-protocols roce
```

- A partir do ONTAP 9.16.1, recomenda-se o uso do controle de fluxo de prioridade (PFC). Configure o PFC usando o `network port modify` comando:

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- Antes do ONTAP 9.16.1, recomenda-se a utilização do controlo de fluxo global predefinido (GFC). Se a configuração de controle de fluxo tiver sido alterada, configure o GFC usando o `network port modify` comando:

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

Configuração do sistema cliente

Para obter informações sobre sistemas operacionais cliente compatíveis para NFS sobre RDMA, consulte o "Matriz de interoperabilidade NetApp (IMT)". Para RNICs compatíveis com RoCE v2, consulte a respetiva documentação do fornecedor RNIC.

Embora o cliente e o servidor possam ser conetados diretamente, o uso de switches é recomendado para melhorar o desempenho do failover.

O cliente, o servidor, todos os switches e todas as portas nos switches devem ser configurados usando quadros jumbo. A configuração de controle de fluxo nos clientes e switches deve corresponder à configuração de controle de fluxo do ONTAP. A partir do ONTAP 9.16.1, é prática recomendada ativar e configurar o controle de fluxo de prioridade no ONTAP, nos switches e nos clientes. Antes do ONTAP 9.16.1, recomenda-se a utilização de controlo de fluxo global.

Depois que essa configuração for confirmada, você poderá montar a exportação NFS usando RDMA.

System Manager

Você deve estar usando o ONTAP 9.12,1 ou posterior para configurar interfaces de rede com o NFS através do RDMA usando o Gerenciador de sistemas.

Passos

1. Verifique se o RDMA é suportado. Navegue até **rede > portas Ethernet** e selecione o nó apropriado na exibição de grupo. Quando você expandir o nó, observe o campo **protocolos RDMA** para uma determinada porta: O valor **RoCE** indica que RDMA é suportado; um traço (**-**) indica que não é suportado.
2. Para adicionar uma VLAN, selecione * VLAN*. Selecione o nó apropriado. No menu suspenso **Port**, as portas disponíveis exibem o texto **RoCE Enabled** se suportarem RDMA. Nenhum texto é exibido se eles não suportarem RDMA.
3. Siga o fluxo de trabalho em Ative o storage nas para servidores Linux usando NFS para configurar um novo servidor NFS.

   Ao adicionar interfaces de rede, você terá a opção de selecionar **usar portas RoCE**. Selecione esta opção para todas as interfaces de rede que você deseja usar NFS sobre RDMA.

CLI

1. Verifique se o acesso RDMA está ativado no servidor NFS com o comando:

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   Por padrão, `-rdma` deve estar habilitado. Se não estiver, ative o acesso RDMA no servidor NFS:

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. Monte o cliente via NFSv4,0 através de RDMA:
   a. A entrada para o parâmetro proto depende da versão do protocolo IP do servidor. Se for IPv4, use `proto=rdma`. Se for IPv6, use `proto=rdma6`.
   b. Especifique a porta de destino NFS como `port=20049` em vez da porta padrão 2049:

   ```
   mount -o vers=4,minorversion=0,proto=rdma,port=20049
   <Server_IP_address>:/<volume_path> <mount_point>
   ```

3. **OPCIONAL**: Se você precisar desmontar o cliente, execute o comando `unmount <mount_path>`

Mais informações

- Crie um servidor NFS
- Ative o storage nas para servidores Linux usando NFS

Configurar LIFs para NFS em RDMA

Para utilizar NFS sobre RDMA, você deve configurar seus LIFs (interface de rede) para serem compatíveis com RDMA. Tanto o LIF quanto seu par de failover devem ser capazes de suportar RDMA.

Crie um novo LIF

System Manager

Você deve estar executando o ONTAP 9.12,1 ou posterior para criar uma interface de rede para NFS através do RDMA com o Gerenciador de sistemas.

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. + Add Selecione .
3. Quando você seleciona **NFS, SMB/CIFS,S3**, você tem a opção **usar portas RoCE**. Marque a caixa de seleção **Use RoCE Ports**.
4. Selecione a VM de armazenamento e o nó inicial. Atribua um **Nome**, **endereço IP** e **máscara de sub-rede**.
5. Depois de inserir o endereço IP e a máscara de sub-rede, o System Manager filtra a lista de domínios de broadcast para aqueles que têm portas compatíveis com RoCE. Selecione um domínio de broadcast. Opcionalmente, você pode adicionar um gateway.
6. Selecione **Guardar**.

CLI

Passos

1. Criar um LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - A política de serviço deve ser arquivos de dados padrão ou uma política personalizada que inclua o serviço de interface de rede data nfs.
   - O `-rdma-protocols` parâmetro aceita uma lista, que é por padrão vazia. Quando `roce` é adicionado como um valor, o LIF só pode ser configurado em portas que suportam descarga RoCE, afetando a migração de bot LIF e o failover.

Modificar um LIF

System Manager

Você deve estar executando o ONTAP 9.12,1 ou posterior para criar uma interface de rede para NFS através do RDMA com o Gerenciador de sistemas.

Passos

1. Selecione **rede > Visão geral > interfaces de rede**.
2. Selecione **> Editar** ao lado da interface de rede que deseja alterar.
3. Marque **Use RoCE Ports** para habilitar o NFS em RDMA ou desmarque a caixa para desativá-lo. Se a interface de rede estiver em uma porta compatível com RoCE, você verá uma caixa de seleção ao lado de **usar portas RoCE**.
4. Modifique as outras definições conforme necessário.
5. Selecione **Salvar** para confirmar suas alterações.

CLI

1. Você pode verificar o status de seus LIFs com o `network interface show` comando. A política de serviço deve incluir o serviço de interface de rede data nfs. A `-rdma-protocols` lista deve incluir `roce`. Se qualquer uma dessas condições não for verdadeira, modifique o LIF.
2. Para modificar o LIF, execute:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

Modificar um LIF para exigir um determinado protocolo de descarga quando o LIF não está atualmente atribuído a uma porta que suporte esse protocolo produzirá um erro.

Migração de um LIF

O ONTAP também permite migrar interfaces de rede (LIFs) para utilizar o NFS em RDMA. Ao executar essa migração, você deve garantir que a porta de destino seja compatível com RoCE. A partir do ONTAP 9.12,1, pode concluir este procedimento no Gestor de sistema. Ao selecionar uma porta de destino para a interface de rede, o System Manager designará se as portas são compatíveis com RoCE.

Você só pode migrar um LIF para uma configuração NFS por RDMA se:

- É uma interface de rede NFS RDMA (LIF) hospedada em uma porta compatível com RoCE.
- É uma interface de rede TCP NFS (LIF) hospedada em uma porta compatível com RoCE.
- É uma interface de rede TCP NFS (LIF) hospedada em uma porta não compatível com RoCE.

Para obter mais informações sobre como migrar uma interface de rede, Migração de um LIFconsulte .

Mais informações

- Crie um LIF
- Crie um LIF
- Modificar um LIF

- Migração de um LIF

Modificar a configuração NFS

Na maioria dos casos, você não precisa modificar a configuração da VM de storage habilitada por NFS para NFS em RDMA.

Se você está, no entanto, lidando com problemas relacionados a chips de Mellanox e migração de LIF, você deve aumentar o período de graça de bloqueio de NFSv4. Por padrão, o período de carência é definido como 45 segundos. A partir de ONTAP 9.10,1, o período de carência tem um valor máximo de 180 (segundos).

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Introduza o seguinte comando:

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

Para obter mais informações sobre esta tarefa, Especifique o período de tolerância de bloqueio NFSv4consulte .

Configure o SMB com a CLI

Visão geral da configuração SMB com a CLI

Você pode usar os comandos de CLI do ONTAP 9 para configurar o acesso de cliente SMB a arquivos contidos em um novo volume ou qtree em um SVM novo ou existente.

> *SMB* (bloco de mensagens de servidor) refere-se aos dialetos modernos do protocolo Common Internet File System (CIFS). Você ainda verá *CIFS* na interface de linha de comando (CLI) do ONTAP e nas ferramentas de gerenciamento do OnCommand.

Use estes procedimentos se quiser configurar o acesso SMB a um volume ou qtree da seguinte maneira:

- Você deseja usar SMB versão 2 ou posterior.
- Você deseja atender apenas clientes SMB, não clientes NFS (não uma configuração multiprotocolo).
- As permissões de arquivo NTFS serão usadas para proteger o novo volume.
- Você tem o administrador de clusters Privileges, e não o Privileges do administrador da SVM.

  Os Privileges do administrador de cluster são necessários para criar SVMs e LIFs. Os Privileges de administrador do SVM são suficientes para outras tarefas de configuração de SMB.

- Você deseja usar a CLI, não o System Manager ou uma ferramenta de script automatizado.

  Para usar o System Manager para configurar o acesso multiprotocolo nas, "Provisionar storage nas para Windows e Linux usando NFS e SMB"consulte .

- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.

Detalhes sobre a sintaxe de comando estão disponíveis nas páginas de ajuda CLI e man do ONTAP.

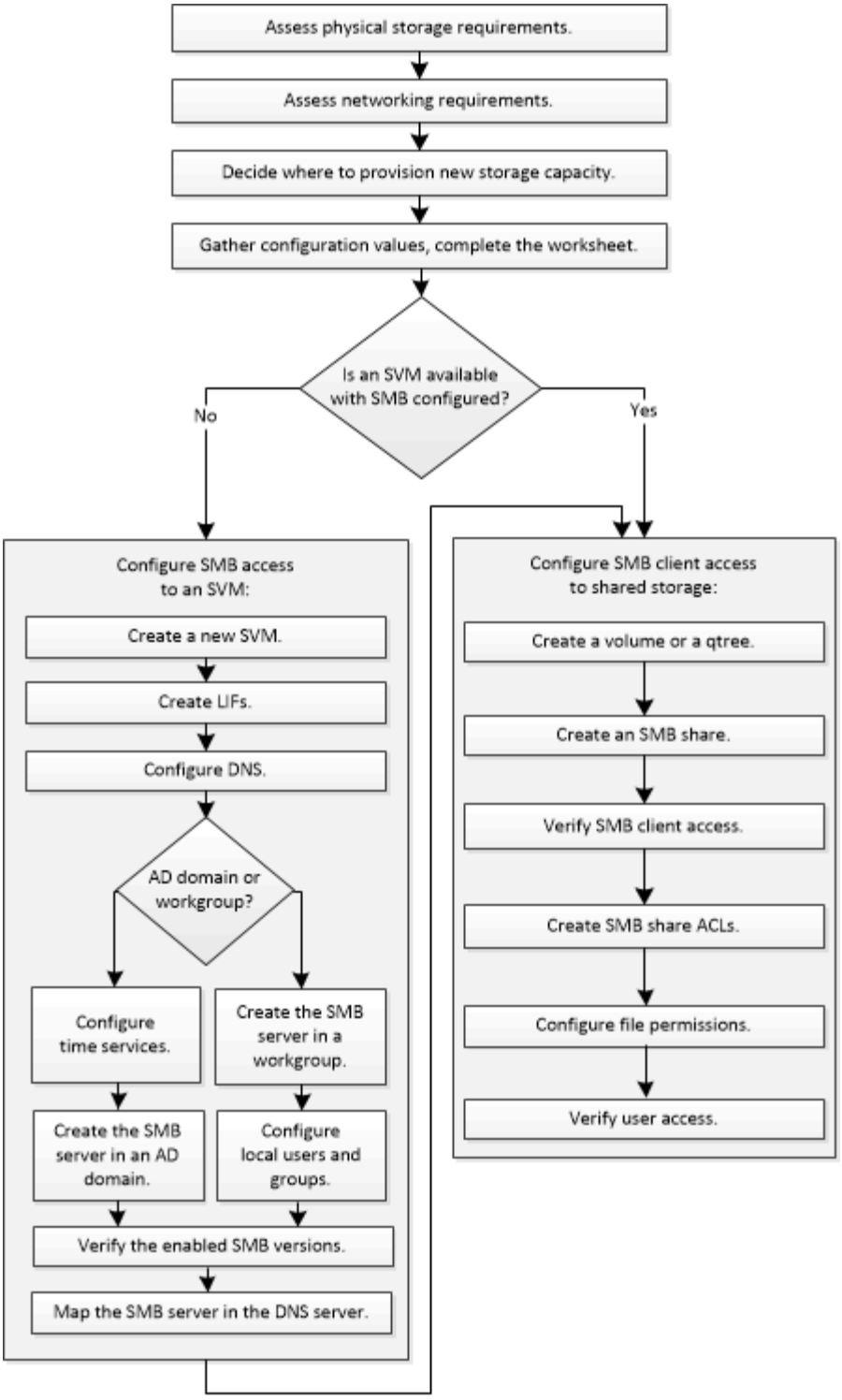
Se pretender obter detalhes sobre a gama de capacidades do protocolo SMB do ONTAP, consulte o "Visão geral de referência SMB".

Outras maneiras de fazer isso em ONTAP

Para executar estas tarefas com…	Consulte…
O Gerenciador de sistema redesenhado (disponível com o ONTAP 9.7 e posterior)	"Provisione storage nas para servidores Windows usando SMB"
System Manager Classic (disponível com o ONTAP 9.7 e versões anteriores)	"Visão geral da configuração SMB"

Fluxo de trabalho de configuração SMB

A configuração do SMB envolve a avaliação dos requisitos de storage físico e rede e, depois, a escolha de um fluxo de trabalho específico para sua meta; a configuração do acesso SMB a uma SVM nova ou existente ou a adição de um volume ou qtree a uma SVM existente que já esteja totalmente configurada para acesso SMB.



Preparação

Avaliar os requisitos de armazenamento físico

Antes de provisionar o storage SMB para clientes, você deve garantir que haja espaço suficiente em um agregado existente para o novo volume. Se não houver, você poderá adicionar discos a um agregado existente ou criar um novo agregado do tipo desejado.

Passos

1. Exibir espaço disponível em agregados existentes: `storage aggregate show`

   Se houver um agregado com espaço suficiente, Registre seu nome na Planilha.

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. Se não houver agregados com espaço suficiente, adicione discos a um agregado existente usando o `storage aggregate add-disks` comando ou crie um novo agregado usando o `storage aggregate create` comando.

Avaliar os requisitos de rede

Antes de fornecer armazenamento SMB aos clientes, você deve verificar se a rede está configurada corretamente para atender aos requisitos de provisionamento SMB.

Antes de começar

Os seguintes objetos de rede de cluster devem ser configurados:

- Portas físicas e lógicas
- Domínios de broadcast
- Sub-redes (se necessário)
- IPspaces (conforme necessário, além do IPspace padrão)
- Grupos de failover (conforme necessário, além do grupo de failover padrão para cada domínio de broadcast)
- Firewalls externos

Passos

1. Exiba as portas físicas e virtuais disponíveis: `network port show`
   - Quando possível, você deve usar a porta com a velocidade mais alta para a rede de dados.
   - Todos os componentes da rede de dados devem ter a mesma configuração de MTU para obter o

melhor desempenho.

2. Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, verifique se a sub-rede existe e tem endereços suficientes disponíveis: `network subnet show`

   As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. As sub-redes são criadas usando o `network subnet create` comando.

3. Exibir IPspaces disponíveis: `network ipspace show`

   Você pode usar o IPspace padrão ou um IPspace personalizado.

4. Se você quiser usar endereços IPv6, verifique se IPv6 está ativado no cluster: `network options ipv6 show`

   Se necessário, você pode ativar o IPv6 usando o `network options ipv6 modify` comando.

Decida onde provisionar nova capacidade de storage SMB

Antes de criar um novo volume ou qtree SMB, você precisa decidir se deve colocá-lo em uma SVM nova ou existente e quanto de configuração o SVM precisa. Esta decisão determina o seu fluxo de trabalho.

Opções

- Se você quiser provisionar um volume ou qtree em um novo SVM ou em um SVM existente que tenha o SMB habilitado, mas não configurado, execute as etapas em ""Configurando o acesso SMB a um SVM"" e "adicionando capacidade de storage a um SVM habilitado para SMB".

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

  Você pode optar por criar um novo SVM se uma das seguintes opções for verdadeira:

  - Você está habilitando o SMB em um cluster pela primeira vez.
  - Você tem SVMs existentes em um cluster no qual não deseja ativar o suporte a SMB.
  - Você tem um ou mais SVMs habilitados para SMB em um cluster e deseja uma das seguintes conexões:
    - Para uma floresta ou grupo de trabalho diferente do ative Directory.
    - Para um servidor SMB em um namespace isolado (cenário de alocação a vários clientes). Você também deve escolher essa opção para provisionar storage em uma SVM existente que tenha SMB habilitado, mas não configurado. Esse pode ser o caso se você criou o SVM para acesso à SAN ou se nenhum protocolo foi habilitado quando o SVM foi criado.

  Depois de ativar o SMB no SVM, proceda ao provisionamento de um volume ou qtree.

- Se você quiser provisionar um volume ou qtree em um SVM existente totalmente configurado para acesso SMB, execute as etapas em ""adicionando capacidade de storage a um SVM habilitado para SMB"".

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

Folha de cálculo para recolher informações de configuração SMB

A folha de cálculo de configuração SMB permite-lhe recolher as informações necessárias para configurar o acesso SMB para clientes.

Você deve completar uma ou ambas as seções da Planilha, dependendo da decisão tomada sobre onde provisionar o armazenamento:

- Se você estiver configurando o acesso SMB a um SVM, deve concluir ambas as seções.

  Configurando o acesso SMB a uma SVM

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

- Se você estiver adicionando capacidade de storage a uma SVM habilitada para SMB, deverá concluir apenas a segunda seção.

  Configurando o acesso de cliente SMB ao armazenamento compartilhado

As páginas de manual do comando contêm detalhes sobre os parâmetros.

Configurando o acesso SMB a uma SVM

Parâmetros para criar um SVM

Você fornece esses valores com o `vserver create` comando se estiver criando um novo SVM.

Campo	Descrição	O seu valor
`-vserver`	Nome fornecido para o novo SVM que é um nome de domínio totalmente qualificado (FQDN) ou que segue outra convenção que impõe nomes exclusivos de SVM em um cluster.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para a nova capacidade de armazenamento SMB.	
`-rootvolume`	Um nome exclusivo fornecido para o volume raiz da SVM.	
`-rootvolume-security-style`	Use o estilo de segurança NTFS para o SVM.	`ntfs`
`-language`	Use a configuração de idioma padrão neste fluxo de trabalho.	`C.UTF-8`

Campo	Descrição	O seu valor
`ipspace`	Opcional: Os IPspaces são espaços de endereço IP distintos nos quais os SVMs residem.	

Parâmetros para criar um LIF

Você fornece esses valores com o `network interface create` comando quando você está criando LIFs.

Campo	Descrição	O seu valor
`-lif`	Um nome que você fornece para o novo LIF.	
`-role`	Use a função de LIF de dados neste fluxo de trabalho.	`data`
`-data-protocol`	Utilize apenas o protocolo SMB neste fluxo de trabalho.	`cifs`
`-home-node`	O nó ao qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-home-port`	A porta ou grupo de interface para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.	
`-address`	O endereço IPv4 ou IPv6 no cluster que será usado para acesso aos dados pelo novo LIF.	
`-netmask`	A máscara de rede e o gateway para o LIF.	
`-subnet`	Um conjunto de endereços IP. Usado em vez `-address` de e `-netmask` para atribuir endereços e netmasks automaticamente.	
`-firewall-policy`	Use a política de firewall de dados padrão neste fluxo de trabalho.	`data`

Campo	Descrição	O seu valor
`-auto-revert`	Opcional: Especifica se um LIF de dados é automaticamente revertido para seu nó inicial na inicialização ou em outras circunstâncias. A predefinição é `false`.	

Parâmetros para resolução de nome de host DNS

Você fornece esses valores com o `vserver services name-service dns create` comando quando você está configurando o DNS.

Campo	Descrição	O seu valor
`-domains`	Até cinco nomes de domínio DNS.	
`-name-servers`	Até três endereços IP para cada servidor de nomes DNS.	

Configurando um servidor SMB em um domínio do ative Directory

Parâmetros para configuração do serviço de tempo

Você fornece esses valores com o `cluster time-service ntp server create` comando quando você está configurando serviços de tempo.

Campo	Descrição	O seu valor
`-server`	O nome do host ou o endereço IP do servidor NTP para o domínio do ative Directory.	

Parâmetros para criar um servidor SMB em um domínio do ative Directory

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar informações de domínio.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	

Campo	Descrição	O seu valor
`-domain`	O nome de domínio totalmente qualificado (FQDN) do domínio do ative Directory a associar ao servidor SMB.	
`-ou`	Opcional: A unidade organizacional dentro do domínio do ative Directory a associar ao servidor SMB. Por padrão, este parâmetro é definido como computadores.	
`-netbios-aliases`	Opcional: Uma lista de aliases NetBIOS, que são nomes alternativos ao nome do servidor SMB.	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Configurando um servidor SMB em um grupo de trabalho

Parâmetros para criar um servidor SMB em um grupo de trabalho

Você fornece esses valores com o `vserver cifs create` comando ao criar um novo servidor SMB e especificar versões SMB compatíveis.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o servidor SMB.	
`-cifs-server`	O nome do servidor SMB (até 15 carateres).	
`-workgroup`	O nome do grupo de trabalho (até 15 carateres).	
`-comment`	Opcional: Um comentário de texto para o servidor. Os clientes Windows podem ver esta descrição do servidor SMB ao navegar em servidores na rede.	

Parâmetros para criar usuários locais

Você fornece esses valores ao criar usuários locais usando o `vserver cifs users-and-groups local-user create` comando. Eles são necessários para servidores SMB em grupos de trabalho e opcionais em domínios do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o usuário local.	
`-user-name`	O nome do utilizador local (até 20 carateres).	
`-full-name`	Opcional: O nome completo do usuário. Se o nome completo contiver um espaço, insira o nome completo entre aspas duplas.	
`-description`	Opcional: Uma descrição para o usuário local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	
`-is-account-disabled`	Opcional: Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.	

Parâmetros para criar grupos locais

Você fornece esses valores ao criar grupos locais usando o `vserver cifs users-and-groups local-group create` comando. Eles são opcionais para servidores SMB em domínios e grupos de trabalho do AD.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o grupo local.	
`-group-name`	O nome do grupo local (até 256 carateres).	
`-description`	Opcional: Uma descrição para o grupo local. Se a descrição contiver um espaço, coloque o parâmetro entre aspas.	

Adição de capacidade de storage a uma SVM habilitada para SMB

Parâmetros para criar um volume

Você fornece esses valores com o `volume create` comando se estiver criando um volume em vez de uma qtree.

Campo	Descrição	O seu valor
`-vserver`	Nome de uma SVM nova ou existente que hospedará o novo volume.	
`-volume`	Um nome descritivo exclusivo que você fornece para o novo volume.	
`-aggregate`	O nome de um agregado no cluster com espaço suficiente para o novo volume SMB.	
`-size`	Um número inteiro fornecido para o tamanho do novo volume.	
`-security-style`	Utilize o estilo de segurança NTFS para este fluxo de trabalho.	`ntfs`
`-junction-path`	Localização sob a raiz (/) onde o novo volume deve ser montado.	

Parâmetros para criar uma qtree

Você fornece esses valores com o `volume qtree create` comando se estiver criando uma qtree em vez de um volume.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual reside o volume que contém a qtree.	
`-volume`	O nome do volume que conterá a nova qtree.	
`-qtree`	Um nome descritivo exclusivo que você fornece para a nova qtree, 64 carateres ou menos.	
`-qtree-path`	O argumento de caminho de qtree no formato `/vol/volume_name/qtree_name\>` pode ser especificado em vez de especificar volume e qtree como argumentos separados.	

Parâmetros para criar compartilhamentos SMB

Você fornece esses valores com o `vserver cifs share create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome do SVM no qual criar o compartilhamento SMB.	
`-share-name`	O nome do compartilhamento SMB que você deseja criar (até 256 carateres).	
`-path`	O nome do caminho para o compartilhamento SMB (até 256 carateres). Esse caminho deve existir em um volume antes de criar o compartilhamento.	
`-share-properties`	Opcional: Uma lista de propriedades de compartilhamento. As predefinições são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.	
`-comment`	Opcional: Um comentário de texto para o servidor (até 256 carateres). Os clientes Windows podem ver esta descrição do compartilhamento SMB ao navegar na rede.	

Parâmetros para criar listas de controle de acesso (ACLs) de compartilhamento SMB

Você fornece esses valores com o `vserver cifs share access-control create` comando.

Campo	Descrição	O seu valor
`-vserver`	O nome da SVM no qual criar a ACL SMB.	
`-share`	O nome do compartilhamento SMB no qual criar.	
`-user-group-type`	O tipo de usuário ou grupo a ser adicionado à ACL do compartilhamento. O tipo padrão é `windows`	`windows`

Campo	Descrição	O seu valor
`-user-or-group`	O usuário ou grupo a adicionar à ACL do compartilhamento. Se você especificar o nome de usuário, você deve incluir o domínio do usuário usando o formato "nome de usuário".	
`-permission`	Especifica as permissões para o usuário ou grupo.	`[No_access
Read	Change	Full_Control]`

Configurar o acesso SMB a uma SVM

Configurar o acesso SMB a uma SVM

Se você ainda não tiver um SVM configurado para acesso de cliente SMB, crie e configure um novo SVM ou configure um SVM existente. A configuração do SMB envolve a abertura do acesso ao volume raiz do SVM, a criação de um servidor SMB, a criação de um LIF, a ativação da resolução do nome de host, a configuração de serviços de nome e, se desejado, a ativação da segurança Kerberos.

Criar um SVM

Se você ainda não tiver pelo menos um SVM em um cluster para fornecer acesso aos dados a clientes SMB, será necessário criar um.

Antes de começar

- A partir do ONTAP 9.13,1, é possível definir uma capacidade máxima para uma VM de armazenamento. Você também pode configurar alertas quando o SVM se aproximar de um nível de capacidade limite. Para obter mais informações, Gerenciar a capacidade do SVMconsulte .

Passos

1. Criar um SVM: `vserver create -vserver` *`svm_name`* `-rootvolume` *`root_volume_name`* `-aggregate` *`aggregate_name`* `-rootvolume-security-style ntfs -language C.UTF-8 -ipspace` *`ipspace_name`*
   - Utilize a definição NTFS para a `-rootvolume-security-style` opção.
   - Utilize a opção C.UTF-8 predefinida `-language`.
   - A `ipspace` definição é opcional.
2. Verifique a configuração e o status do SVM recém-criado: `vserver show -vserver` *`vserver_name`*

   O `Allowed Protocols` campo deve incluir CIFS. Você pode editar esta lista mais tarde.

   O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no IPspace : `ipspaceA`

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação.

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

A partir do ONTAP 9.13,1, é possível definir um modelo de grupo de políticas de QoS adaptável, aplicando um limite mínimo de taxa de transferência e limite máximo a volumes no SVM. Só é possível aplicar essa política depois de criar o SVM. Para saber mais sobre esse processo, Defina um modelo de grupo de políticas adaptávelconsulte .

Verifique se o protocolo SMB está ativado na SVM

Antes de poder configurar e utilizar SMB em SVMs, tem de verificar se o protocolo está ativado.

Sobre esta tarefa

Isso geralmente é feito durante a configuração do SVM, mas se você não ativou o protocolo durante a configuração, poderá ativá-lo mais tarde usando o `vserver add-protocols` comando.

Não é possível adicionar ou remover um protocolo de um LIF depois de criado.

Você também pode desativar protocolos em SVMs usando o `vserver remove-protocols` comando.

Passos

1. Verifique quais protocolos estão atualmente ativados e desativados para o SVM: `vserver show -vserver vserver_name -protocols`

   Você também pode usar o `vserver show-protocols` comando para exibir os protocolos atualmente habilitados em todos os SVMs no cluster.

2. Se necessário, ative ou desative um protocolo:
   - Para ativar o protocolo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
   - Para desativar um protocolo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. Confirme se os protocolos ativados e desativados foram atualizados corretamente: `vserver show -vserver vserver_name -protocols`

Exemplo

O comando a seguir exibe quais protocolos estão atualmente ativados e desativados (permitidos e não permitidos) no SVM chamado VS1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    -----------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

O comando a seguir permite o acesso por SMB adicionando `cifs` à lista de protocolos habilitados no SVM chamado VS1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

Abra a política de exportação do volume raiz da SVM

A política de exportação padrão do volume raiz da SVM deve incluir uma regra para permitir que todos os clientes tenham acesso aberto por meio do SMB. Sem essa regra,

todos os clientes SMB têm acesso negado ao SVM e seus volumes.

Sobre esta tarefa

Quando um novo SVM é criado, uma política de exportação padrão (chamada padrão) é criada automaticamente para o volume raiz do SVM. Você deve criar uma ou mais regras para a política de exportação padrão antes que os clientes possam acessar os dados no SVM.

Você deve verificar se todo o acesso SMB está aberto na política de exportação padrão e, mais tarde, restringir o acesso a volumes individuais criando políticas de exportação personalizadas para volumes individuais ou qtrees.

Passos

1. Se você estiver usando uma SVM existente, verifique a política de exportação de volume raiz padrão: `vserver export-policy rule show`

   A saída do comando deve ser semelhante ao seguinte:

   ```
   cluster::> vserver export-policy rule show -vserver vs1.example.com
   -policyname default -instance

                                      Vserver: vs1.example.com
                                  Policy Name: default
                                   Rule Index: 1
                              Access Protocol: cifs
   Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                               RO Access Rule: any
                               RW Access Rule: any
   User ID To Which Anonymous Users Are Mapped: 65534
                     Superuser Security Types: any
                 Honor SetUID Bits in SETATTR: true
                    Allow Creation of Devices: true
   ```

   Se existir uma regra que permita o acesso aberto, esta tarefa está concluída. Caso contrário, avance para o passo seguinte.

2. Crie uma regra de exportação para o volume raiz da SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verifique a criação de regras usando o `vserver export-policy rule show` comando.

Resultados

Qualquer cliente SMB agora pode acessar qualquer volume ou qtree criado no SVM.

Crie um LIF

Um LIF é um endereço IP associado a uma porta física ou lógica. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, continuando assim a se comunicar com a rede.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

  As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- O mecanismo para especificar o tipo de tráfego Tratado por um LIF foi alterado. Para o ONTAP 9.5 e anteriores, LIFs usaram funções para especificar o tipo de tráfego que ele lidaria. A partir do ONTAP 9.6, os LIFs usam políticas de serviço para especificar o tipo de tráfego que ele lidaria.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- A partir do ONTAP 9.7, se outros LIFs já existirem para o SVM na mesma sub-rede, você não precisará especificar a porta inicial do LIF. O ONTAP escolhe automaticamente uma porta aleatória no nó inicial especificado no mesmo domínio de broadcast que os outros LIFs já configurados na mesma sub-rede.

Passos

1. Criar um LIF:

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

ONTAP 9 .5 e anteriores
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

ONTAP 9 1.6 e posterior
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - O `-role` parâmetro não é necessário ao criar um LIF usando uma política de serviço (começando com ONTAP 9.6).
   - O `-data-protocol` parâmetro não é necessário ao criar um LIF usando uma política de serviço

(começando com ONTAP 9.6). Ao usar o ONTAP 9.5 e anteriores, o `-data-protocol` parâmetro deve ser especificado quando o LIF é criado e não pode ser modificado mais tarde sem destruir e recriar o LIF de dados.

- `-home-node` É o nó para o qual o LIF retorna quando o `network interface revert` comando é executado no LIF.

  Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

  Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.

  > A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "Configurar políticas de firewall para LIFs"consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.

2. Verifique se o LIF foi criado com sucesso:

   ```
   network interface show
   ```

3. Verifique se o endereço IP configurado está acessível:

Para verificar um…	Utilizar…
Endereço IPv4	`network ping`
Endereço IPv6	`network ping6`

Exemplos

O comando a seguir cria um LIF e especifica os valores de endereço IP e máscara de rede usando os `-address` parâmetros e `-netmask`:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

O comando a seguir cria um LIF e atribui valores de endereço IP e máscara de rede da sub-rede especificada (chamado client1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados datalif1 e datalif3 são configurados com endereços IPv4 e o datalif4 é configurado com um endereço IPv6:

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

O comando a seguir mostra como criar um LIF de dados nas atribuído com a `default-data-files` política de serviço:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

Ative DNS para resolução de nome de host

Você pode usar o `vserver services name-service dns` comando para habilitar o DNS em uma SVM e configurá-lo para usar o DNS para resolução de nome de host. Os

nomes de host são resolvidos usando servidores DNS externos.

Antes de começar

Um servidor DNS em todo o site deve estar disponível para pesquisas de nome de host.

Você deve configurar mais de um servidor DNS para evitar um único ponto de falha. O `vserver services name-service dns create` comando emite um aviso se você inserir apenas um nome de servidor DNS.

Sobre esta tarefa

O *Network Management Guide* contém informações sobre a configuração de DNS dinâmico na SVM.

Passos

1. Habilite o DNS na SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   O comando a seguir habilita servidores de servidor DNS externos no SVM VS1:

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   A partir do ONTAP 9.2, o `vserver services name-service dns create` comando executa uma validação automática de configuração e relata uma mensagem de erro se o ONTAP não puder entrar em Contato com o servidor de nomes.

2. Exiba as configurações do domínio DNS usando o `vserver services name-service dns show` comando. ""

   O comando a seguir exibe as configurações DNS para todos os SVMs no cluster:

   ```
   vserver services name-service dns show
                                              Name
   Vserver           State     Domains             Servers
   ----------------- --------- ------------------- -------------
   cluster1          enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   vs1.example.com   enabled   example.com         192.0.2.201,
                                                   192.0.2.202
   ```

   O comando a seguir exibe informações detalhadas de configuração de DNS para SVM VS1:

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. Valide o status dos servidores de nomes usando o `vserver services name-service dns check` comando.

   O `vserver services name-service dns check` comando está disponível a partir de ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

Configure um servidor SMB em um domínio do ative Directory

Configurar serviços de tempo

Antes de criar um servidor SMB em um controlador de domínio ativo, você deve garantir que a hora do cluster e a hora nos controladores de domínio do domínio ao qual o servidor SMB pertencerá correspondem dentro de cinco minutos.

Sobre esta tarefa

Você deve configurar os serviços NTP do cluster para usar os mesmos servidores NTP para sincronização de tempo que o domínio do ative Directory usa.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Passos

1. Configure os serviços de tempo usando o `cluster time-service ntp server create` comando.
   - Para configurar serviços de tempo sem autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address`
   - Para configurar serviços de tempo com autenticação simétrica, digite o seguinte comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`
2. Verifique se os serviços de tempo estão configurados corretamente usando o `cluster time-service ntp server show` comando.

```
cluster time-service ntp server show
```

```
Server                         Version
------------------------------ -------
10.10.10.1                     auto
10.10.10.2                     auto
```

Comandos para gerenciar a autenticação simétrica em servidores NTP

A partir do ONTAP 9.5, o protocolo de tempo de rede (NTP) versão 3 é suportado. O NTPv3 inclui autenticação simétrica usando chaves SHA-1, o que aumenta a segurança da rede.

Para fazer isso…	Use este comando…
Configurar um servidor NTP sem autenticação simétrica	`cluster time-service ntp server create -server server_name`
Configure um servidor NTP com autenticação simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Ativar autenticação simétrica para um servidor NTP existente pode ser modificado para ativar a autenticação adicionando o ID de chave necessária.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configurar uma chave NTP partilhada	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` As chaves compartilhadas são referidas por um ID. O ID, seu tipo e valor devem ser idênticos no nó e no servidor NTP
Configure um servidor NTP com um ID de chave desconhecido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure um servidor com um ID de chave não configurado no servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` O ID, tipo e valor da chave devem ser idênticos ao ID, tipo e valor da chave configurados no servidor NTP.

Para fazer isso…	Use este comando…
Desativar a autenticação simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Crie um servidor SMB em um domínio do ative Directory

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o domínio do ative Directory (AD) ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM e a um controlador de domínio AD do domínio ao qual você deseja ingressar no servidor SMB.

Qualquer usuário autorizado a criar contas de máquina no domínio do AD ao qual você está ingressando no servidor SMB pode criar o servidor SMB no SVM. Isso pode incluir usuários de outros domínios.

A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

Sobre esta tarefa

Ao criar um servidor SMB em um domínio do diretório de atividades:

- Você deve usar o nome de domínio totalmente qualificado (FQDN) ao especificar o domínio.
- A configuração padrão é adicionar a conta de máquina do servidor SMB ao objeto de computador do ative Directory.
- Pode optar por adicionar o servidor SMB a uma unidade organizacional (ou) diferente utilizando a `-ou` opção.
- Opcionalmente, você pode optar por adicionar uma lista delimitada por vírgulas de um ou mais aliases NetBIOS (até 200) para o servidor SMB.

  A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores originais.

As `vserver cifs` páginas man contêm parâmetros opcionais adicionais e requisitos de nomeação.

> A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conetar a um controlador de domínio (DC). Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão.

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas. O ONTAP requer criptografia para comunicações do controlador de domínio quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3. .

"Gerenciamento de SMB" Contém mais informações sobre as opções de configuração do servidor SMB.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um domínio AD: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

   O comando a seguir cria o servidor SMB "ssssmb_server01" no domínio "'example.com`":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   O comando a seguir cria o servidor SMB "ssssmb_server02" no domínio "mydomain.com`" e autentica o administrador do ONTAP com um arquivo keytab:

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   Neste exemplo, o comando output mostra que um servidor SMB chamado "'SMB_SERVER01'" foi criado na SVM vs1.example.com e foi associado ao domínio "'example.com`".

   ```
   cluster1::> vserver cifs show -vserver vs1

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                              Authentication Style: domain
                 CIFS Server Administrative Status: up
                           CIFS Server Description: -
                           List of NetBIOS Aliases: -
   ```

4. Se desejar, ative a comunicação criptografada com o controlador de domínio (ONTAP 9.8 e posterior): `vserver cifs security modify -vserver svm_name -encryption-required-for-dc -connection true`

Exemplos

O comando a seguir cria um servidor SMB chamado "ssssmb_server02" no SVM vs2.example.com no domínio "'example.com`". A conta da máquina é criada no contentor "'ou-eng, ou-corp, DC-example, DC-com'". Ao servidor SMB é atribuído um alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                        Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

O comando a seguir permite que um usuário de um domínio diferente, neste caso um administrador de um domínio confiável, crie um servidor SMB chamado "sssmb_server03" no SVM vs3.example.com. A `-domain` opção especifica o nome do domínio inicial (especificado na configuração DNS) no qual você deseja criar o servidor SMB. A `username` opção especifica o administrador do domínio confiável.

- Domínio doméstico: example.com
- Domínio confiável: trust.lab.com
- Nome de usuário para o domínio confiável: Administrator1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

Crie arquivos keytab para autenticação SMB

A partir do ONTAP 9.7, o ONTAP oferece suporte à autenticação SVM com servidores do ative Directory (AD) usando arquivos keytab. Os ADMINISTRADORES DE ANÚNCIOS geram um arquivo keytab e o disponibilizam aos administradores do ONTAP como um URI (identificador de recurso uniforme), que é fornecido quando `vserver cifs` os

comandos exigem autenticação Kerberos com o domínio AD.

Os ADMINISTRADORES DE ANÚNCIOS podem criar os arquivos keytab usando o comando padrão do Windows Server `ktpass`. O comando deve ser executado no domínio primário onde a autenticação é necessária. O `ktpass` comando pode ser usado para gerar arquivos keytab somente para usuários de domínio primário; chaves geradas usando usuários de domínio confiável não são suportadas.

Os arquivos keytab são gerados para usuários administrativos específicos do ONTAP. Desde que a senha do usuário administrativo não seja alterada, as chaves geradas para o tipo de criptografia e domínio específicos não serão alteradas. Portanto, um novo arquivo keytab é necessário sempre que a senha do usuário admin é alterada.

São suportados os seguintes tipos de encriptação:

- AES256-SHA1
- DES-CBC-MD5

> O ONTAP não oferece suporte ao tipo de criptografia DES-CBC-CRC.

- RC4-HMAC

AES256 é o tipo de criptografia mais alto e deve ser usado se ativado no sistema ONTAP.

Os arquivos keytab podem ser gerados especificando a senha de administrador ou usando uma senha gerada aleatoriamente. No entanto, a qualquer momento, apenas uma opção de senha pode ser usada, porque uma chave privada específica para o usuário admin é necessária no servidor AD para descriptografar as chaves dentro do arquivo keytab. Qualquer alteração na chave privada para um administrador específico invalidará o arquivo keytab.

Configure um servidor SMB em um grupo de trabalho

Configure um servidor SMB em uma visão geral do grupo de trabalho

A configuração de um servidor SMB como membro em um grupo de trabalho consiste em criar o servidor SMB e, em seguida, criar usuários e grupos locais.

Você pode configurar um servidor SMB em um grupo de trabalho quando a infraestrutura de domínio do Microsoft ative Directory não estiver disponível.

Um servidor SMB no modo de grupo de trabalho suporta apenas autenticação NTLM e não suporta autenticação Kerberos.

Crie um servidor SMB em um grupo de trabalho

Você pode usar o `vserver cifs create` comando para criar um servidor SMB no SVM e especificar o grupo de trabalho ao qual ele pertence.

Antes de começar

Os SVM e LIFs que você está usando para fornecer dados devem ter sido configurados para permitir o protocolo SMB. Os LIFs devem ser capazes de se conetar aos servidores DNS configurados no SVM.

Sobre esta tarefa

Os servidores SMB no modo de grupo de trabalho não suportam os seguintes recursos SMB:

- Protocolo de SMB3 testemunhas
- SMB3 ações da CA
- SQL sobre SMB
- Redirecionamento de pasta
- Perfis de roaming
- Objeto de política de grupo (GPO)
- Serviço de Snapshot de volume (VSS)

As `vserver cifs` páginas man contêm parâmetros de configuração opcionais adicionais e requisitos de nomenclatura.

Passos

1. Verifique se o SMB está licenciado no cluster: `system license show -package cifs`

   A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

   Não é necessária uma licença CIFS se o servidor SMB for utilizado apenas para autenticação.

2. Crie o servidor SMB em um grupo de trabalho: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

   O comando a seguir cria o servidor SMB "ssssmb_server01" no grupo de trabalho "'workgroup01":

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. Verifique a configuração do servidor SMB usando o `vserver cifs show` comando.

   No exemplo a seguir, o comando output mostra que um servidor SMB chamado "sssmb_server01" foi criado na SVM vs1.example.com no grupo de trabalho "'workgroup01"":

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                      Fully Qualified Domain Name: -
                              Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

Depois de terminar

Para um servidor CIFS em um grupo de trabalho, você deve criar usuários locais e, opcionalmente, grupos locais, no SVM.

Informações relacionadas

"Gerenciamento de SMB"

Crie contas de usuário locais

Você pode criar uma conta de usuário local que pode ser usada para autorizar o acesso aos dados contidos no SVM em uma conexão SMB. Você também pode usar contas de usuário locais para autenticação ao criar uma sessão SMB.

Sobre esta tarefa

A funcionalidade de usuário local é ativada por padrão quando o SVM é criado.

Ao criar uma conta de usuário local, você deve especificar um nome de usuário e especificar o SVM para associar a conta.

As `vserver cifs users-and-groups local-user` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o usuário local: `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   Os seguintes parâmetros opcionais podem ser úteis:

   - `-full-name`

     O nome completo dos usuários.

   - `-description`

     Uma descrição para o utilizador local.

   - `-is-account-disabled {true|false}`

     Especifica se a conta de usuário está ativada ou desativada. Se este parâmetro não for especificado, o padrão é ativar a conta de usuário.

   O comando solicita a senha do usuário local.

2. Introduza uma palavra-passe para o utilizador local e, em seguida, confirme a palavra-passe.
3. Verifique se o usuário foi criado com sucesso: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir cria um usuário local ""SMB_SERVER01"", com um nome completo ""Sue Chang"", associado ao SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator            Built-in administrator
account
vs1      SMB_SERVER01\sue            Sue Chang
```

Crie grupos locais

É possível criar grupos locais que podem ser usados para autorizar o acesso aos dados associados ao SVM em uma conexão SMB. Você também pode atribuir Privileges que definem quais direitos de usuário ou recursos um membro do grupo tem.

Sobre esta tarefa

A funcionalidade de grupo local é ativada por padrão quando o SVM é criado.

Ao criar um grupo local, você deve especificar um nome para o grupo e especificar o SVM para associar o grupo. Você pode especificar um nome de grupo com ou sem o nome de domínio local e, opcionalmente, especificar uma descrição para o grupo local. Não é possível adicionar um grupo local a outro grupo local.

As `vserver cifs users-and-groups local-group` páginas man contêm detalhes sobre parâmetros opcionais e requisitos de nomeação.

Passos

1. Crie o grupo local: `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   O seguinte parâmetro opcional pode ser útil:

   - `-description`

     Uma descrição para o grupo local.

2. Verifique se o grupo foi criado com sucesso: `vserver cifs users-and-groups local-group show -vserver vserver_name`

Exemplo

O exemplo a seguir cria um grupo local "SMB_SERVER01" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

Depois de terminar

Você deve adicionar membros ao novo grupo.

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Se você não quiser mais que um usuário local, usuário de domínio ou grupo de domínio tenha direitos de acesso ou Privileges com base na associação a um grupo, você pode remover o membro do grupo.

Você deve ter em mente o seguinte ao adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o ONTAP deve ser capaz de resolver o nome para um SID.

Você deve ter em mente o seguinte ao remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- Para remover um membro de um grupo local, o ONTAP deve ser capaz de resolver seu nome para um SID.

Passos

1. Adicione um membro ou remova um membro de um grupo.
   - Adicionar um membro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.

- Remover um membro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

Exemplos

O exemplo a seguir adiciona um usuário local ""SMB_SERVER01"" ao grupo local ""SMB_SERVER01" engenharia" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER01"" e "'SMB_SERVER01' james' do grupo local "'SMB_SERVER01' Engineering" no SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Verifique as versões do SMB ativadas

Sua versão do ONTAP 9 determina quais versões do SMB estão habilitadas por padrão para conexões com clientes e controladores de domínio. Você deve verificar se o servidor SMB oferece suporte aos clientes e às funcionalidades necessárias em seu ambiente.

Sobre esta tarefa

Para conexões com clientes e controladores de domínio, você deve ativar o SMB 2,0 e posterior sempre que possível. Por motivos de segurança, você deve evitar o uso do SMB 1,0 e desativá-lo se tiver verificado que não é necessário no seu ambiente.

No ONTAP 9, as versões 2,0 e posteriores do SMB são ativadas por padrão para conexões de clientes, mas a versão do SMB 1,0 habilitada por padrão depende da versão do ONTAP.

- A partir do ONTAP 9 P8.1, o SMB 1,0 pode ser desativado em SVMs.

  A `-smb1-enabled` opção para o `vserver cifs options modify` comando ativa ou desativa o SMB 1,0.

- Começando com ONTAP 9.3, ele é desativado por padrão em novos SVMs.

Se o servidor SMB estiver em um domínio do ative Directory (AD), você poderá habilitar o SMB 2,0 para se conetar a um controlador de domínio (DC) começando com o ONTAP 9.1. Isso é necessário se você tiver desabilitado o SMB 1,0 em DCs. A partir do ONTAP 9.2, o SMB 2,0 é ativado por padrão para conexões DC.

Se `-smb1-enabled-for-dc-connections` estiver definido como `false` enquanto `-smb1-enabled` estiver definido como `true`, o ONTAP nega conexões SMB 1,0 como cliente, mas continua a aceitar conexões SMB 1,0 de entrada como servidor.

"Gerenciamento de SMB" Contém detalhes sobre as versões e funcionalidades do SMB suportadas.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Verifique quais versões SMB estão ativadas:

```
vserver cifs options show
```

Você pode rolar a lista para baixo para exibir as versões SMB habilitadas para conexões de cliente e, se estiver configurando um servidor SMB em um domínio AD, para conexões de domínio AD.

3. Ative ou desative o protocolo SMB para ligações de clientes, conforme necessário:
   - Para ativar uma versão SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
true
```

Valores possíveis para `smb_version`:

- `-smb1-enabled`
- `-smb2-enabled`
- `-smb3-enabled`
- `-smb31-enabled`

O comando a seguir habilita o SMB 3,1 no SVM vs1.example.com:
`cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - Para desativar uma versão SMB:

```
vserver cifs options modify -vserver <vserver_name> -<smb_version>
false
```

4. Se o servidor SMB estiver em um domínio do ative Directory, ative ou desative o protocolo SMB para conexões DC, conforme necessário:
   - Para ativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections true
```

- Para desativar uma versão SMB:

```
vserver cifs security modify -vserver <vserver_name> -smb2-enabled
-for-dc-connections false
```

5. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Mapeie o servidor SMB no servidor DNS

O servidor DNS do seu site deve ter uma entrada apontando o nome do servidor SMB e quaisquer aliases NetBIOS para o endereço IP do LIF de dados para que os usuários do Windows possam mapear uma unidade para o nome do servidor SMB.

Antes de começar

Você deve ter acesso administrativo ao servidor DNS do seu site. Se não tiver acesso administrativo, deverá pedir ao administrador DNS para executar esta tarefa.

Sobre esta tarefa

Se você usar aliases NetBIOS para o nome do servidor SMB, é uma prática recomendada criar pontos de entrada de servidor DNS para cada alias.

Passos

1. Inicie sessão no servidor DNS.
2. Criar entradas de pesquisa direta (A - Registro de endereço) e inversa (PTR - Registro de ponteiro) para mapear o nome do servidor SMB para o endereço IP do LIF de dados.
3. Se você usar aliases NetBIOS, crie uma entrada de pesquisa de nome canônico Alias (CNAME resource record) para mapear cada alias para o endereço IP do LIF de dados do servidor SMB.

Resultados

Depois que o mapeamento é propagado pela rede, os usuários do Windows podem mapear uma unidade para o nome do servidor SMB ou seus aliases NetBIOS.

Configurar o acesso de cliente SMB ao armazenamento partilhado

Configurar o acesso de cliente SMB ao armazenamento partilhado

Para fornecer acesso de cliente SMB ao storage compartilhado em uma SVM, você precisa criar um volume ou qtree para fornecer um contêiner de storage e, em seguida, criar ou modificar um compartilhamento para esse contêiner. Em seguida, você pode configurar permissões de compartilhamento e arquivo e testar o acesso a partir de

sistemas cliente.

Antes de começar

- O SMB deve estar completamente configurado no SVM.
- Todas as atualizações da configuração dos serviços de nome devem estar concluídas.
- Quaisquer adições ou modificações a um domínio do ative Directory ou configuração de grupo de trabalho devem estar concluídas.

Crie um volume ou um contêiner de storage de qtree

Crie um volume

Você pode criar um volume e especificar seu ponto de junção e outras propriedades usando o `volume create` comando.

Sobre esta tarefa

Um volume deve incluir um *caminho de junção* para que seus dados sejam disponibilizados aos clientes. Você pode especificar o caminho de junção ao criar um novo volume. Se você criar um volume sem especificar um caminho de junção, será necessário *montar* o volume no namespace SVM usando o `volume mount` comando.

Antes de começar

- O SMB deve ser configurado e executado.
- O estilo de segurança da SVM deve ser NTFS.
- A partir do ONTAP 9.13,1, você pode criar volumes com análise de capacidade e acompanhamento de atividades habilitados. Para ativar o acompanhamento de capacidade ou atividade, emita o `volume create` comando com `-analytics-state` ou `-activity-tracking-state` defina como `on`.

  Para saber mais sobre análise de capacidade e acompanhamento de atividades, "Ative a análise do sistema de ficheiros" consulte .

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`svm_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path` *`junction_path`*`]`

   As opções para `-junction-path` são as seguintes:

   - Diretamente sob a raiz, por exemplo, `/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado diretamente no volume raiz da SVM.

   - Em um diretório existente, por exemplo, `/existing_dir/new_vol`

     Você pode criar um novo volume e especificar que ele seja montado em um volume existente (em uma hierarquia existente), expresso como um diretório.

   Se você quiser criar um volume em um novo diretório (em uma nova hierarquia em um novo volume), por exemplo, `/new_dir/new_vol` será necessário criar primeiro um novo volume pai que seja juntado ao

volume raiz SVM. Em seguida, você criaria o novo volume filho no caminho de junção do novo volume pai (novo diretório).

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction`

Exemplos

O comando a seguir cria um novo volume chamado users1 no SVM vs1.example.com e no agregado aggr1. O novo volume é disponibilizado em `/users`. O volume tem 750 GB de tamanho e sua garantia de volume é do tipo volume (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

O comando a seguir cria um novo volume chamado "'home4" na SVM"'vs1.example.com`'" e o agregado "'aggr1". O diretório `/eng/` já existe no namespace para o VS1 SVM, e o novo volume é disponibilizado no `/eng/home`, que se torna o diretório home do `/eng/` namespace. O volume é de 750 GB de tamanho e sua garantia de volume é do tipo `volume` (por padrão).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

Crie uma qtree

Você pode criar uma qtree para conter seus dados e especificar suas propriedades usando o `volume qtree create` comando.

Antes de começar

- O SVM e o volume que conterá a nova qtree já devem existir.
- O estilo de segurança da SVM deve ser NTFS e o SMB deve ser configurado e executado.

Passos

1. Crie a qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   Você pode especificar o volume e a qtree como argumentos separados ou especificar o argumento de caminho de qtree no formato `/vol/volume_name/_qtree_name`.

2. Verifique se a qtree foi criada com o caminho de junção desejado: `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

Exemplo

O exemplo a seguir cria uma qtree chamada qt01 localizada no SVM vs1.example.com que tem um caminho de junção `/vol/data1` :

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

Requisitos e considerações para criar um compartilhamento SMB

Antes de criar um compartilhamento SMB, você deve entender os requisitos para caminhos de compartilhamento e propriedades de compartilhamento, especialmente para diretórios base.

Criar um compartilhamento SMB implica especificar uma estrutura de caminho de diretório (usando a `-path` opção no `vserver cifs share create` comando) que os clientes acessarão. O caminho do diretório corresponde ao caminho de junção de um volume ou qtree que você criou no namespace SVM. O caminho do diretório e o caminho de junção correspondente devem existir antes de criar seu compartilhamento.

Os caminhos de compartilhamento têm os seguintes requisitos:

- Um nome de caminho de diretório pode ter até 255 carateres.
- Se houver um espaço no nome do caminho, toda a cadeia de carateres deve ser colocada em aspas (por

exemplo, "`/new volume/mount here`").

- Se o caminho UNC (`\\servername\sharename\filepath`) do compartilhamento contiver mais de 256 carateres (excluindo o "\" inicial no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível.

  Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 carateres.

Os padrões de propriedade de compartilhamento podem ser alterados:

- As propriedades iniciais padrão para todos os compartilhamentos são `oplocks`, `browsable`, `changenotify` e `show-previous-versions`.
- É opcional especificar propriedades de compartilhamento quando você cria um compartilhamento.

  No entanto, se você especificar propriedades de compartilhamento ao criar o compartilhamento, os padrões não serão usados. Se você usar o `-share-properties` parâmetro ao criar um compartilhamento, especifique todas as propriedades de compartilhamento que deseja aplicar ao compartilhamento usando uma lista delimitada por vírgulas.

- Para designar um compartilhamento de diretório base, use a `homedirectory` propriedade.

  Este recurso permite configurar um compartilhamento que mapeia para diferentes diretórios com base no usuário que se coneta a ele e um conjunto de variáveis. Em vez de ter que criar compartilhamentos separados para cada usuário, você pode configurar um único compartilhamento com alguns parâmetros do diretório base para definir a relação de um usuário entre um ponto de entrada (o compartilhamento) e seu diretório inicial (um diretório no SVM).

  ⓘ Não é possível adicionar ou remover esta propriedade depois de criar a partilha.

Os compartilhamentos do diretório base têm os seguintes requisitos:

- Antes de criar diretórios home do SMB, você deve adicionar pelo menos um caminho de pesquisa do diretório home usando o `vserver cifs home-directory search-path add` comando.
- Os compartilhamentos do diretório base especificados pelo valor de `homedirectory` no `-share -properties` parâmetro devem incluir a `%w` variável dinâmica (nome de usuário do Windows) no nome do compartilhamento.

  O nome do compartilhamento pode também conter a `%d` variável dinâmica (nome de domínio) (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, `home1_%w`).

- Se o compartilhamento for usado por administradores ou usuários para se conetar a diretórios home de outros usuários (usando opções para o `vserver cifs home-directory modify` comando), o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (~).

"Gerenciamento de SMB" e `vserver cifs share` as páginas de manual têm informações adicionais.

Crie um compartilhamento SMB

Você deve criar um compartilhamento SMB antes de compartilhar dados de um servidor SMB com clientes SMB. Ao criar um compartilhamento, você pode definir propriedades

de compartilhamento, como designar o compartilhamento como um diretório inicial. Você também pode personalizar o compartilhamento configurando configurações opcionais.

Antes de começar

O caminho do diretório para o volume ou qtree deve existir no namespace SVM antes de criar o compartilhamento.

Sobre esta tarefa

Quando você cria um compartilhamento, a ACL de compartilhamento padrão (permissões de compartilhamento padrão) é `Everyone / Full Control`. Depois de testar o acesso ao compartilhamento, você deve remover a ACL de compartilhamento padrão e substituí-la por uma alternativa mais segura.

Passos

1. Se necessário, crie a estrutura do caminho do diretório para o compartilhamento.

   O `vserver cifs share create` comando verifica o caminho especificado na `-path` opção durante a criação de compartilhamento. Se o caminho especificado não existir, o comando falhará.

2. Crie um compartilhamento SMB associado ao SVM especificado: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verifique se o compartilhamento foi criado:`vserver cifs share show -share-name share_name`

Exemplos

O comando a seguir cria um compartilhamento SMB chamado "'SHARE1" no SVM `vs1.example.com`. Seu caminho de diretório é `/users`, e é criado com propriedades padrão.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

Verifique o acesso do cliente SMB

Você deve verificar se configurou o SMB corretamente acessando e gravando dados no compartilhamento. Você deve testar o acesso usando o nome do servidor SMB e quaisquer aliases NetBIOS.

Passos

1. Faça login em um cliente Windows.
2. Teste o acesso usando o nome do servidor SMB:

   a. No Explorador do Windows, mapeie uma unidade para a partilha no seguinte formato: `\\SMB_Server_Name\Share_Name`

      Se o mapeamento não for bem-sucedido, é possível que o mapeamento DNS ainda não tenha se propagado pela rede. Você deve testar o acesso usando o nome do servidor SMB posteriormente.

      Se o servidor SMB tiver o nome vs1.example.com e o compartilhamento tiver o nome SHARE1, você deverá inserir o seguinte: `\\vs0.example.com\SHARE1`

   b. Na unidade recém-criada, crie um arquivo de teste e exclua o arquivo.

   Você verificou o acesso de gravação ao compartilhamento usando o nome do servidor SMB.

3. Repita a Etapa 2 para qualquer alias NetBIOS.

Criar listas de controle de acesso de compartilhamento SMB

A configuração de permissões de compartilhamento criando listas de controle de acesso (ACLs) para compartilhamentos SMB permite controlar o nível de acesso a um compartilhamento para usuários e grupos.

Antes de começar

Você deve ter decidido quais usuários ou grupos terão acesso ao compartilhamento.

Sobre esta tarefa

Você pode configurar ACLs de nível de compartilhamento usando nomes de usuário ou grupo do Windows locais ou de domínio.

Antes de criar uma nova ACL, você deve excluir a ACL de compartilhamento padrão `Everyone / Full Control` , que representa um risco de segurança.

No modo de grupo de trabalho, o nome de domínio local é o nome do servidor SMB.

Passos

1. Excluir a ACL de compartilhamento padrão:`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um…	Digite o comando…
Usuário do Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`

Se você quiser configurar ACLs usando um…	Digite o comando…
Grupo Windows	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. Verifique se a ACL aplicada ao compartilhamento está correta usando o `vserver cifs share access-control show` comando.

Exemplo

O comando a seguir `Change` dá permissões ao grupo Windows "equipe de vendas" para o compartilhamento "vendas" no vs1.example.com`"SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

Os comandos a seguir `Change` dão permissão ao grupo local do Windows chamado "Tiger Team" e `Full_Control` permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "d.atavol5" no "VS1" SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

Configurar permissões de arquivo NTFS em um compartilhamento

Para habilitar o acesso a arquivos aos usuários ou grupos que têm acesso a um compartilhamento, você deve configurar permissões de arquivo NTFS em arquivos e diretórios nesse compartilhamento a partir de um cliente Windows.

Antes de começar

O administrador que executa esta tarefa deve ter permissões NTFS suficientes para alterar permissões nos objetos selecionados.

Sobre esta tarefa

"Gerenciamento de SMB" E a documentação do Windows contém informações sobre como definir permissões NTFS padrão e avançadas.

Passos

1. Inicie sessão num cliente Windows como administrador.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:

    a. Selecione uma letra **Drive**.

    b. Na caixa **pasta**, digite o nome do servidor SMB que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

    Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\SHARE1`.

Você pode especificar o endereço IP da interface de dados para o servidor SMB em vez do nome do servidor SMB.

c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

4. Selecione o arquivo ou diretório para o qual você deseja definir permissões de arquivo NTFS.
5. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
6. Selecione a guia **Segurança**.

   A guia Segurança exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa permissões para <Object> exibe uma lista de permissões de permissão e negação em vigor para o usuário ou grupo selecionado.

7. Clique em **Editar**.

   A caixa permissões para <Object> será aberta.

8. Execute as ações desejadas:

Se você quiser	Faça o seguinte…
Defina permissões NTFS padrão para um novo usuário ou grupo	a. Clique em **Add**. A janela Selecionar usuário, computadores, contas de serviço ou grupos será exibida. b. Na caixa **Digite os nomes de objeto a selecionar**, digite o nome do usuário ou grupo no qual você deseja adicionar permissão NTFS. c. Clique em **OK**.
Alterar ou remover permissões NTFS padrão de um usuário ou grupo	Na caixa **Group (Grupo) ou User Names (nomes de usuário)**, selecione o usuário ou grupo que deseja alterar ou remover.

9. Execute as ações desejadas:

Se você quiser…	Faça o seguinte
Defina permissões NTFS padrão para um usuário ou grupo novo ou existente	Na caixa **Permissions for <Object>**, selecione as caixas **allow** ou **deny** para o tipo de acesso que você deseja permitir ou não permitir para o usuário ou grupo selecionado.
Remover um usuário ou grupo	Clique em **Remover**.

Se algumas ou todas as caixas de permissão padrão não forem selecionáveis, é porque as permissões são herdadas do objeto pai. A caixa **Special Permissions** não é selecionável. Se estiver selecionado, significa que um ou mais direitos avançados granulares foram definidos para o usuário ou grupo selecionado.

10. Depois de terminar de adicionar, remover ou editar permissões NTFS nesse objeto, clique em **OK**.

Verifique o acesso do usuário

Você deve testar se os usuários configurados podem acessar o compartilhamento SMB e os arquivos nele contidos.

Passos

1. Em um cliente Windows, faça login como um dos usuários que agora tem acesso ao compartilhamento.
2. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
3. Preencha a caixa **Map Network Drive**:
   a. Selecione uma letra **Drive**.
   b. Na caixa **pasta**, digite o nome do compartilhamento que você fornecerá aos usuários.

      Se o nome do servidor SMB for SMB_SERVER01 e o compartilhamento for chamado "'SHARE1", você digitaria `\\SMB_SERVER01\share1`.

   c. Clique em **Finish**.

   A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.
4. Crie um arquivo de teste, verifique se ele existe, escreva texto nele e remova o arquivo de teste.

Gerencie SMB com a CLI

Visão geral da SMB

Os recursos de acesso a arquivos ONTAP estão disponíveis para o protocolo SMB. Você pode habilitar um servidor CIFS, criar compartilhamentos e ativar serviços Microsoft.

SMB (bloco de mensagens de servidor) refere-se aos dialetos modernos do protocolo Common Internet File System (CIFS). Você ainda verá *CIFS* na interface de linha de comando (CLI) do ONTAP e nas ferramentas de gerenciamento do OnCommand.

Suporte ao servidor SMB

Visão geral do suporte ao servidor SMB

Você pode ativar e configurar servidores SMB em máquinas virtuais de armazenamento (SVMs) para permitir que os clientes SMB acessem arquivos no cluster.

- Cada SVM de dados no cluster pode ser vinculado a exatamente um domínio do active Directory.

- Os SVMs de dados não precisam estar vinculados ao mesmo domínio.
- Vários SVMs podem ser vinculados ao mesmo domínio.

Você deve configurar as SVMs e LIFs que você está usando para fornecer dados antes de criar um servidor SMB. Se sua rede de dados não for plana, talvez você também precise configurar IPspaces, domínios de broadcast e sub-redes.

Informações relacionadas

"Gerenciamento de rede"

Modificar servidores SMB

"Administração do sistema"

Versões e funcionalidade SMB compatíveis

O bloco de mensagens de servidor (SMB) é um protocolo de compartilhamento remoto de arquivos usado por clientes e servidores Microsoft Windows. No ONTAP 9, todas as versões SMB são suportadas; no entanto, o suporte padrão ao SMB 1,0 depende da versão do ONTAP. Você deve verificar se o servidor SMB do ONTAP suporta os clientes e a funcionalidade necessária no seu ambiente.

As informações mais recentes sobre quais clientes SMB e controladores de domínio o ONTAP suporta estão disponíveis na *ferramenta Matriz de interoperabilidade*.

O SMB 2,0 e versões posteriores são ativados por padrão para servidores SMB do ONTAP 9 e podem ser ativados ou desativados conforme necessário. A tabela a seguir mostra o suporte ao SMB 1,0 e a configuração padrão.

Funcionalidade SMB 1,0:	**Nestes lançamentos do ONTAP 9:**			
	9,0	9,1	9,2	9,3 e mais tarde
Está ativado por predefinição	Sim	Sim	Sim	Não
Pode ser ativado ou desativado	Não	Sim * 9,1 P8 ou posterior necessário.	Sim	Sim

As configurações padrão para conexões SMB 1,0 e 2,0 para controladores de domínio também dependem da versão do ONTAP. Mais informações estão disponíveis na `vserver cifs security modify` página de manual. Para ambientes com servidores CIFS existentes que executam o SMB 1,0, você deve migrar para uma versão SMB posterior o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

A tabela a seguir mostra quais recursos SMB são suportados em cada versão SMB. Algumas funcionalidades SMB estão ativadas por predefinição e algumas requerem uma configuração adicional.

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
		1,0	2,0	2,1	3,0	3.1.1
Funcionalidade SMB 1,0 legada		X	X	X	X	X
Alças duráveis			X	X	X	X
Operações combinadas			X	X	X	X
Operações assíncronas			X	X	X	X
Tamanhos aumentados do buffer de leitura e gravação			X	X	X	X
Maior escalabilidade			X	X	X	X
Assinatura SMB	X	X	X	X	X	X
Formato de arquivo de fluxo de dados alternativo (ADS)	X	X	X	X	X	X
MTU grande (ativada por predefinição a partir de ONTAP 9.7)	X			X	X	X
Calços de leasing				X	X	X

Esta funcionalidade:	Requer habilitação:	É suportado no ONTAP 9 para estas versões SMB:				
Compartilhamentos disponíveis continuamente	X				X	X
Alças persistentes					X	X
Testemunha					X	X
CRIPTOGRAFIA SMB: AES-128-CCM	X				X	X
Escalabilidade horizontal (exigida pelos compartilhamentos da CA)					X	X
Failover transparente					X	X
Multicanal SMB (começando com ONTAP 9.4)	X				X	X
Integridade de pré-autenticação						X
Failover de cliente de cluster v,2 (CCFv2)						X
Criptografia SMB: AES-128-GCM (começando com ONTAP 9.1)	X					X

Informações relacionadas

Utilizar a assinatura SMB para melhorar a segurança da rede

Definir o nível mínimo de segurança de autenticação do servidor SMB

Configuração da criptografia SMB necessária em servidores SMB para transferências de dados por SMB

"Interoperabilidade do NetApp"

Recursos do Windows não suportados

Antes de usar o CIFS na rede, você precisa estar ciente de certos recursos do Windows que o ONTAP não oferece suporte.

O ONTAP não suporta os seguintes recursos do Windows:

- Sistema de arquivos criptografados (EFS)
- Registo de eventos do NT File System (NTFS) no diário de alterações
- Microsoft File Replication Service (FRS)
- Serviço de Indexação do Microsoft Windows
- Armazenamento remoto por meio do HSM (Hierarchical Storage Management)
- Gerenciamento de cotas de clientes Windows
- Semântica de cota do Windows
- O arquivo LMHOSTS
- Compactação nativa NTFS

Configure os serviços de nomes NIS ou LDAP no SVM

Com o acesso SMB, o mapeamento do usuário para um usuário UNIX é sempre realizado, mesmo quando você acessa dados em um volume de estilo de segurança NTFS. Se você mapear usuários do Windows para usuários UNIX correspondentes cujas informações são armazenadas em armazenamentos de diretório NIS ou LDAP ou se você usar LDAP para mapeamento de nomes, configure esses serviços de nomes durante a configuração SMB.

Antes de começar

Você precisa ter personalizado a configuração do banco de dados dos serviços de nomes para corresponder à infraestrutura do serviço de nomes.

Sobre esta tarefa

Os SVMs usam os bancos de dados ns-switch de serviços de nome para determinar a ordem na qual procurar as fontes para um determinado banco de dados de serviço de nome. A fonte ns-switch pode ser qualquer combinação de `files`, `nis`, ou `ldap`. Para o banco de dados de grupos, o ONTAP tenta obter as associações de grupos de todas as fontes configuradas e, em seguida, usa as informações de associação de grupo consolidado para verificações de acesso. Se uma dessas fontes não estiver disponível no momento da obtenção de informações do grupo UNIX, o ONTAP não poderá obter as credenciais UNIX completas e as verificações de acesso subsequentes poderão falhar. Portanto, você deve sempre verificar se todas as fontes do ns-switch estão configuradas para o banco de dados de grupo nas configurações do ns-switch.

O padrão é fazer com que o servidor SMB mapeie todos os usuários do Windows para o usuário UNIX padrão armazenado no banco de dados local `passwd`. Se você quiser usar a configuração padrão, a configuração de serviços de nome de usuário e grupo NIS ou LDAP UNIX ou mapeamento de usuário LDAP é opcional para o acesso SMB.

Passos

1. Se as informações de usuário, grupo e netgroup UNIX forem gerenciadas por serviços de nome NIS, configure os serviços de nome NIS:

   a. Determine a ordem atual dos serviços de nome usando o `vserver services name-service ns-switch show` comando.

      Neste exemplo, os três bancos de dados (`group`, `passwd` e `netgroup`) que podem ser usados `nis` como uma fonte de serviço de nomes estão usando `files` apenas como uma fonte.

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                  Source
      Vserver         Database       Enabled      Order
      --------------- ------------   ---------    ---------
      vs1             hosts          true         dns,
                                                  files
      vs1             group          true         files
      vs1             passwd         true         files
      vs1             netgroup       true         files
      vs1             namemap        true         files
      ```

      Você deve adicionar a `nis` fonte `group` aos bancos de dados e `passwd`, opcionalmente, ao `netgroup` banco de dados.

   b. Ajuste a ordenação do banco de dados ns-switch do serviço de nomes conforme desejado usando o `vserver services name-service ns-switch modify` comando.

      Para obter a melhor performance, você não deve adicionar um serviço de nomes a um banco de dados de serviços de nomes, a menos que se Planeje configurar esse serviço de nomes no SVM.

      Se você modificar a configuração para mais de um banco de dados de serviço de nome, deverá executar o comando separadamente para cada banco de dados de serviço de nome que deseja modificar.

      Neste exemplo, `nis` e `files` são configurados como fontes para os `group` bancos de dados e `passwd`, nessa ordem. O restante dos bancos de dados do serviço de nomes não foi alterado.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database group
      -sources nis,files vserver services name-service ns-switch modify -vserver
      vs1 -database passwd -sources nis,files
      ```

   c. Verifique se a ordem dos serviços de nome está correta usando o `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                    Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. Crie a configuração do serviço de nomes NIS
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

`vserver services name-service nis-domain create -vserver vs1 -domain example.com -servers 10.0.0.60`

> ⓘ A partir de ONTAP 9.2, o campo `-nis-servers` substitui o `-servers` campo . Este novo campo pode ter um nome de host ou um endereço IP para o servidor NIS.

e. Verifique se o serviço de nomes NIS está configurado corretamente: `vserver services name-service nis-domain show vserver <vserver_name>`

`vserver services name-service nis-domain show vserver vs1`

```
Vserver       Domain              Server
------------- ------------------- ---------------
vs1           example.com         10.0.0.60
```

2. Se as informações de usuário, grupo e netgroup UNIX ou mapeamento de nomes for gerenciado por serviços de nomes LDAP, configure os serviços de nomes LDAP usando as informações localizadas "Gerenciamento de NFS".

Como funciona a configuração do switch do serviço de nomes ONTAP

O ONTAP armazena informações de configuração do serviço de nomes em uma tabela equivalente `/etc/nsswitch.conf` ao arquivo em sistemas UNIX. Você deve entender a função da tabela e como o ONTAP a usa para que você possa configurá-la adequadamente para o seu ambiente.

A tabela de switch de serviço de nome do ONTAP determina quais fontes de serviço de nome o ONTAP consulta para obter informações para um determinado tipo de informações de serviço de nome. O ONTAP mantém uma tabela de switch de serviço de nomes separada para cada SVM.

Tipos de banco de dados

A tabela armazena uma lista de serviços de nomes separada para cada um dos seguintes tipos de banco de dados:

Tipo de banco de dados	Define fontes de serviço de nome para…	Fontes válidas são…
hosts	Conversão de nomes de host para endereços IP	ficheiros, dns
grupo	Procurar informações do grupo de utilizadores	arquivos, nis, ldap
passwd	Procurar informações do utilizador	arquivos, nis, ldap
grupo de rede	Procurar informações do netgroup	arquivos, nis, ldap
namemap	Mapeando nomes de usuários	ficheiros, ldap

Tipos de origem

As fontes especificam qual fonte de serviço de nomes usar para recuperar as informações apropriadas.

Especificar tipo de origem…	Para procurar informações em…	Gerenciado pelas famílias de comando…

ficheiros	Arquivos de origem local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos, conforme especificado na configuração do domínio NIS da SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos, conforme especificado na configuração de cliente LDAP do SVM	`vserver services name-service ldap`
dns	Servidores DNS externos conforme especificado na configuração DNS do SVM	`vserver services name-service dns`

Mesmo que você Planeje usar NIS ou LDAP para acesso a dados e autenticação de administração SVM, você ainda deve incluir `files` e configurar usuários locais como um fallback caso a autenticação NIS ou LDAP falhe.

Protocolos usados para acessar fontes externas

Para acessar os servidores para fontes externas, o ONTAP usa os seguintes protocolos:

Fonte do serviço de nomes externo	Protocolo utilizado para acesso
NIS	UDP
DNS	UDP
LDAP	TCP

Exemplo

O exemplo a seguir exibe a configuração do switch de serviço de nomes para o SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para procurar informações de usuários ou grupos, o ONTAP consulta apenas arquivos de fontes locais. Se a consulta não retornar nenhum resultado, a pesquisa falhará.

Para procurar informações de netgroup, o ONTAP primeiro consulta servidores NIS externos. Se a consulta não retornar nenhum resultado, o arquivo netgroup local será marcado em seguida.

Não há entradas de serviço de nomes para o mapeamento de nomes na tabela para o SVM.svm_1. Portanto, o ONTAP consulta apenas arquivos de origem local por padrão.

Gerenciar servidores SMB

Modificar servidores SMB

Pode mover um servidor SMB de um grupo de trabalho para um domínio do ative Directory, de um grupo de trabalho para outro grupo de trabalho ou de um domínio do ative Directory para um grupo de trabalho utilizando o `vserver cifs modify` comando.

Sobre esta tarefa

Você também pode modificar outros atributos do servidor SMB, como o nome do servidor SMB e o status administrativo. Consulte a página de manual para obter detalhes.

Opções

- Mova o servidor SMB de um grupo de trabalho para um domínio do ative Directory:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Mova o servidor SMB do grupo de trabalho para um domínio do ative Directory: `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=`*`example`* `ou` contentor dentro do *`example`* domínio .com.

  A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

- Mover o servidor SMB de um grupo de trabalho para outro grupo de trabalho:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Modifique o grupo de trabalho para o servidor SMB: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
  ```

- Mova o servidor SMB de um domínio do ative Directory para um grupo de trabalho:

  a. Defina o status administrativo do servidor SMB como `down`.

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. Mova o servidor SMB do domínio do ative Directory para um grupo de trabalho: `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

  ```
  cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
  ```

Para entrar no modo de grupo de trabalho, todos os recursos baseados em domínio devem ser desativados e suas configurações removidas automaticamente pelo sistema, incluindo compartilhamentos continuamente disponíveis, cópias de sombra e AES. No entanto, as ACLs de compartilhamento configuradas por domínio, como "EXAMPLE.COM\userName", não funcionarão corretamente, mas não poderão ser removidas pelo ONTAP. Remova essas ACLs de compartilhamento o mais rápido possível usando ferramentas externas após a conclusão do comando. Se o AES estiver ativado, você poderá ser solicitado a fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para desativá-lo no domínio "example.com".

- Modifique outros atributos usando o parâmetro apropriado do `vserver cifs modify` comando.

Use as opções para personalizar servidores SMB

Opções de servidor SMB disponíveis

É útil saber quais opções estão disponíveis ao considerar como personalizar o servidor SMB. Embora algumas opções sejam para uso geral no servidor SMB, várias são usadas para ativar e configurar a funcionalidade SMB específica. As opções de servidor SMB são controladas com a `vserver cifs options modify` opção.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível de privilégio de administrador:

- **Configurando o valor de tempo limite da sessão SMB**

  Configurar esta opção permite especificar o número de segundos de tempo ocioso antes de uma sessão SMB ser desconetada. Uma sessão ociosa é uma sessão na qual um usuário não tem arquivos ou diretórios abertos no cliente. O valor padrão é de 900 segundos.

- **Configurando o usuário UNIX padrão**

  Configurar esta opção permite especificar o utilizador UNIX predefinido que o servidor SMB utiliza. O ONTAP cria automaticamente um usuário padrão chamado "'pcuser'" (com um UID de 65534), cria um grupo chamado "'pcuser'" (com um GID de 65534) e adiciona o usuário padrão ao grupo "'pcuser'". Quando você cria um servidor SMB, o ONTAP configura automaticamente "'pcuser'" como o usuário UNIX padrão.

- **Configurando o usuário UNIX convidado**

  A configuração desta opção permite especificar o nome de um usuário UNIX ao qual os usuários que fazem login de domínios não confiáveis são mapeados, o que permite que um usuário de um domínio não confiável se conete ao servidor SMB. Por padrão, essa opção não está configurada (não há valor padrão); portanto, o padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor SMB.

- * Ativar ou desativar a execução de concessão de leitura para bits de modo*

  Ativar ou desativar esta opção permite que você especifique se deseja permitir que clientes SMB executem arquivos executáveis com bits de modo UNIX aos quais eles têm acesso de leitura, mesmo quando o bit executável UNIX não está definido. Esta opção está desativada por predefinição.

- **Ativar ou desativar a capacidade de eliminar ficheiros só de leitura de clientes NFS**

Ativar ou desativar esta opção determina se os clientes NFS devem excluir arquivos ou pastas com o conjunto de atributos somente leitura. A semântica de exclusão NTFS não permite a exclusão de um arquivo ou pasta quando o atributo somente leitura é definido. A semântica de exclusão do UNIX ignora o bit somente leitura, usando as permissões do diretório pai para determinar se um arquivo ou pasta pode ser excluído. A configuração padrão é `disabled`, o que resulta em semântica de exclusão NTFS.

- **Configurando endereços de servidor do Windows Internet Name Service**

  Configurar esta opção permite especificar uma lista de endereços de servidor WINS (Serviço de nomes de Internet do Windows) como uma lista delimitada por vírgulas. Você deve especificar endereços IPv4. Os endereços IPv6 não são suportados. Não há valor padrão.

A lista a seguir especifica as opções do servidor SMB que estão disponíveis no nível avançado de privilégio:

- **Concessão de permissões de grupo UNIX para usuários CIFS**

  Configurar esta opção determina se o usuário CIFS de entrada que não é o proprietário do arquivo pode receber a permissão de grupo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `true`, a permissão de grupo será concedida para o arquivo. Se o usuário CIFS não for o proprietário do arquivo de estilo de segurança UNIX e esse parâmetro estiver definido como `false`, as regras UNIX normais serão aplicáveis para conceder a permissão de arquivo. Este parâmetro é aplicável a arquivos de estilo de segurança UNIX que têm permissão definida como `mode bits` e não é aplicável a arquivos com o modo de segurança NTFS ou NFSv4. A predefinição é `false`.

- **Ativar ou desativar o SMB 1,0**

  O SMB 1,0 é desativado por padrão em uma SVM para a qual um servidor SMB é criado no ONTAP 9.3.

  > ⓘ A partir do ONTAP 9.3, o SMB 1,0 é desativado por padrão para novos servidores SMB criados no ONTAP 9.3. Você deve migrar para uma versão SMB mais recente o mais rápido possível para se preparar para melhorias de segurança e conformidade. Contacte o seu representante da NetApp para obter mais informações.

- **Ativar ou desativar o SMB 2.x**

  SMB 2,0 é a versão mínima de SMB que suporta failover de LIF. Se desativar o SMB 2.x, o ONTAP também desativa automaticamente o SMB 3.X.

  O SMB 2,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,0**

  O SMB 3,0 é a versão mínima para SMB compatível com compartilhamentos disponíveis continuamente. O Windows Server 2012 e o Windows 8 são as versões mínimas do Windows que suportam SMB 3,0.

  O SMB 3,0 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- **Ativar ou desativar o SMB 3,1**

  O Windows 10 é a única versão do Windows que suporta SMB 3,1.

  O SMB 3,1 é compatível apenas com SVMs. A opção é ativada por padrão em SVMs

- * Ativar ou desativar a descarga de cópia ODX*

  O descarregamento de cópia ODX é usado automaticamente por clientes Windows que o suportam. Esta opção está ativada por predefinição.

- * Ativar ou desativar o mecanismo de cópia direta para descarga de cópia ODX*

  O mecanismo de cópia direta aumenta o desempenho da operação de descarga de cópia quando os clientes do Windows tentam abrir o arquivo de origem de uma cópia em um modo que impede que o arquivo seja alterado enquanto a cópia está em andamento. Por padrão, o mecanismo de cópia direta está ativado.

- * Ativar ou desativar referências automáticas de nós*

  Com referências automáticas de nós, o servidor SMB refere automaticamente os clientes a um data LIF local para o nó que hospeda os dados acessados através do compartilhamento solicitado.

- **Ativar ou desativar políticas de exportação para SMB**

  Esta opção está desativada por predefinição.

- * Ativar ou desativar usando pontos de junção como pontos de reparação*

  Se esta opção estiver ativada, o servidor SMB expõe pontos de junção para clientes SMB como pontos de reparação. Esta opção é válida apenas para ligações SMB 2.x ou SMB 3,0. Esta opção está ativada por predefinição.

  Esta opção é suportada apenas em SVMs. A opção é ativada por padrão em SVMs

- **Configurando o número máximo de operações simultâneas por conexão TCP**

  O valor padrão é 255.

- **Ativar ou desativar a funcionalidade de grupos e utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- **Ativar ou desativar a autenticação de utilizadores locais do Windows**

  Esta opção está ativada por predefinição.

- * Ativar ou desativar a funcionalidade de cópia de sombra VSS*

  O ONTAP usa a funcionalidade de cópia de sombra para executar backups remotos de dados armazenados usando a solução Hyper-V sobre SMB.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- **Configurando a profundidade do diretório de cópia de sombra**

  A configuração desta opção permite definir a profundidade máxima dos diretórios para criar cópias de sombra ao usar a funcionalidade de cópia de sombra.

  Esta opção é suportada apenas em SVMs e apenas para configurações Hyper-V em SMB. A opção é ativada por padrão em SVMs

- * Ativar ou desativar recursos de pesquisa de vários domínios para mapeamento de nomes*

  Se ativado, quando um usuário UNIX é mapeado para um usuário de domínio do Windows usando um curinga (*) na parte de domínio do nome de usuário do Windows (por exemplo, * / joe), o ONTAP procura o usuário especificado em todos os domínios com confiança bidirecional para o domínio doméstico. O domínio inicial é o domínio que contém a conta de computador do servidor SMB.

  Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Se esta opção estiver ativada e uma lista de preferências estiver configurada, a lista de preferências será utilizada para efetuar pesquisas de mapeamento de nomes de vários domínios.

  O padrão é habilitar pesquisas de mapeamento de nomes de vários domínios.

- **Configurando o tamanho do setor do sistema de arquivos**

  A configuração desta opção permite configurar o tamanho do setor do sistema de arquivos em bytes que o ONTAP reporta para clientes SMB. Existem dois valores válidos para esta opção: `4096` E `512`. O valor padrão é `4096`. Talvez seja necessário definir esse valor `512` se o aplicativo Windows suportar apenas um tamanho de setor de 512 bytes.

- **Ativar ou desativar o controlo de Acesso Dinâmico**

  Ativar esta opção permite proteger objetos no servidor SMB utilizando o controlo de Acesso Dinâmico (DAC), incluindo a utilização de auditoria para encenar políticas de acesso centrais e utilizar objetos de Diretiva de Grupo para implementar políticas de acesso centrais. A opção está desativada por predefinição.

  Esta opção é suportada apenas em SVMs.

- * Definir as restrições de acesso para sessões não autenticadas (restringir anônimo)*

  Definir esta opção determina quais são as restrições de acesso para sessões não autenticadas. As restrições são aplicadas a usuários anônimos. Por padrão, não há restrições de acesso para usuários anônimos.

- * Ativar ou desativar a apresentação de ACLs NTFS em volumes com segurança eficaz UNIX (volumes estilo de segurança UNIX ou volumes mistos estilo de segurança com segurança eficaz UNIX)*

  Ativar ou desativar esta opção determina como a segurança de arquivos em arquivos e pastas com segurança UNIX é apresentada aos clientes SMB. Se ativado, o ONTAP apresenta arquivos e pastas em volumes com segurança UNIX para clientes SMB como tendo segurança de arquivos NTFS com ACLs NTFS. Se desativado, o ONTAP apresenta volumes com segurança UNIX como volumes FAT, sem segurança de arquivos. Por padrão, os volumes são apresentados como tendo segurança de arquivos NTFS com ACLs NTFS.

- * Habilitando ou desativando a funcionalidade de abertura falsa do SMB*

  A ativação dessa funcionalidade melhora o desempenho do SMB 2.x e do SMB 3,0, otimizando como o ONTAP faz solicitações abertas e fechadas ao consultar informações de atributos em arquivos e diretórios. Por padrão, a funcionalidade de abertura falsa do SMB está ativada. Essa opção é útil somente para conexões feitas com SMB 2.x ou posterior.

- * Ativar ou desativar as extensões UNIX*

Ativar esta opção ativa extensões UNIX num servidor SMB. As extensões UNIX permitem que a segurança de estilo POSIX/UNIX seja exibida através do protocolo SMB. Por predefinição, esta opção está desativada.

Se você tiver clientes SMB baseados em UNIX, como clientes Mac OSX, em seu ambiente, você deve habilitar extensões UNIX. A habilitação de extensões UNIX permite que o servidor SMB transmita informações de segurança POSIX/UNIX sobre SMB para o cliente baseado em UNIX, o que converte as informações de segurança em segurança POSIX/UNIX.

- * Ativar ou desativar o suporte para pesquisas de nomes curtos*

  Ativar esta opção permite que o servidor SMB realize pesquisas em nomes curtos. Uma consulta de pesquisa com esta opção ativada tenta corresponder a nomes de arquivo 8,3 juntamente com nomes de arquivo longos. O valor padrão para este parâmetro é `false`.

- * Ativar ou desativar o suporte para publicidade automática de capacidades DFS*

  Ativar ou desativar esta opção determina se os servidores SMB anunciam automaticamente os recursos DFS para clientes SMB 2.x e SMB 3,0 que se conetam a compartilhamentos. O ONTAP usa referências DFS na implementação de links simbólicos para acesso SMB. Se ativado, o servidor SMB sempre anuncia recursos DFS, independentemente de o acesso a links simbólicos estar habilitado. Se estiver desativado, o servidor SMB anunciará os recursos DFS somente quando os clientes se conetarem a compartilhamentos onde o acesso ao link simbólico está habilitado.

- **Configurando o número máximo de créditos SMB**

  A partir do ONTAP 9.4, a configuração da `-max-credits` opção permite limitar o número de créditos a serem concedidos em uma conexão SMB quando clientes e servidor estão executando o SMB versão 2 ou posterior. O valor padrão é 128.

- * Ativar ou desativar o suporte para SMB Multichannel*

  Ativar a `-is-multichannel-enabled` opção no ONTAP 9.4 e versões posteriores permite que o servidor SMB estabeleça várias conexões para uma única sessão SMB quando as NICs apropriadas são implantadas no cluster e em seus clientes. Isso melhora a taxa de transferência e a tolerância a falhas. O valor padrão para este parâmetro é `false`.

  Quando o Multichannel SMB está ativado, você também pode especificar os seguintes parâmetros:

  - O número máximo de conexões permitido por sessão multicanal. O valor padrão para este parâmetro é 32.
  - O número máximo de interfaces de rede anunciadas por sessão multicanal. O valor padrão para este parâmetro é 256.

Configurando opções de servidor SMB

Você pode configurar as opções de servidor SMB a qualquer momento depois de criar um servidor SMB em uma máquina virtual de storage (SVM).

Passo

1. Execute a ação desejada:

Se pretender configurar as opções do servidor SMB…	Digite o comando…
No nível de privilégios de administrador	`vserver cifs options modify -vserver` *`vserver_name options`*
Em nível avançado de privilégios	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

Para obter mais informações sobre como configurar as opções do servidor SMB, consulte a página de manual do `vserver cifs options modify` comando.

Configure a permissão Grant UNIX group para usuários SMB

Você pode configurar essa opção para conceder permissões de grupo para acessar arquivos ou diretórios, mesmo que o usuário SMB de entrada não seja o proprietário do arquivo.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a permissão Grant UNIX group conforme apropriado:

Se você quiser	Introduza o comando
Ative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify –grant-unix-group-perms-to-others true`
Desative o acesso aos arquivos ou diretórios para obter permissões de grupo, mesmo que o usuário não seja o proprietário do arquivo	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Configurar restrições de acesso para usuários anônimos

Por padrão, um usuário anônimo e não autenticado (também conhecido como *null user*) pode acessar certas informações na rede. Você pode usar uma opção de servidor SMB para configurar restrições de acesso para o usuário anônimo.

Sobre esta tarefa

A `-restrict-anonymous` opção servidor SMB corresponde à `RestrictAnonymous` entrada do Registro no Windows.

Os usuários anônimos podem listar ou enumerar certos tipos de informações de sistema de hosts do Windows na rede, incluindo nomes e detalhes de usuários, políticas de conta e nomes de compartilhamento. Você pode controlar o acesso para o usuário anônimo especificando uma das três configurações de restrição de acesso:

Valor	Descrição
`no-restriction` (predefinição)	Não especifica restrições de acesso para usuários anônimos.
`no-enumeration`	Especifica que somente a enumeração é restrita para usuários anônimos.
`no-access`	Especifica que o acesso é restrito para usuários anônimos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração restringir anônimo: `vserver cifs options modify -vserver` *`vserver_name`* `-restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para dados de estilo de segurança UNIX

Gerencie como a segurança de arquivos é apresentada aos clientes SMB para visão geral de dados em estilo de segurança UNIX

Você pode escolher como deseja apresentar a segurança de arquivos a clientes SMB para dados de estilo de segurança UNIX ativando ou desativando a apresentação de ACLs NTFS para clientes SMB. Há vantagens em cada configuração, que você deve entender para escolher a configuração mais adequada para seus requisitos de negócios.

Por padrão, o ONTAP apresenta permissões UNIX em volumes estilo de segurança UNIX para clientes SMB como ACLs NTFS. Existem cenários em que isso é desejável, incluindo o seguinte:

- Você deseja exibir e editar permissões UNIX usando a guia **Segurança** na caixa Propriedades do Windows.

  Não é possível modificar permissões de um cliente Windows se a operação não for permitida pelo sistema UNIX. Por exemplo, você não pode alterar a propriedade de um arquivo que você não possui, porque o sistema UNIX não permite essa operação. Essa restrição impede que clientes SMB ignorem permissões UNIX definidas nos arquivos e pastas.

- Os usuários estão editando e salvando arquivos no volume estilo de segurança UNIX usando certos aplicativos do Windows, por exemplo, Microsoft Office, onde o ONTAP deve preservar permissões UNIX durante operações de salvamento.

- Existem certos aplicativos do Windows no seu ambiente que esperam ler ACLs NTFS em arquivos que usam.

Em certas circunstâncias, você pode querer desativar a apresentação de permissões UNIX como ACLs NTFS. Se esta funcionalidade estiver desativada, o ONTAP apresenta volumes de estilo de segurança UNIX como volumes FAT para clientes SMB. Existem razões específicas pelas quais você pode querer apresentar volumes de estilo de segurança UNIX como volumes FAT para clientes SMB:

- Você só altera permissões UNIX usando montagens em clientes UNIX.

  A guia Segurança não está disponível quando um volume de estilo de segurança UNIX é mapeado em um cliente SMB. A unidade mapeada parece ser formatada com o sistema de arquivos FAT, que não tem permissões de arquivo.

- Você está usando aplicativos sobre SMB que definem ACLs NTFS em arquivos e pastas acessados, o que pode falhar se os dados residirem em volumes de estilo de segurança UNIX.

  Se o ONTAP relatar o volume como FAT, o aplicativo não tenta alterar uma ACL.

Informações relacionadas

Configurando estilos de segurança no FlexVol volumes

Configurando estilos de segurança no qtrees

Ative ou desative a apresentação de ACLs NTFS para dados de estilo de segurança UNIX

Você pode ativar ou desativar a apresentação de ACLs NTFS para clientes SMB para dados de estilo de segurança UNIX (volumes de estilo de segurança UNIX e volumes mistos de estilo de segurança com segurança efetiva UNIX).

Sobre esta tarefa

Se você ativar essa opção, o ONTAP apresenta arquivos e pastas em volumes com estilo de segurança UNIX eficaz para clientes SMB como tendo ACLs NTFS. Se desativar esta opção, os volumes são apresentados como volumes FAT para clientes SMB. O padrão é apresentar ACLs NTFS a clientes SMB.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a configuração da opção ACL NTFS UNIX: `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de

segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

  Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

  Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Gerenciar configurações de segurança do servidor SMB

Como o ONTAP lida com a autenticação de cliente SMB

Antes que os usuários possam criar conexões SMB para acessar dados contidos no SVM, elas devem ser autenticadas pelo domínio ao qual o servidor SMB pertence. O servidor SMB suporta dois métodos de autenticação, Kerberos e NTLM (NTLMv1 ou

NTLMv2). Kerberos é o método padrão usado para autenticar usuários de domínio.

Autenticação Kerberos

O ONTAP oferece suporte à autenticação Kerberos ao criar sessões SMB autenticadas.

Kerberos é o serviço de autenticação principal do ative Directory. O servidor Kerberos, ou serviço KDC (Centro de distribuição de chaves Kerberos), armazena e recupera informações sobre princípios de segurança no ative Directory. Ao contrário do modelo NTLM, os clientes do ative Directory que desejam estabelecer uma sessão com outro computador, como o servidor SMB, contatam diretamente um KDC para obter suas credenciais de sessão.

Autenticação NTLM

A autenticação de cliente NTLM é feita usando um protocolo de resposta de desafio baseado no conhecimento compartilhado de um segredo específico do usuário com base em uma senha.

Se um usuário criar uma conexão SMB usando uma conta de usuário local do Windows, a autenticação é feita localmente pelo servidor SMB usando NTLMv2.

Diretrizes para configurações de segurança de servidor SMB em uma configuração de recuperação de desastres SVM

Antes de criar um SVM configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), você deve saber como as configurações de segurança do servidor SMB são gerenciadas no SVM de destino.

- As configurações de segurança de servidor SMB não padrão não são replicadas para o destino.

  Quando você cria um servidor SMB no SVM de destino, todas as configurações de segurança do servidor SMB são definidas como valores padrão. Quando o destino de recuperação de desastres da SVM é inicializado, atualizado ou ressincido, as configurações de segurança do servidor SMB na origem não são replicadas para o destino.

- Você deve configurar manualmente configurações de segurança de servidor SMB não padrão.

  Se você tiver configurações de segurança de servidor SMB não padrão configuradas no SVM de origem, será necessário configurar manualmente essas mesmas configurações no SVM de destino depois que o destino se tornar leitura-gravação (depois que a relação SnapMirror for interrompida).

Exibir informações sobre as configurações de segurança do servidor SMB

Você pode exibir informações sobre as configurações de segurança do servidor SMB em suas máquinas virtuais de armazenamento (SVMs). Pode utilizar estas informações para verificar se as definições de segurança estão corretas.

Sobre esta tarefa

Uma configuração de segurança exibida pode ser o valor padrão para esse objeto ou um valor não padrão configurado usando a CLI do ONTAP ou usando objetos de diretiva de grupo (GPOs) do ative Directory.

Não use o `vserver cifs security show` comando para servidores SMB no modo de grupo de trabalho, porque algumas das opções não são válidas.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as configurações de segurança em uma SVM especificada	`vserver cifs security show -vserver` *vserver_name*
Configurações ou configurações de segurança específicas no SVM	`vserver cifs security show -vserver` _vserver_name_ `-fields [fieldname,...]` Você pode inserir `-fields ?` para determinar quais campos você pode usar.

Exemplo

O exemplo a seguir mostra todas as configurações de segurança do SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                          Kerberos Clock Skew:        5 minutes
                          Kerberos Ticket Age:        10 hours
                         Kerberos Renewal Age:        7 days
                         Kerberos KDC Timeout:        3 seconds
                          Is Signing Required:        false
               Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:       false
                         LM Compatibility Level:       lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:       false
                        Client Session Security:       none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:         false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:         false
 AES session key enabled for NetLogon channel:         false
  Try Channel Binding For AD LDAP Connections:         false
```

Observe que as configurações exibidas dependem da versão do ONTAP em execução.

O exemplo a seguir mostra a inclinação do relógio Kerberos para SVM VS1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Ative ou desative a complexidade de senha necessária para usuários SMB locais

A complexidade de senha necessária fornece segurança aprimorada para usuários locais de SMB em suas máquinas virtuais de armazenamento (SVMs). A funcionalidade de complexidade de palavra-passe necessária está ativada por predefinição. Você pode desativá-lo e reativá-lo a qualquer momento.

Antes de começar

Usuários locais, grupos locais e autenticação de usuário local devem estar habilitados no servidor CIFS.

Sobre esta tarefa

Não use o `vserver cifs security modify` comando para um servidor CIFS no modo de grupo de trabalho porque algumas das opções não são válidas.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a complexidade de senha necessária para usuários SMB locais seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-password-complexity -required false`

2. Verifique a configuração de segurança para a complexidade necessária da senha: `vserver cifs security show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir mostra que a complexidade de senha necessária está habilitada para usuários SMB locais para SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

Informações relacionadas

Exibindo informações sobre as configurações de segurança do servidor CIFS

Usando usuários locais e grupos para autenticação e autorização

Requisitos para senhas de usuários locais

Alterando senhas de contas de usuário locais

Modifique as configurações de segurança Kerberos do servidor CIFS

Você pode modificar certas configurações de segurança Kerberos do servidor CIFS, incluindo o tempo máximo permitido de distorção do relógio Kerberos, a vida útil do ticket Kerberos e o número máximo de dias de renovação de ticket.

Sobre esta tarefa

Modificar as configurações do Kerberos do servidor CIFS usando o `vserver cifs security modify` comando modifica as configurações somente na máquina virtual de armazenamento (SVM) única que você especificar com o `-vserver` parâmetro. Você pode gerenciar centralmente as configurações de segurança Kerberos para todos os SVMs no cluster que pertencem ao mesmo domínio do ative Directory usando os GPOs (objetos de diretiva de grupo) do ative Directory.

Passos

1. Execute uma ou mais das seguintes ações:

Se você quiser…	Digite…
Especifique o tempo máximo permitido de distorção do relógio Kerberos em minutos (9.13.1 e posterior) ou segundos (9.12.1 ou anterior).	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* A predefinição é 5 minutos.
Especifique a vida útil do ticket Kerberos em horas.	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` A predefinição é 10 horas.

Especifique o número máximo de dias de renovação do ticket.	`vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days` A configuração padrão é de 7 dias.
Especifique o tempo limite para sockets em KDCs após o qual todos os KDCs são marcados como inalcançáveis.	`vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds` A predefinição é 3 segundos.

2. Verifique as configurações de segurança do Kerberos:

   `vserver cifs security show -vserver vserver_name`

Exemplo

O exemplo a seguir faz as seguintes alterações na segurança Kerberos: "'Kerberos Clock Skew'" está definido como 3 minutos e "'Kerberos Ticket Age'" está definido como 8 horas para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
         Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                 false
              Is AES Encryption Enabled:                 false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                 false
```

Informações relacionadas

"Exibindo informações sobre as configurações de segurança do servidor CIFS"

"GPOs compatíveis"

"Aplicando objetos de Diretiva de Grupo a servidores CIFS"

Defina o nível mínimo de segurança de autenticação do servidor SMB

Você pode definir o nível mínimo de segurança do servidor SMB, também conhecido como *LMCompatibilityLevel*, em seu servidor SMB para atender aos requisitos de segurança da sua empresa para acesso ao cliente SMB. O nível mínimo de segurança é o nível mínimo dos tokens de segurança que o servidor SMB aceita de clientes SMB.

Sobre esta tarefa

- Os servidores SMB no modo de grupo de trabalho suportam apenas a autenticação NTLM. A autenticação Kerberos não é suportada.
- LMCompatibilityLevel aplica-se apenas à autenticação de cliente SMB, não à autenticação de administrador.

Você pode definir o nível mínimo de segurança de autenticação para um dos quatro níveis de segurança suportados.

Valor	Descrição
`lm-ntlm-ntlmv2-krb` (predefinição)	A máquina virtual de armazenamento (SVM) aceita segurança de autenticação LM, NTLM, NTLMv2 e Kerberos.
`ntlm-ntlmv2-krb`	O SVM aceita segurança de autenticação NTLM, NTLMv2 e Kerberos. O SVM nega a autenticação LM.
`ntlmv2-krb`	O SVM aceita a segurança de autenticação NTLMv2 e Kerberos. O SVM nega a autenticação LM e NTLM.
`krb`	O SVM aceita apenas a segurança de autenticação Kerberos. O SVM nega a autenticação LM, NTLM e NTLMv2.

Passos

1. Defina o nível mínimo de segurança de autenticação: `vserver cifs security modify -vserver` *`vserver_name`* `-lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verifique se o nível de segurança de autenticação está definido para o nível desejado: `vserver cifs security show -vserver` *`vserver_name`*

Informações relacionadas

Ativar ou desativar a encriptação AES para comunicação baseada no Kerberos

Configurar segurança forte para comunicação baseada no Kerberos usando criptografia AES

Para uma segurança mais forte com comunicação baseada no Kerberos, é possível ativar a criptografia AES-256 e AES-128 no servidor SMB. Por padrão, quando você cria um servidor SMB no SVM, a criptografia AES (Advanced Encryption Standard) é desativada. Você deve habilitá-lo para aproveitar a segurança forte fornecida pela

criptografia AES.

A comunicação relacionada ao Kerberos para SMB é usada durante a criação do servidor SMB na SVM, bem como durante a fase de configuração da sessão SMB. O servidor SMB suporta os seguintes tipos de criptografia para comunicação Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se você quiser usar o tipo de criptografia de segurança mais alto para comunicação Kerberos, ative a criptografia AES para comunicação Kerberos no SVM.

Quando o servidor SMB é criado, o controlador de domínio cria uma conta de máquina de computador no ative Directory. Neste momento, o KDC se torna ciente dos recursos de criptografia da conta de máquina específica. Posteriormente, um tipo de criptografia específico é selecionado para criptografar o ticket de serviço que o cliente apresenta ao servidor durante a autenticação.

A partir do ONTAP 9.12,1, você pode especificar quais tipos de criptografia anunciar no KDC do ative Directory (AD). Pode utilizar a `-advertised-enc-types` opção para ativar os tipos de encriptação recomendados e pode utilizá-la para desativar os tipos de encriptação mais fracos. Aprenda a "Ative e desative os tipos de criptografia para comunicação baseada no Kerberos".

> As novas instruções Intel AES (Intel AES NI) estão disponíveis no SMB 3,0, melhorando o algoritmo AES e acelerando a criptografia de dados com famílias de processadores suportadas.começando com SMB 3,1.1, AES-128-GCM substitui AES-128-CCM como o algoritmo hash usado pela criptografia SMB.

Informações relacionadas

Modificação das configurações de segurança Kerberos do servidor CIFS

Ativar ou desativar a encriptação AES para comunicação baseada no Kerberos

Para aproveitar a segurança mais forte com a comunicação baseada no Kerberos, você deve usar a criptografia AES-256 e AES-128 no servidor SMB. A partir do ONTAP 9.13,1, a encriptação AES é ativada por predefinição. Se você não quiser que o servidor SMB selecione os tipos de criptografia AES para comunicação baseada em Kerberos com o KDC do ative Directory (AD), você pode desativar a criptografia AES.

Se a encriptação AES está ativada por predefinição e se tem a opção de especificar tipos de encriptação depende da versão do ONTAP.

Versão de ONTAP	A encriptação AES está ativada …	Você pode especificar tipos de criptografia?
9.13.1 e mais tarde	Por padrão	Sim
9.12.1	Manualmente	Sim
9.11.1 e anteriores	Manualmente	Não

A partir do ONTAP 9.12,1, a criptografia AES é ativada e desativada usando a `-advertised-enc-types` opção, que permite especificar os tipos de criptografia anunciados para o AD KDC. A configuração padrão é `rc4` e `des`, mas quando um tipo AES é especificado, a criptografia AES é ativada. Você também pode usar a opção para desativar explicitamente os tipos de criptografia RC4 e DES mais fracos. No ONTAP 9.11,1 e anterior, você deve usar a `-is-aes-encryption-enabled` opção para ativar e desativar a criptografia AES e os tipos de criptografia não podem ser especificados.

Para melhorar a segurança, a máquina virtual de armazenamento (SVM) altera a senha da conta de máquina no AD sempre que a opção de segurança AES é modificada. A alteração da senha pode exigir credenciais administrativas do AD para a unidade organizacional (ou) que contém a conta da máquina.

Se um SVM for configurado como um destino de recuperação de desastres em que a identidade não seja preservada (a `-identity-preserve` opção está definida como `false` na configuração do SnapMirror), as configurações de segurança do servidor SMB não padrão não serão replicadas para o destino. Se você ativou a criptografia AES no SVM de origem, será necessário habilitá-la manualmente.

Exemplo 1. Passos

ONTAP 9.12,1 e posterior

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
Desativado	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

   Nota: a `-is-aes-encryption-enabled` opção está obsoleta no ONTAP 9.12,1 e pode ser removida em uma versão posterior.

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

ONTAP 9.11,1 e anteriores

1. Execute uma das seguintes ações:

Se você quiser que os tipos de criptografia AES para comunicação Kerberos sejam…	Digite o comando…
Ativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
Desativado	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. Verifique se a criptografia AES está ativada ou desativada conforme desejado: `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   O `is-aes-encryption-enabled` campo é exibido `true` se a criptografia AES estiver ativada e `false` se estiver desativada.

Exemplos

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

O exemplo a seguir habilita os tipos de criptografia AES para o servidor SMB no SVM VS2. O administrador é solicitado a inserir as credenciais administrativas do AD para a UO que contém o servidor SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

Informações relacionadas

"O usuário de domínio não consegue fazer login no cluster com Domain-Tunnel"

Utilize a assinatura SMB para melhorar a segurança da rede

Utilize a assinatura SMB para melhorar a visão geral da segurança da rede

A assinatura SMB ajuda a garantir que o tráfego de rede entre o servidor SMB e o cliente não seja comprometido; isso evita ataques de repetição. Por padrão, o ONTAP oferece suporte à assinatura SMB quando solicitado pelo cliente. Opcionalmente, o administrador de armazenamento pode configurar o servidor SMB para exigir assinatura SMB.

Como as políticas de assinatura SMB afetam a comunicação com um servidor CIFS

Além das configurações de segurança de assinatura SMB do servidor CIFS, duas diretivas de assinatura SMB em clientes Windows controlam a assinatura digital de comunicações entre clientes e o servidor CIFS. Você pode configurar a configuração que atende aos requisitos da sua empresa.

As diretivas SMB do cliente são controladas por meio das configurações de diretiva de segurança local do Windows, que são configuradas usando o MMC (Console de Gerenciamento da Microsoft) ou GPOs do ative Directory. Para obter mais informações sobre a assinatura SMB do cliente e problemas de segurança, consulte a documentação do Microsoft Windows.

Aqui estão descrições das duas políticas de assinatura SMB em clientes Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuração controla se a capacidade de assinatura SMB do cliente está ativada. Ele é habilitado por padrão. Quando essa configuração é desativada no cliente, as comunicações do cliente com o servidor CIFS dependem da configuração de assinatura SMB no servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuração controla se o cliente requer assinatura SMB para se comunicar com um servidor. Ele está desativado por padrão. Quando essa configuração é desativada no cliente, o comportamento de assinatura SMB é baseado na configuração de diretiva `Microsoft network client: Digitally sign communications (if server agrees)` e na configuração no servidor CIFS.

> Se o seu ambiente incluir clientes Windows configurados para exigir assinatura SMB, você deverá ativar a assinatura SMB no servidor CIFS. Se você não fizer isso, o servidor CIFS não poderá fornecer dados a esses sistemas.

Os resultados efetivos das configurações de assinatura SMB do cliente e do servidor CIFS dependem se as sessões SMB usam SMB 1,0 ou SMB 2.x e posterior.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 1,0:

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura desativada e não necessária	Não assinado	Assinado
Assinatura ativada e não necessária	Não assinado	Assinado
Assinatura desativada e necessária	Assinado	Assinado
Assinatura ativada e necessária	Assinado	Assinado

Clientes Windows SMB 1 mais antigos e alguns clientes SMB 1 não Windows podem não conseguir se conetar se a assinatura estiver desativada no cliente, mas necessária no servidor CIFS.

A tabela a seguir resume o comportamento eficaz de assinatura SMB se a sessão usar SMB 2.x ou SMB 3,0:

Para clientes SMB 2.x e SMB 3,0, a assinatura SMB está sempre ativada. Não pode ser desativado.

Cliente	ONTAP—assinatura não necessária	ONTAP - assinatura necessária
Assinatura não necessária	Não assinado	Assinado
Assinatura necessária	Assinado	Assinado

A tabela a seguir resume o comportamento padrão de assinatura SMB de cliente e servidor da Microsoft:

Protocolo	Algoritmo hash	Pode ativar/desativar	Pode exigir/não exigir	Padrão do cliente	Padrão do servidor	DC predefinido
SMB 1,0	MD5	Sim	Sim	Ativado (não necessário)	Desativado (não necessário)	Obrigatório
SMB 2.x	HMAC SHA-256	Não	Sim	Não é necessário	Não é necessário	Obrigatório
SMB 3,0	AES-CMAC.	Não	Sim	Não é necessário	Não é necessário	Obrigatório

A Microsoft não recomenda mais o uso `Digitally sign communications (if client agrees)` das configurações de Diretiva de Grupo ou `Digitally sign communications (if server agrees)` . A Microsoft também não recomenda mais o uso das `EnableSecuritySignature` configurações do Registro. Essas opções afetam apenas o comportamento do SMB 1 e podem ser substituídas pela `Digitally sign communications (always)` configuração de Diretiva de Grupo ou pela `RequireSecuritySignature` configuração do Registro. Você também pode obter mais informações do blog da Microsoft.http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx[The Fundamentos de assinatura SMB (abrangendo SMB1 e SMB2)]

Impacto na performance da assinatura SMB

Quando as sessões SMB usam a assinatura SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB assinado. A descarga de assinatura SMB é ativada por padrão quando a assinatura SMB está ativada.

O desempenho aprimorado de assinatura SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impactos na performance da assinatura SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A maioria dos clientes do Windows negocia a assinatura SMB por padrão se estiver habilitada no servidor. Se você precisar de proteção SMB para alguns de seus clientes Windows e se a assinatura SMB estiver causando problemas de desempenho, você poderá desativar a assinatura SMB em qualquer um de seus clientes Windows que não precisem de proteção contra ataques de repetição. Para obter informações sobre como desativar a assinatura SMB em clientes Windows, consulte a documentação do Microsoft Windows.

Recomendações para configurar a assinatura SMB

Você pode configurar o comportamento de assinatura SMB entre clientes SMB e o servidor CIFS para atender aos seus requisitos de segurança. As configurações escolhidas ao configurar a assinatura SMB no servidor CIFS dependem de quais são os requisitos de segurança.

Você pode configurar a assinatura SMB no cliente ou no servidor CIFS. Considere as seguintes recomendações ao configurar a assinatura SMB:

Se…	Recomendação…
Você deseja aumentar a segurança da comunicação entre o cliente e o servidor	Torne a assinatura SMB necessária no cliente ativando a `Require Option (Sign always)` configuração de segurança no cliente.
Você deseja que todo o tráfego SMB para uma determinada máquina virtual de storage (SVM) seja assinado	Torne necessária a assinatura SMB no servidor CIFS configurando as configurações de segurança para exigir assinatura SMB.

Consulte a documentação da Microsoft para obter mais informações sobre como configurar as configurações de segurança do cliente Windows.

Diretrizes para assinatura SMB quando vários dados LIFS são configurados

Se você ativar ou desativar a assinatura SMB necessária no servidor SMB, você deve estar ciente das diretrizes para várias configurações LIFS de dados para um SVM.

Quando você configura um servidor SMB, pode haver várias LIFs de dados configuradas. Nesse caso, o

servidor DNS contém várias `A` entradas de Registro para o servidor CIFS, todas usando o mesmo nome de host do servidor SMB, mas cada uma com um endereço IP exclusivo. Por exemplo, um servidor SMB que tem duas LIFs de dados configuradas pode ter as seguintes entradas de Registro DNS `A`:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

O comportamento normal é que, ao alterar a configuração de assinatura SMB necessária, apenas novas conexões de clientes são afetadas pela alteração na configuração de assinatura SMB. No entanto, há uma exceção a esse comportamento. Há um caso em que um cliente tem uma conexão existente com um compartilhamento, e o cliente cria uma nova conexão com o mesmo compartilhamento após a configuração ser alterada, mantendo a conexão original. Nesse caso, tanto a conexão SMB nova quanto a existente adotam os novos requisitos de assinatura SMB.

Considere o seguinte exemplo:

1. Client1 coneta-se a um compartilhamento sem a assinatura SMB necessária usando o caminho `O:\`.
2. O administrador de armazenamento modifica a configuração do servidor SMB para exigir assinatura SMB.
3. O Client1 coneta-se ao mesmo compartilhamento com a assinatura SMB necessária usando o caminho `S:\` (mantendo a conexão usando o caminho `O:\`).
4. O resultado é que a assinatura SMB é usada ao acessar dados `O:\` nas unidades e `S:\` .

Ative ou desative a assinatura SMB necessária para o tráfego SMB de entrada

Você pode impor o requisito para que os clientes assinem mensagens SMB habilitando a assinatura SMB necessária. Se ativado, o ONTAP aceita mensagens SMB somente se elas tiverem assinaturas válidas. Se você quiser permitir a assinatura SMB, mas não a exigir, você pode desativar a assinatura SMB necessária.

Sobre esta tarefa

Por padrão, a assinatura SMB necessária está desativada. Você pode ativar ou desativar a assinatura SMB necessária a qualquer momento.

> A assinatura SMB não está desativada por padrão nas seguintes circunstâncias:
>
> 1. A assinatura SMB necessária está ativada e o cluster é revertido para uma versão do ONTAP que não suporta assinatura SMB.
> 2. O cluster é posteriormente atualizado para uma versão do ONTAP que suporte a assinatura SMB.
>
>   Nestas circunstâncias, a configuração de assinatura SMB que foi originalmente configurada em uma versão suportada do ONTAP é mantida por meio de reversão e atualização subsequente.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de assinatura SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (non-ID-Preserve), a configuração de segurança de assinatura SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se você ativou a assinatura SMB necessária na SVM de origem, habilite manualmente a assinatura SMB necessária no SVM de destino.

Passos

1. Execute uma das seguintes ações:

Se você quiser que a assinatura SMB seja necessária…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Verifique se a assinatura SMB necessária está ativada ou desativada determinando se o valor no `Is Signing Required` campo na saída do comando a seguir está definido para o valor desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Exemplo

O exemplo a seguir habilita a assinatura SMB necessária para o SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Determine se as sessões SMB são assinadas

Você pode exibir informações sobre sessões SMB conetadas no servidor CIFS. Você pode usar essas informações para determinar se as sessões SMB são assinadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Todas as sessões assinadas em uma máquina virtual de storage (SVM) especificada	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Detalhes de uma sessão assinada com um Session ID específico no SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Exemplos

O comando a seguir exibe informações de sessão sobre sessões assinadas no SVM VS1. A saída de resumo padrão não exibe o campo de saída "'is Session signed'":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

O comando a seguir exibe informações detalhadas da sessão, incluindo se a sessão está assinada, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Monitoramento de estatísticas de sessão assinadas pelo SMB

Monitorar estatísticas de sessão assinadas pelo SMB

Você pode monitorar estatísticas de sessões SMB e determinar quais sessões estabelecidas são assinadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível de privilégio avançado fornece o `signed_sessions` contador que você pode usar para monitorar o número de sessões SMB assinadas. O `signed_sessions` contador está disponível com os seguintes objetos estatísticos:

- `cifs` Permite monitorar a assinatura SMB para todas as sessões SMB.
- `smb1` Permite monitorar a assinatura SMB para sessões SMB 1,0.
- `smb2` Permite monitorar a assinatura SMB para sessões SMB 2.x e SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `smb2` objeto.

Se você quiser comparar o número de sessão assinada com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `signed_sessions` o contador.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra

fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado
   `set -privilege advanced`
2. Iniciar uma coleta de dados
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.
3. Use o `statistics stop` comando para parar de coletar dados para a amostra.
4. Exibir estatísticas de assinatura SMB:

Se você quiser ver informações para…	**Digite…**
Sessões assinadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sessões assinadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.
5. Voltar para o nível de privilégio de administrador
   `set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de assinatura SMB 2.x e SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

O comando a seguir interrompe a coleta de dados para a amostra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

O comando a seguir mostra sessões SMB assinadas e sessões SMB estabelecidas por nó da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

O comando a seguir mostra sessões SMB assinadas para node2 da amostra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

O seguinte comando volta para o nível de privilégio admin:

```
cluster1::*> set -privilege admin
```

Informações relacionadas

Determinar se as sessões SMB são assinadas

"Visão geral do gerenciamento e monitoramento de desempenho"

Configurar a criptografia SMB necessária em servidores SMB para transferências de dados por SMB

Visão geral da criptografia SMB

A encriptação SMB para transferências de dados através de SMB é um melhoramento de segurança que pode ativar ou desativar em servidores SMB. Você também pode configurar a configuração de criptografia SMB desejada em uma base de compartilhamento por compartilhamento por meio de uma configuração de propriedade de compartilhamento.

Por padrão, quando você cria um servidor SMB na máquina virtual de storage (SVM), a criptografia SMB é desativada. Você deve habilitá-lo para aproveitar a segurança aprimorada fornecida pela criptografia SMB.

Para criar uma sessão SMB encriptada, o cliente SMB tem de suportar a encriptação SMB. Os clientes Windows que começam com o Windows Server 2012 e o Windows 8 suportam a encriptação SMB.

A criptografia SMB no SVM é controlada por meio de duas configurações:

- Uma opção de segurança de servidor SMB que habilita a funcionalidade no SVM
- Uma propriedade de compartilhamento SMB que configura a configuração de criptografia SMB em uma base de compartilhamento por compartilhamento

Você pode decidir se deseja exigir criptografia para acesso a todos os dados no SVM ou se exige que a criptografia SMB acesse dados somente em compartilhamentos selecionados. As configurações de nível SVM substituem as configurações de nível de compartilhamento.

A configuração eficaz de criptografia SMB depende da combinação das duas configurações e é descrita na tabela a seguir:

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Verdadeiro	Falso	A criptografia no nível do servidor está habilitada para todos os compartilhamentos na SVM. Com essa configuração, a criptografia acontece para toda a sessão SMB.
Verdadeiro	Verdadeiro	A criptografia no nível do servidor é ativada para todos os compartilhamentos no SVM, independentemente da criptografia no nível de compartilhamento. Com essa configuração, a criptografia acontece para toda a sessão SMB.

Encriptação SMB do servidor SMB ativada	Compartilhar criptografar a configuração de dados ativada	Comportamento de criptografia do lado do servidor
Falso	Verdadeiro	A criptografia no nível de compartilhamento está ativada para compartilhamentos específicos. Com essa configuração, a criptografia acontece a partir da conexão em árvore.
Falso	Falso	Nenhuma criptografia está ativada.

Os clientes SMB que não suportam encriptação não podem estabelecer ligação a um servidor SMB ou partilha que requeira encriptação.

As alterações nas definições de encriptação entram em vigor para novas ligações. As ligações existentes não são afetadas.

Impacto na performance da criptografia SMB

Quando as sessões SMB usam criptografia SMB, todas as comunicações SMB de e para clientes Windows têm um impactos na performance, o que afeta tanto os clientes quanto o servidor (ou seja, os nós no cluster que executa o SVM que contém o servidor SMB).

O impactos no desempenho mostra como aumento do uso da CPU tanto nos clientes quanto no servidor, embora a quantidade de tráfego de rede não mude.

A extensão do impactos no desempenho depende da versão do ONTAP 9 que você está executando. A partir do ONTAP 9.7, um novo algoritmo de criptografia off-load pode permitir melhor desempenho no tráfego SMB criptografado. A descarga de criptografia SMB é ativada por padrão quando a criptografia SMB está ativada.

O desempenho aprimorado da criptografia SMB requer a capacidade de descarga AES-NI. Consulte o Hardware Universe (HWU) para verificar se a descarga AES-NI é suportada para sua plataforma.

Melhorias adicionais de desempenho também são possíveis se você for capaz de usar SMB versão 3,11, que suporta o algoritmo GCM muito mais rápido.

Dependendo da sua rede, versão do ONTAP 9, versão do SMB e implementação do SVM, o impacto na performance da criptografia SMB pode variar muito. Você pode verificá-lo somente por meio de testes em seu ambiente de rede.

A encriptação SMB está desativada por predefinição no servidor SMB. Você deve habilitar a criptografia SMB somente nos compartilhamentos SMB ou servidores SMB que exigem criptografia. Com a criptografia SMB, o ONTAP realiza processamento adicional de descriptografar as solicitações e criptografar as respostas para cada solicitação. A criptografia SMB deve, portanto, ser ativada somente quando necessário.

Ative ou desative a encriptação SMB necessária para o tráfego SMB de entrada

Se pretender exigir encriptação SMB para o tráfego SMB de entrada, pode ativá-la no servidor CIFS ou no nível de partilha. Por padrão, a criptografia SMB não é necessária.

Sobre esta tarefa

Você pode ativar a criptografia SMB no servidor CIFS, que se aplica a todos os compartilhamentos no servidor CIFS. Se não pretender a encriptação SMB necessária para todos os partilhas no servidor CIFS ou se pretender ativar a encriptação SMB necessária para o tráfego SMB de entrada numa base de partilha por partilha, pode desativar a encriptação SMB necessária no servidor CIFS.

Quando você configura uma relação de recuperação de desastres de máquina virtual de storage (SVM), o valor selecionado para a `-identity-preserve` opção `snapmirror create` do comando determina os detalhes de configuração replicados no SVM de destino.

Se você definir `-identity-preserve` a opção como `true` (ID-Preserve), a configuração de segurança de criptografia SMB será replicada para o destino.

Se você definir `-identity-preserve` a opção como `false` (não-ID-Preserve), a configuração de segurança de criptografia SMB não será replicada para o destino. Nesse caso, as configurações de segurança do servidor CIFS no destino são definidas com os valores padrão. Se tiver ativado a encriptação SMB na SVM de origem, tem de ativar manualmente a encriptação SMB do servidor CIFS no destino.

Passos

1. Execute uma das seguintes ações:

Se pretender que a encriptação SMB necessária para o tráfego SMB de entrada no servidor CIFS seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. Verifique se a criptografia SMB necessária no servidor CIFS está ativada ou desativada conforme desejado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   O `is-smb-encryption-required` campo é exibido `true` se a criptografia SMB necessária estiver ativada no servidor CIFS e `false` se estiver desativada.

Exemplo

O exemplo a seguir habilita a criptografia SMB necessária para o tráfego SMB de entrada para o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

Determine se os clientes estão conetados usando sessões SMB criptografadas

Você pode exibir informações sobre sessões SMB conetadas para determinar se os clientes estão usando conexões SMB criptografadas. Isso pode ser útil para determinar se as sessões de cliente SMB estão se conetando com as configurações de segurança desejadas.

Sobre esta tarefa

As sessões de clientes SMB podem ter um dos três níveis de criptografia:

- `unencrypted`

  A sessão SMB não está encriptada. Nem a criptografia no nível de máquina virtual de storage (SVM) nem no nível de compartilhamento são configuradas.

- `partially-encrypted`

  A criptografia é iniciada quando ocorre a conexão em árvore. A criptografia no nível de compartilhamento está configurada. A criptografia no nível da SVM não está ativada.

- `encrypted`

  A sessão SMB está totalmente encriptada. A criptografia no nível da SVM está ativada. A encriptação do nível de partilha pode ou não estar ativada. A configuração de criptografia no nível da SVM substitui a configuração de criptografia no nível de compartilhamento.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Sessões com uma configuração de criptografia especificada para sessões em um SVM especificado	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`

Se você quiser exibir informações sobre…	Digite o comando…
A configuração de criptografia para um Session ID específico em um SVM especificado	`vserver cifs session show -vserver` *`vserver_name`* `-session-id` *`integer`* `-instance`

Exemplos

O comando a seguir exibe informações detalhadas da sessão, incluindo a configuração de criptografia, em uma sessão SMB com um Session ID de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
                Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                Open Shares: 1
                 Open Files: 1
                 Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Monitorar estatísticas de criptografia SMB

Você pode monitorar estatísticas de criptografia SMB e determinar quais sessões estabelecidas e conexões de compartilhamento são criptografadas e quais não são.

Sobre esta tarefa

O `statistics` comando no nível avançado de privilégios fornece os seguintes contadores, que podem ser utilizados para monitorizar o número de sessões SMB encriptadas e partilhar ligações:

Nome do contador	Descrições
`encrypted_sessions`	Fornece o número de sessões criptografadas do SMB 3,0

Nome do contador	Descrições
`encrypted_share_connections`	Fornece o número de compartilhamentos criptografados nos quais uma conexão em árvore aconteceu
`rejected_unencrypted_sessions`	Fornece o número de configurações de sessão rejeitadas devido à falta de capacidade de criptografia do cliente
`rejected_unencrypted_shares`	Fornece o número de mapeamentos de compartilhamento rejeitados devido à falta de capacidade de criptografia do cliente

Esses contadores estão disponíveis com os seguintes objetos estatísticos:

- `cifs` Permite monitorizar a encriptação SMB para todas as sessões SMB 3,0.

  As estatísticas SMB 3,0 são incluídas na saída para o `cifs` objeto. Se você quiser comparar o número de sessões criptografadas com o número total de sessões, você pode comparar a saída para o contador com a saída `established_sessions` para `encrypted_sessions` o contador.

  Se você quiser comparar o número de conexões de compartilhamento criptografadas com o número total de conexões de compartilhamento, você pode comparar a saída para o contador com a saída `connected_shares` para `encrypted_share_connections` o contador.

- `rejected_unencrypted_sessions` Fornece o número de vezes que uma tentativa foi feita para estabelecer uma sessão SMB que requer criptografia de um cliente que não suporta criptografia SMB.
- `rejected_unencrypted_shares` Fornece o número de vezes que uma tentativa foi feita para se conetar a um compartilhamento SMB que requer criptografia de um cliente que não suporta criptografia SMB.

Você deve iniciar uma coleta de amostras de estatísticas antes de poder visualizar os dados resultantes. Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências.

Passos

1. Defina o nível de privilégio como avançado
   `set -privilege advanced`
2. Iniciar uma coleta de dados
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Se você não especificar o `-sample-id` parâmetro, o comando gera um identificador de amostra para você e define esse exemplo como a amostra padrão para a sessão CLI. O valor para `-sample-id` é uma cadeia de texto. Se você executar esse comando durante a mesma sessão CLI e não especificar o `-sample-id` parâmetro, o comando sobrescreverá a amostra padrão anterior.

   Opcionalmente, você pode especificar o nó no qual deseja coletar estatísticas. Se você não especificar o nó, a amostra coletará estatísticas para todos os nós no cluster.

3. Use o `statistics stop` comando para parar de coletar dados para a amostra.
4. Exibir estatísticas de criptografia SMB:

Se você quiser ver informações para…	Digite…
Sessões criptografadas	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	Sessões criptografadas e sessões estabelecidas
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento criptografadas
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
Conexões de compartilhamento criptografadas e compartilhamentos conetados	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
Sessões não criptografadas rejeitadas	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	Conexões de compartilhamento não criptografadas rejeitadas
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

Se você quiser exibir informações apenas para um único nó, especifique o parâmetro opcional `-node`.

5. Voltar para o nível de privilégio de administrador
`set -privilege admin`

Exemplos

O exemplo a seguir mostra como você pode monitorar as estatísticas de criptografia SMB 3,0 na máquina virtual de armazenamento (SVM) VS1.

O seguinte comando move-se para o nível de privilégio avançado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

O comando a seguir inicia a coleta de dados para uma nova amostra:

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

O comando a seguir interrompe a coleta de dados para essa amostra:

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

O comando a seguir mostra sessões criptografadas SMB e sessões estabelecidas SMB pelo nó da amostra:

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    --------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

O comando a seguir mostra o número de sessões SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

O comando a seguir mostra o número de compartilhamentos SMB conetados e compartilhamentos SMB criptografados pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    --------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

O comando a seguir mostra o número de conexões de compartilhamento SMB não criptografadas rejeitadas pelo nó da amostra:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

Informações relacionadas

Determinando quais objetos e contadores de estatísticas estão disponíveis

"Visão geral do gerenciamento e monitoramento de desempenho"

Comunicação de sessão LDAP segura

Conceitos de assinatura e vedação LDAP

A partir do ONTAP 9, você pode configurar a assinatura e a vedação para habilitar a segurança da sessão LDAP em consultas para um servidor AD (ative Directory). Você

deve configurar as configurações de segurança do servidor CIFS na máquina virtual de armazenamento (SVM) para corresponder às do servidor LDAP.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. Uma opção *LDAP Security Level* indica se o tráfego LDAP precisa ser assinado, assinado e selado, ou não. A predefinição é `none`.

A assinatura LDAP e a vedação no tráfego CIFS são ativadas no SVM com a `-session-security-for-ad-ldap` opção de `vserver cifs security modify` comando.

Ative a assinatura LDAP e a vedação no servidor CIFS

Antes que o servidor CIFS possa usar assinatura e vedação para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor CIFS para habilitar a assinatura e a vedação LDAP.

Antes de começar

Você deve consultar o administrador do servidor AD para determinar os valores de configuração de segurança apropriados.

Passos

1. Configure a configuração de segurança do servidor CIFS que permite o tráfego assinado e selado com servidores LDAP do ative Directory: `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap {none|sign|seal}`

   Você pode ativar assinatura (`sign`, integridade de dados), assinatura e vedação (`seal`, integridade e criptografia de dados) ou nenhum `none`, sem assinatura ou vedação). O valor padrão é `none`.

2. Verifique se a configuração de segurança de assinatura e vedação LDAP está definida corretamente: `vserver cifs security show -vserver` *`vserver_name`*

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX, como usuários, grupos e netgroups, você deverá ativar a configuração correspondente com `-session-security` a opção do `vserver services name-service ldap client modify` comando.

Configurar LDAP em TLS

Exporte uma cópia do certificado de CA raiz autoassinado

Para usar LDAP em SSL/TLS para proteger a comunicação do ative Directory, primeiro você deve exportar uma cópia do certificado CA raiz autoassinado do ative Directory Service para um arquivo de certificado e convertê-lo em um arquivo de texto ASCII. Esse arquivo de texto é usado pelo ONTAP para instalar o certificado na máquina virtual de storage (SVM).

Antes de começar

O Serviço de certificados do ative Directory já deve estar instalado e configurado para o domínio ao qual o servidor CIFS pertence. Você pode encontrar informações sobre a instalação e configuração dos Serviços de

certificados do ative diretor consultando a Biblioteca Microsoft TechNet.

"Microsoft TechNet Library: technet.microsoft.com"

Passo

1. Obtenha um certificado de CA raiz do controlador de domínio que está no `.pem` formato de texto.

   "Microsoft TechNet Library: technet.microsoft.com"

Depois de terminar

Instale o certificado no SVM.

Informações relacionadas

"Microsoft TechNet Library"

Instale o certificado de CA raiz autoassinado no SVM

Se a autenticação LDAP com TLS for necessária ao vincular a servidores LDAP, primeiro você deverá instalar o certificado de CA raiz autoassinado no SVM.

Sobre esta tarefa

Quando o LDAP sobre TLS está ativado, o cliente LDAP do ONTAP no SVM não oferece suporte a certificados revogados no ONTAP 9.0 e 9,1.

A partir do ONTAP 9.2, todos os aplicativos do ONTAP que usam comunicações TLS podem verificar o status do certificado digital usando o protocolo OCSP (Online Certificate Status Protocol). Se o OCSP estiver ativado para LDAP através de TLS, os certificados revogados serão rejeitados e a conexão falhará.

Passos

1. Instale o certificado CA raiz autoassinado:
   a. Inicie a instalação do certificado: `security certificate install -vserver vserver_name -type server-ca`

      A saída do console exibe a seguinte mensagem: `Please enter Certificate: Press <Enter> when done`

   b. Abra o arquivo de certificado `.pem` com um editor de texto, copie o certificado, incluindo as linhas que começam com `-----BEGIN CERTIFICATE-----` e terminam com `-----END CERTIFICATE-----`, e cole o certificado após o prompt de comando.
   c. Verifique se o certificado é exibido corretamente.
   d. Conclua a instalação pressionando Enter.
2. Verifique se o certificado está instalado: `security certificate show -vserver *vserver_name*`

Ative LDAP através de TLS no servidor

Antes que o servidor SMB possa usar TLS para comunicação segura com um servidor LDAP do ative Directory, você deve modificar as configurações de segurança do servidor SMB para ativar o LDAP sobre TLS.

A partir do ONTAP 9.10,1, a vinculação de canal LDAP é suportada por padrão para conexões LDAP do ative

Directory (AD) e serviços de nome. O ONTAP tentará a vinculação de canais com conexões LDAP somente se o Start-TLS ou LDAPS estiver ativado junto com a segurança da sessão definida para assinar ou selar. Para desativar ou reativar a vinculação de canais LDAP com servidores AD, use o `-try-channel-binding-for-ad-ldap` parâmetro com o `vserver cifs security modify` comando.

Para saber mais, consulte:

- "Visão geral da LDAP"
- "2020 requisitos de vinculação de canal LDAP e assinatura LDAP para Windows".

Passos

1. Configure a configuração de segurança do servidor SMB que permite a comunicação LDAP segura com servidores LDAP do ative Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verifique se a configuração de segurança LDAP sobre TLS está definida como `true`: `vserver cifs security show -vserver vserver_name`

> Se o SVM usar o mesmo servidor LDAP para consultar o mapeamento de nomes ou outras informações do UNIX (como usuários, grupos e netgroups), você também deve modificar a `-use-start-tls` opção usando o `vserver services name-service ldap client modify` comando.

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Configure o usuário padrão do Windows para mapeamentos de usuários UNIX no servidor SMB

Configure o usuário UNIX padrão

Você pode configurar o usuário UNIX padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar o usuário UNIX padrão.

Sobre esta tarefa

Por padrão, o nome do usuário UNIX padrão é "'pcuser'", o que significa que, por padrão, o mapeamento de usuário para o usuário UNIX padrão está habilitado. Você pode especificar outro nome para usar como usuário UNIX padrão. O nome especificado deve existir nos bancos de dados do serviço de nomes configurados para a máquina virtual de storage (SVM). Se essa opção for definida como uma cadeia de carateres nula, ninguém poderá acessar o servidor CIFS como um usuário padrão UNIX. Ou seja, cada usuário deve ter uma conta no banco de dados de senhas antes de poder acessar o servidor CIFS.

Para que um usuário se conete ao servidor CIFS usando a conta de usuário UNIX padrão, o usuário deve atender aos seguintes pré-requisitos:

- O utilizador está autenticado.
- O usuário está no banco de dados de usuários do Windows local do servidor CIFS, no domínio doméstico do servidor CIFS ou em um domínio confiável (se pesquisas de mapeamento de nomes de vários domínios estiverem ativadas no servidor CIFS).
- O nome de usuário não é explicitamente mapeado para uma cadeia de carateres nula.

Passos

1. Configure o usuário UNIX padrão:

Se você quiser …	Introduza …
Use o usuário padrão do UNIX "'pcuser'"	`vserver cifs options modify -default -unix-user pcuser`
Use outra conta de usuário UNIX como usuário padrão	`vserver cifs options modify -default -unix-user` *`user_name`*
Desative o usuário UNIX padrão	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verifique se o usuário UNIX padrão está configurado corretamente: `vserver cifs options show -vserver` *`vserver_name`*

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : pcuser
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Configure o usuário UNIX convidado

Configurar a opção de usuário UNIX convidado significa que os usuários que fazem login de domínios não confiáveis são mapeados para o usuário UNIX convidado e podem se conetar ao servidor CIFS. Alternativamente, se você quiser que a autenticação de usuários de domínios não confiáveis falhe, você não deve configurar o usuário UNIX convidado. O padrão é não permitir que usuários de domínios não confiáveis se conetem ao servidor CIFS (a conta UNIX convidada não está configurada).

Sobre esta tarefa

Você deve ter em mente o seguinte ao configurar a conta UNIX Guest:

- Se o servidor CIFS não puder autenticar o usuário em um controlador de domínio para o domínio doméstico ou um domínio confiável ou o banco de dados local e essa opção estiver ativada, o servidor CIFS considera o usuário como um usuário convidado e mapeia o usuário para o usuário UNIX especificado.
- Se essa opção for definida como uma cadeia de carateres nula, o usuário UNIX convidado será desativado.
- Você deve criar um usuário UNIX para usar como usuário UNIX convidado em um dos bancos de dados do serviço de nomes de máquina virtual de armazenamento (SVM).
- Um usuário conetado como um usuário convidado é automaticamente membro do grupo BUILTIN/convidados no servidor CIFS.
- A opção 'homedirs-public' aplica-se apenas a utilizadores autenticados. Um usuário conetado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite…
Configure o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user` *`unix_name`*
Desative o usuário UNIX convidado	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verifique se o usuário UNIX convidado está configurado corretamente: `vserver cifs options show -vserver vserver_name`

   No exemplo a seguir, tanto o usuário UNIX padrão quanto o usuário UNIX convidado no SVM VS1 são configurados para usar o usuário UNIX "'pcuser'":

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

Mapeie o grupo administrators para root

Se você tiver apenas clientes CIFS em seu ambiente e sua máquina virtual de storage (SVM) tiver sido configurada como um sistema de storage multiprotocolo, você deverá ter pelo menos uma conta do Windows que tenha privilégios de raiz para acessar arquivos no SVM; caso contrário, não será possível gerenciar o SVM porque não tem direitos de usuário suficientes.

Sobre esta tarefa

No entanto, se o sistema de armazenamento tiver sido configurado apenas para NTFS, o `/etc` diretório tem uma ACL no nível do ficheiro que permite ao grupo de administradores aceder aos ficheiros de configuração do ONTAP.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Configure a opção de servidor CIFS que mapeia o grupo de administradores para fazer root conforme apropriado:

Se você quiser…	Então…
Mapeie os membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` Todas as contas do grupo administrators são consideradas root, mesmo que você não tenha uma `/etc/usermap.cfg` entrada mapeando as contas para root. Se você criar um arquivo usando uma conta que pertence ao grupo administrators, o arquivo será de propriedade do root quando você exibir o arquivo de um cliente UNIX.
Desative o mapeamento dos membros do grupo de administradores para fazer root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` As contas no grupo administrators não são mais mapeadas para o root. Você só pode mapear explicitamente um único usuário para o root.

3. Verifique se a opção está definida para o valor desejado: `vserver cifs options show -vserver` *`vserver_name`*
4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exiba informações sobre quais tipos de usuários estão conetados em sessões SMB

Você pode exibir informações sobre que tipo de usuários estão conetados em sessões SMB. Isso pode ajudar você a garantir que apenas o tipo apropriado de usuário esteja se conetando por sessões SMB na máquina virtual de storage (SVM).

Sobre esta tarefa

Os seguintes tipos de usuários podem se conetar através de sessões SMB:

- `local-user`

  Autenticado como um usuário CIFS local

- `domain-user`

  Autenticado como um usuário de domínio (do domínio doméstico do servidor CIFS ou de um domínio confiável)

- `guest-user`

  Autenticado como usuário convidado

- `anonymous-user`

  Autenticado como um usuário anônimo ou nulo

Passos

1. Determine que tipo de usuário está conetado em uma sessão SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Se você quiser exibir informações de tipo de usuário para sessões estabelecidas…	Digite o seguinte comando…
Para todas as sessões com um tipo de usuário especificado	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	Para um usuário específico

Exemplos

O comando a seguir exibe informações de sessão sobre o tipo de usuário para sessões no SVM VS1 estabelecido pelo usuário "" iebubs user1":

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

Opções de comando para limitar o consumo excessivo de recursos do cliente Windows

As opções para o `vserver cifs options modify` comando permitem controlar o consumo de recursos para clientes Windows. Isso pode ser útil se algum cliente estiver fora dos limites normais de consumo de recursos, por exemplo, se houver um número excepcionalmente alto de arquivos abertos, sessões abertas ou solicitações Change Notify.

As seguintes opções para o `vserver cifs options modify` comando foram adicionadas para controlar o consumo de recursos do cliente Windows. Se o valor máximo de qualquer uma dessas opções for excedido, a solicitação será negada e uma mensagem EMS será enviada. Uma mensagem de aviso EMS também é enviada quando 80% do limite configurado para essas opções é atingido.

- `-max-opens-same-file-per-tree`

  Número máximo de aberturas no mesmo arquivo por árvore CIFS

- `-max-same-user-sessions-per-connection`

  Número máximo de sessões abertas pelo mesmo usuário por conexão

- `-max-same-tree-connect-per-session`

  O número máximo de árvores se coneta no mesmo compartilhamento por sessão

- `-max-watches-set-per-tree`

  Número máximo de relógios (também conhecido como *change notifica*) estabelecido por árvore

Consulte as páginas man para ver os limites padrão e para exibir a configuração atual.

A partir do ONTAP 9.4, os servidores que executam o SMB versão 2 ou posterior podem limitar o número de solicitações pendentes (*créditos SMB*) que o cliente pode enviar para o servidor em uma conexão SMB. O gerenciamento de créditos SMB é iniciado pelo cliente e controlado pelo servidor.

O número máximo de solicitações pendentes que podem ser concedidas em uma conexão SMB é controlado pela `-max-credits` opção. O valor padrão para essa opção é 128.

Melhore o desempenho do cliente com os oplocks tradicionais e de leasing

Melhore o desempenho do cliente com a visão geral tradicional e dos oplocks de leasing

Os oplocks tradicionais (bloqueios oportunistas) e os oplocks de leasing permitem que um cliente SMB em determinados cenários de compartilhamento de arquivos execute o armazenamento em cache do lado do cliente de informações de leitura antecipada, gravação e bloqueio. Um cliente pode então ler ou gravar em um arquivo sem lembrar regularmente o servidor de que precisa de acesso ao arquivo em questão. Isso melhora o desempenho reduzindo o tráfego de rede.

Os calços de leasing são uma forma melhorada de oplocks disponíveis com o protocolo SMB 2,1 e posterior. Os locks permitem que um cliente obtenha e preserve o estado de cache do cliente em várias aberturas SMB originadas de si mesmo.

Os calços podem ser controlados de duas maneiras:

- Por uma propriedade share, usando o `vserver cifs share create` comando quando o compartilhamento é criado, ou o `vserver share properties` comando após a criação.
- Por uma propriedade de qtree, usando o `volume qtree create` comando quando a qtree é criada, ou os `volume qtree oplock` comandos após a criação.

Escreva considerações sobre perda de dados de cache ao usar os oplocks

Em algumas circunstâncias, se um processo tem um oplock exclusivo em um arquivo e um segundo processo tenta abrir o arquivo, o primeiro processo deve invalidar dados em cache e flush escreve e bloqueia. O cliente deve então abandonar o oplock e o acesso ao arquivo. Se houver uma falha de rede durante esse flush, os dados de gravação em cache podem ser perdidos.

- Possibilidades de perda de dados

  Qualquer aplicativo que tenha dados gravados em cache pode perder esses dados sob o seguinte conjunto de circunstâncias:

- A conexão é feita usando SMB 1,0.
- Tem um oplock exclusivo no arquivo.
- É dito para interromper esse oplock ou fechar o arquivo.
- Durante o processo de limpeza do cache de gravação, a rede ou o sistema de destino gera um erro.

- Erro de manipulação e conclusão de gravação

  O cache em si não tem nenhum tratamento de erros - os aplicativos fazem.quando o aplicativo faz uma gravação no cache, a gravação é sempre concluída. Se o cache, por sua vez, faz uma gravação no sistema de destino em uma rede, ele deve assumir que a gravação é concluída porque, se não fizer, os dados são perdidos.

Ative ou desative os oplocks ao criar compartilhamentos SMB

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Os Oplocks são ativados em compartilhamentos SMB residentes em máquinas virtuais de armazenamento (SVMs). Em algumas circunstâncias, você pode querer desativar os oplocks. Você pode ativar ou desativar os oplocks em uma base de compartilhamento por compartilhamento.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a configuração de volume de oplock A desativação de oplocks na partilha desativa os oplocks oportunistas e de leasing.

Você pode especificar outras propriedades de compartilhamento além de especificar a propriedade de compartilhamento de oplock usando uma lista delimitada por vírgulas. Você também pode especificar outros parâmetros de compartilhamento.

Passos

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]` Se desejar que o compartilhamento tenha apenas as propriedades padrão de compartilhamento, que são `oplocks`, `browsable` e `changenotify` ativadas, não será necessário especificar o `-share -properties` parâmetro ao criar um compartilhamento SMB. Se você quiser qualquer combinação de propriedades de compartilhamento diferente do padrão, especifique o `-share-properties` parâmetro com a lista de propriedades de compartilhamento a ser usada para esse compartilhamento.
Desative os oplocks em um compartilhamento durante a criação de compartilhamento	Introduza o seguinte comando: `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` Ao desativar os oplocks, você deve especificar uma lista de propriedades de compartilhamento ao criar o compartilhamento, mas não deve especificar a `oplocks` propriedade.

Informações relacionadas

Ativar ou desativar os oplocks em compartilhamentos SMB existentes

Monitorização do estado de oplock

Comandos para ativar ou desativar oplocks em volumes e qtrees

Oplocks permitem que os clientes bloqueiem arquivos e armazenem conteúdo de cache localmente, o que pode aumentar o desempenho para operações de arquivos. Você precisa saber os comandos para ativar ou desativar os oplocks em volumes ou qtrees. Você também deve saber quando você pode ativar ou desativar os oplocks em volumes e qtrees.

- Os calços são ativados em volumes por predefinição.
- Não é possível desativar os oplocks ao criar um volume.
- Você pode ativar ou desativar os oplocks em volumes existentes para SVMs a qualquer momento.
- Você pode ativar os oplocks em qtrees para SVMs.

  A configuração do modo de oplock é uma propriedade da ID de qtree 0, a qtree padrão que todos os volumes têm. Se você não especificar uma configuração de oplock ao criar uma qtree, a qtree herdará a configuração de oplock do volume pai, que é habilitada por padrão. No entanto, se você especificar uma configuração de oplock na nova qtree, ela terá precedência sobre a configuração de oplock no volume.

Se você quiser…	Use este comando…
Ative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `enable`
Desative os oplocks em volumes ou qtrees	`volume qtree oplocks` com o `-oplock-mode` parâmetro definido como `disable`

Informações relacionadas

Monitorização do estado de oplock

Ative ou desative os oplocks em compartilhamentos SMB existentes

Os Oplocks são ativados em compartilhamentos SMB em máquinas virtuais de armazenamento (SVMs) por padrão. Em algumas circunstâncias, você pode querer desativar os oplocks; alternativamente, se você tiver desabilitado previamente os oplocks em uma ação, você pode querer reativar os oplocks.

Sobre esta tarefa

Se os oplocks estiverem ativados no volume que contém uma partilha, mas a propriedade de partilha de oplock para essa partilha estiver desativada, os oplocks serão desativados para essa partilha. A desativação de oplocks em um compartilhamento tem precedência sobre a ativação de oplocks no volume. Desativar os oplocks na partilha, desativa os oplocks oportunistas e de leasing. Você pode ativar ou desativar os oplocks em compartilhamentos existentes a qualquer momento.

Passo

1. Execute a ação aplicável:

Se você quiser…	Então…
Ative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais a serem adicionadas usando uma lista delimitada por vírgulas. As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento. Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.
Desative os oplocks em um compartilhamento modificando um compartilhamento existente	Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` Você pode especificar propriedades de compartilhamento adicionais para remover usando uma lista delimitada por vírgulas. As propriedades de compartilhamento que você remover são excluídas da lista existente de propriedades de compartilhamento; no entanto, as propriedades de compartilhamento configuradas anteriormente que você não remove permanecem em vigor.

Exemplos

O comando a seguir habilita os oplocks para o compartilhamento chamado "Engenharia" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

O comando a seguir desativa os oplocks para a ação chamada "Engenharia" no SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

Informações relacionadas

Ativar ou desativar os oplocks ao criar compartilhamentos SMB

Monitorização do estado de oplock

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Monitorar o status de oplock

Você pode monitorar e exibir informações sobre o status de oplock Você pode usar essas informações para determinar quais arquivos têm oplocks, quais são o nível de oplock e o nível de estado de oplock e se o leasing de oplock é usado. Você também pode determinar informações sobre bloqueios que você pode precisar quebrar manualmente.

Sobre esta tarefa

Você pode exibir informações sobre todos os oplocks em forma de resumo ou em um formulário de lista detalhado. Você também pode usar parâmetros opcionais para exibir informações sobre um subconjunto menor de bloqueios existentes. Por exemplo, você pode especificar que a saída retorna apenas bloqueia com o endereço IP do cliente especificado ou com o caminho especificado.

Você pode exibir as seguintes informações sobre os oplocks tradicionais e de leasing:

- SVM, nó, volume e LIF em que o oplock
- Bloquear UUID
- Endereço IP do cliente com o oplock
- Caminho no qual o oplock é estabelecido
- Protocolo de bloqueio (SMB) e tipo (oplock)
- Estado de bloqueio
- Nível do calço
- Estado da conexão e tempo de expiração do SMB
- Abra o ID do grupo se for concedida uma locação de oplock

Consulte a `vserver oplocks show` página de manual para obter uma descrição detalhada de cada parâmetro.

Passos

1. Apresentar o estado de oplock utilizando o `vserver locks show` comando.

Exemplos

O comando a seguir exibe informações padrão sobre todos os bloqueios. O oplock no ficheiro apresentado é concedido com um `read-batch` nível de oplock:

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

O exemplo a seguir exibe informações mais detalhadas sobre o bloqueio em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um leasing de oplock é concedido no arquivo com um `batch` nível de oplock a um cliente com um endereço IP de `10.3.1.3`:

> Ao exibir informações detalhadas, o comando fornece saída separada para informações de oplock e sharelock. Este exemplo mostra apenas a saída da secção de oplock

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Informações relacionadas

Ativar ou desativar os oplocks ao criar compartilhamentos SMB

Ativar ou desativar os oplocks em compartilhamentos SMB existentes

Comandos para ativar ou desativar oplocks em volumes e qtrees

Aplique objetos de Diretiva de Grupo a servidores SMB

Aplicar objetos de Diretiva de Grupo à visão geral dos servidores SMB

Seu servidor SMB oferece suporte a objetos de Diretiva de Grupo (GPOs), um conjunto de regras conhecidas como *atributos de diretiva de grupo* que se aplicam a computadores em um ambiente do ative Directory. Você pode usar GPOs para gerenciar centralmente as configurações de todas as máquinas virtuais de storage (SVMs) no cluster que pertence ao mesmo domínio do ative Directory.

Quando os GPOs estão ativados no servidor SMB, o ONTAP envia consultas LDAP ao servidor do ative Directory solicitando informações de GPO. Se houver definições de GPO aplicáveis ao servidor SMB, o

servidor do ative Directory retornará as seguintes informações de GPO:

- Nome GPO
- Versão GPO atual
- Localização da definição GPO
- Listas de UUIDs (identificadores universalmente exclusivos) para conjuntos de políticas GPO

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

GPOs compatíveis

Embora nem todos os objetos de Diretiva de Grupo (GPOs) sejam aplicáveis às máquinas virtuais de storage (SVMs) habilitadas para CIFS, os SVMs podem reconhecer e processar o conjunto relevante de GPOs.

Os GPOs a seguir são compatíveis atualmente com SVMs:

- Definições avançadas de configuração da política de auditoria:

  Acesso a objetos: Preparação da Política de Acesso Central

  Especifica o tipo de eventos a serem auditados para o estadiamento da política de acesso central (CAP), incluindo as seguintes configurações:

  - Não faça auditoria
  - Audite apenas eventos de sucesso
  - Auditar apenas eventos de falha
  - Audite eventos de sucesso e falha

  > Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

  Defina utilizando a `Audit Central Access Policy Staging` definição no `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO.

  > Para usar configurações avançadas de GPO de diretiva de auditoria, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições do registo:

  - Intervalo de atualização da política de grupo para SVM habilitado para CIFS

    Defina utilizando o `Registry` GPO.

- Atualizar desvio aleatório da política de grupo

  Defina utilizando o `Registry` GPO.

- Publicação hash para BranchCache

  A publicação Hash para o GPO BranchCache corresponde ao modo de operação BranchCache. Os três modos de operação suportados a seguir são suportados:

  - Por compartilhamento
  - Todos os compartilhamentos
  - Desativado definido utilizando o `Registry` GPO.

- Suporte à versão hash para BranchCache

  As seguintes três configurações de versão hash são suportadas:

  - BranchCache versão 1
  - BranchCache versão 2
  - BranchCache versões 1 e 2 definidas usando o `Registry` GPO.

> Para usar as configurações de GPO do BranchCache, o BranchCache deve ser configurado no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se o BranchCache não estiver configurado no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

- Definições de segurança
  - Política de auditoria e log de eventos
    - Audite eventos de logon

      Especifica o tipo de eventos de logon a serem auditados, incluindo as seguintes configurações:

      - Não faça auditoria
      - Audite apenas eventos de sucesso
      - Auditoria em eventos de falha
      - Audite eventos de sucesso e falha definidos usando a `Audit logon events` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

    - Auditar o acesso a objeto

      Especifica o tipo de acesso a objeto a ser auditado, incluindo as seguintes configurações:

      - Não faça auditoria
      - Audite apenas eventos de sucesso
      - Auditoria em eventos de falha

- Audite eventos de sucesso e falha definidos usando a `Audit object access` configuração no `Local Policies/Audit Policy` GPO.

> Se qualquer uma das três opções de auditoria estiver definida (auditar apenas eventos de sucesso, auditar apenas eventos de falha, auditar eventos de sucesso e falha), o ONTAP fará a auditoria de eventos de sucesso e falha.

- Método de retenção de log

  Especifica o método de retenção do log de auditoria, incluindo as seguintes configurações:

  - Substituir o registo de eventos quando o tamanho do ficheiro de registo exceder o tamanho máximo do registo
  - Não substituir o registo de eventos (limpar registo manualmente) definido utilizando a `Retention method for security log` definição no `Event Log` GPO.

- Tamanho máximo do registo

  Especifica o tamanho máximo do log de auditoria.

  Defina utilizando a `Maximum security log size` definição no `Event Log` GPO.

> Para usar a diretiva de auditoria e as configurações de GPO de log de eventos, a auditoria deve ser configurada no SVM habilitado para CIFS ao qual você deseja aplicar essas configurações. Se a auditoria não estiver configurada no SVM, as configurações do GPO não serão aplicadas e serão descartadas.

◦ Segurança do sistema de arquivos

Especifica uma lista de arquivos ou diretórios nos quais a segurança de arquivos é aplicada por meio de um GPO.

Defina utilizando o `File System` GPO.

> O caminho do volume para o qual o GPO de segurança do sistema de arquivos está configurado deve existir na SVM.

◦ Política Kerberos

- Inclinação máxima do relógio

  Especifica a tolerância máxima em minutos para a sincronização do relógio do computador.

  Defina utilizando a `Maximum tolerance for computer clock synchronization` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima do bilhete

  Especifica a vida útil máxima em horas para o ticket de usuário.

  Defina utilizando a `Maximum lifetime for user ticket` definição no `Account Policies/Kerberos Policy` GPO.

- Idade máxima de renovação do bilhete

  Especifica o tempo de vida máximo em dias para a renovação do ticket do usuário.

Defina utilizando a `Maximum lifetime for user ticket renewal` definição no `Account Policies/Kerberos Policy` GPO.

- Atribuição de direitos de utilizador (direitos de privilégio)
  - Assuma a propriedade

    Especifica a lista de usuários e grupos que têm o direito de assumir a propriedade de qualquer objeto que possa ser protegido.

    Defina utilizando a `Take ownership of files or other objects` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio de segurança

    Especifica a lista de usuários e grupos que podem especificar opções de auditoria para acesso a objetos de recursos individuais, como arquivos, pastas e objetos do ative Directory.

    Defina utilizando a `Manage auditing and security log` definição no `Local Policies/User Rights Assignment` GPO.

  - Privilégio Change Notify (verificação de desvio transversal)

    Especifica a lista de usuários e grupos que podem atravessar árvores de diretório, mesmo que os usuários e grupos possam não ter permissões no diretório atravessado.

O mesmo privilégio é necessário para que os usuários recebam notificações de alterações em arquivos e diretórios. Defina utilizando a `Bypass traverse checking` definição no `Local Policies/User Rights Assignment` GPO.

- Valores do registo
  - Definição de assinatura necessária

    Especifica se a assinatura SMB necessária está ativada ou desativada.

Defina utilizando a `Microsoft network server: Digitally sign communications (always)` definição no `Security Options` GPO.

- Restringir o anonimato

Especifica quais são as restrições para usuários anônimos e inclui as seguintes três configurações de GPO:

- Sem enumeração de contas SAM (Security Account Manager):

  Esta configuração de segurança determina quais permissões adicionais são concedidas para conexões anônimas ao computador. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM`

`accounts` definição no `Local Policies/Security Options` GPO.

- Nenhuma enumeração de contas e compartilhamentos SAM

  Esta configuração de segurança determina se a enumeração anônima de contas e compartilhamentos SAM é permitida. Esta opção é apresentada como `no-enumeration` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Do not allow anonymous enumeration of SAM accounts and shares` definição no `Local Policies/Security Options` GPO.

- Restringir o acesso anônimo a compartilhamentos e pipes nomeados

  Essa configuração de segurança restringe o acesso anônimo a compartilhamentos e pipes. Esta opção é apresentada como `no-access` no ONTAP se estiver ativada.

  Defina utilizando a `Network access: Restrict anonymous access to Named Pipes and Shares` definição no `Local Policies/Security Options` GPO.

  Ao exibir informações sobre políticas de grupo definidas e aplicadas, o `Resultant restriction for anonymous user` campo de saída fornece informações sobre a restrição resultante das três configurações de GPO anônimo restrito. As possíveis restrições resultantes são as seguintes:

° `no-access`

O usuário anônimo tem acesso negado aos compartilhamentos especificados e pipes nomeados e não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se o `Network access: Restrict anonymous access to Named Pipes and Shares` GPO estiver ativado.

° `no-enumeration`

O usuário anônimo tem acesso aos compartilhamentos especificados e pipes nomeados, mas não pode usar enumeração de contas e compartilhamentos SAM. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`O ou os `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPOs estão ativados.

° `no-restriction`

O usuário anônimo tem acesso total e pode usar enumeração. Esta restrição resultante é vista se ambas as seguintes condições forem cumpridas:

- O `Network access: Restrict anonymous access to Named Pipes and Shares` GPO está desativado.
- `Network access: Do not allow anonymous enumeration of SAM accounts`Os GPOs e `Network access: Do not allow anonymous enumeration of SAM accounts and shares` os GPOs estão desativados.

- Grupos restritos

  Você pode configurar grupos restritos para gerenciar centralmente a associação de grupos internos ou definidos pelo usuário. Quando você aplica um grupo restrito por meio de uma política de grupo, a associação de um grupo local de servidor CIFS é definida automaticamente para corresponder às configurações da lista de membros definidas na política de grupo aplicada.

  Defina utilizando o `Restricted Groups` GPO.

- Definições da política de acesso central

  Especifica uma lista de políticas de acesso central. As políticas de acesso central e as regras de política de acesso central associadas determinam permissões de acesso para vários arquivos no SVM.

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

"Auditoria de SMB e NFS e rastreamento de segurança"

Modificação das configurações de segurança Kerberos do servidor CIFS

Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Utilizar a assinatura SMB para melhorar a segurança da rede

Configuração da verificação transversal de derivação

Configurando restrições de acesso para usuários anônimos

Requisitos para usar GPOs com seu servidor SMB

Para usar objetos de diretiva de grupo (GPOs) com seu servidor SMB, o sistema deve atender a vários requisitos.

- O SMB deve ser licenciado no cluster. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.
- Um servidor SMB deve ser configurado e Unido a um domínio do ative Directory do Windows.
- O status de administrador do servidor SMB deve estar ativado.
- Os GPOs devem ser configurados e aplicados à Unidade organizacional do ative Directory (ou) do Windows que contém o objeto de computador servidor SMB.
- O suporte ao GPO deve estar ativado no servidor SMB.

Ative ou desative o suporte de GPO em um servidor CIFS

Você pode ativar ou desativar o suporte de GPO (Group Policy Object) em um servidor CIFS. Se você habilitar o suporte a GPO em um servidor CIFS, os GPOs aplicáveis definidos na diretiva de grupo - a diretiva aplicada à unidade organizacional (ou) que contém o objeto computador servidor CIFS - serão aplicados ao servidor CIFS.

Sobre esta tarefa

Os GPOs não podem ser ativados em servidores CIFS no modo de grupo de trabalho.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ativar GPOs	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
Desativar GPOs	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. Verifique se o suporte GPO está no estado desejado: `vserver cifs group-policy show -vserver +vserver_name_`

   O status da Diretiva de Grupo para servidores CIFS no modo de grupo de trabalho é exibido como "habilitado".

Exemplo

O exemplo a seguir habilita o suporte a GPO na máquina virtual de storage (SVM) VS1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

Informações relacionadas

GPOs compatíveis

Requisitos para usar GPOs com seu servidor CIFS

Como os GPOs são atualizados no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Exibindo informações sobre as configurações do GPO

Como os GPOs são atualizados no servidor SMB

Como os GPOs são atualizados na visão geral do servidor CIFS

Por padrão, o ONTAP recupera e aplica alterações de Objeto de Diretiva de Grupo (GPO) a cada 90 minutos. As configurações de segurança são atualizadas a cada 16 horas. Se você quiser atualizar os GPOs para aplicar novas configurações de política de

GPO antes que o ONTAP as atualize automaticamente, você pode acionar uma atualização manual em um servidor CIFS com um comando ONTAP.

- Por padrão, todos os GPOs são verificados e atualizados conforme necessário a cada 90 minutos.

  Este intervalo é configurável e pode ser definido utilizando as `Refresh interval` definições e `Random offset` GPO.

  O ONTAP consulta o ative Directory quanto a alterações nos GPOs. Se os números de versão do GPO registrados no ative Directory forem maiores do que os do servidor CIFS, o ONTAP recuperará e aplicará os novos GPOs. Se os números de versão forem os mesmos, os GPOs no servidor CIFS não serão atualizados.

- Os GPOs são atualizados a cada 16 horas.

  O ONTAP recupera e aplica GPOs de configurações de segurança a cada 16 horas, independentemente de estes GPOs terem sido alterados ou não.

  > O valor padrão de 16 horas não pode ser alterado na versão atual do ONTAP. É uma configuração padrão do cliente Windows.

- Todos os GPOs podem ser atualizados manualmente com um comando ONTAP.

  Este comando simula o comando Windows `gpupdate.exe`/force.

Informações relacionadas

Atualizar manualmente as definições de GPO no servidor CIFS

Atualizar manualmente as definições de GPO no servidor CIFS

Se pretender atualizar imediatamente as definições do GPO (Group Policy Object) no servidor CIFS, pode atualizar manualmente as definições. Você pode atualizar apenas as configurações alteradas ou forçar uma atualização para todas as configurações, incluindo as configurações que foram aplicadas anteriormente, mas não foram alteradas.

Passo

1. Execute a ação apropriada:

Se você quiser atualizar…	Digite o comando…
Definições GPO alteradas	`vserver cifs group-policy update -vserver` *`vserver_name`*
Todas as definições do GPO	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

Informações relacionadas

Como os GPOs são atualizados no servidor CIFS

Apresentar informações sobre as configurações do GPO

Você pode exibir informações sobre configurações de GPO (Group Policy Object) definidas no ative Directory e sobre configurações GPO aplicadas ao servidor CIFS.

Sobre esta tarefa

Você pode exibir informações sobre todas as configurações de GPO definidas no ative Directory do domínio ao qual o servidor CIFS pertence, ou você pode exibir informações apenas sobre as configurações de GPO aplicadas a um servidor CIFS.

Passos

1. Exiba informações sobre as configurações do GPO executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as configurações de Diretiva de Grupo…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy show-defined -vserver vserver_name`
Aplicado a uma máquina virtual de storage habilitada por CIFS (SVM)	`vserver cifs group-policy show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe as configurações de GPO definidas no ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
```

```
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
```

```
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

O exemplo a seguir exibe as configurações de GPO aplicadas ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Exibir informações detalhadas sobre GPOs de grupo restrito

Você pode exibir informações detalhadas sobre grupos restritos definidos como objetos de Diretiva de Grupo (GPOs) no ative Directory e aplicados ao servidor CIFS.

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome da política de grupo
- Versão da política de grupo
- Link

  Especifica o nível no qual a diretiva de grupo está configurada. Os possíveis valores de saída incluem o seguinte:

  - `Local` Quando a política de grupo é configurada no ONTAP
  - `Site` quando a política de grupo é configurada no nível do site no controlador de domínio
  - `Domain` quando a política de grupo é configurada no nível do domínio no controlador de domínio
  - `OrganizationalUnit` Quando a política de grupo é configurada no nível de unidade organizacional (ou) no controlador de domínio
  - `RSOP` para o conjunto resultante de políticas derivadas de todas as políticas de grupo definidas em vários níveis
- Nome do grupo restrito
- Os usuários e grupos que pertencem e que não pertencem ao grupo restrito

- A lista de grupos aos quais o grupo restrito é adicionado

  Um grupo pode ser membro de grupos que não sejam os listados aqui.

Passo

1. Exiba informações sobre todos os GPOs de grupo restrito executando uma das seguintes ações:

Se você quiser exibir informações sobre todos os GPOs de grupo restrito…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações sobre GPOs de grupo restrito definidos no domínio do ative Directory ao qual pertence o SVM habilitado para CIFS chamado VS1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
             MemberOf: EXAMPLE\group9
```

O exemplo a seguir exibe informações sobre GPOs de grupos restritos aplicados ao SVM VS1 habilitado para CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibir informações sobre políticas de acesso centrais

Você pode exibir informações detalhadas sobre as políticas de acesso central definidas no ative Directory. Você também pode exibir informações sobre as políticas de acesso central aplicadas ao servidor CIFS por meio de objetos de diretiva de grupo (GPOs).

Sobre esta tarefa

Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da política de acesso central
- SID
- Descrição
- Tempo de criação
- Tempo de modificação
- Regras dos membros

> Os servidores CIFS no modo de grupo de trabalho não são exibidos porque não suportam GPOs.

Passo

1. Exiba informações sobre políticas de acesso central executando uma das seguintes ações:

Se você quiser exibir informações sobre todas as políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-policy show-defined -vserver` *vserver_name*
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-policy show-applied -vserver` *vserver_name*

Exemplo

O exemplo a seguir exibe informações de todas as políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

O exemplo a seguir exibe informações de todas as políticas de acesso central aplicadas às máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                 SID
-------- --------------------
----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre as regras da política de acesso central

Exibir informações sobre as regras da política de acesso central

Você pode exibir informações detalhadas sobre regras de política de acesso central associadas a políticas de acesso centrais definidas no ative Directory. Você também pode exibir informações sobre regras de políticas de acesso centrais aplicadas ao servidor CIFS por meio de GPOs de diretiva de acesso central (objetos de diretiva de grupo).

Sobre esta tarefa

Você pode exibir informações detalhadas sobre regras de política de acesso central definidas e aplicadas. Por padrão, as seguintes informações são exibidas:

- Nome do SVM
- Nome da regra de acesso central
- Descrição
- Tempo de criação
- Tempo de modificação
- Permissões atuais

- Permissões propostas
- Direcionar recursos

Se você quiser exibir informações sobre todas as regras de política de acesso central associadas às políticas de acesso central…	Digite o comando…
Definido no ative Directory	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
Aplicado a um servidor CIFS	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

Exemplo

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central definidas no ative Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver    Name
---------- --------------------
vs1        r1
           Description: rule #1
         Creation Time: Tue Oct 22 09:33:48 2013
     Modification Time: Tue Oct 22 09:33:48 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1        r2
           Description: rule #2
         Creation Time: Tue Oct 22 10:27:57 2013
     Modification Time: Tue Oct 22 10:27:57 2013
   Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
  Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

O exemplo a seguir exibe informações de todas as regras de política de acesso central associadas às políticas de acesso central aplicadas a máquinas virtuais de armazenamento (SVMs) no cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
            Description: rule #1
          Creation Time: Tue Oct 22 09:33:48 2013
      Modification Time: Tue Oct 22 09:33:48 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
            Description: rule #2
          Creation Time: Tue Oct 22 10:27:57 2013
      Modification Time: Tue Oct 22 10:27:57 2013
    Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
   Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Informações relacionadas

Protegendo o acesso aos arquivos usando o controle de acesso dinâmico (DAC)

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Comandos para gerenciar senhas de contas de computador de servidores SMB

Você precisa saber os comandos para alterar, redefinir e desativar senhas e para configurar agendas de atualização automática. Você também pode configurar um agendamento no servidor SMB para atualizá-lo automaticamente.

Se você quiser…	Use este comando…
Altere a senha da conta de domínio quando o ONTAP estiver sincronizado com os serviços do AD	`vserver cifs domain password change`
Redefina a senha da conta de domínio quando o ONTAP não estiver sincronizado com os serviços do AD	`vserver cifs domain password reset`
Configurar servidores SMB para alterações automáticas de senha de conta de computador	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`

Se você quiser…	Use este comando…
Desativar alterações automáticas de senha de conta de computador em servidores SMB	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

Consulte a página de manual de cada comando para obter mais informações.

Gerenciar conexões do controlador de domínio

Exibir informações sobre servidores descobertos

Você pode exibir informações relacionadas a servidores LDAP e controladores de domínio descobertos em seu servidor CIFS.

Passo

1. Para exibir informações relacionadas aos servidores descobertos, digite o seguinte comando: `vserver cifs domain discovered-servers show`

Exemplo

O exemplo a seguir mostra os servidores descobertos para o SVM VS1:

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

Redefinir e redescobrir servidores

Parar ou iniciar o servidor CIFS

Redefinir e redescobrir servidores

Redefinir e redescobrir servidores no servidor CIFS permite que o servidor CIFS descarte informações armazenadas sobre servidores LDAP e controladores de domínio. Depois de descartar as informações do servidor, o servidor CIFS readquire as informações atuais sobre esses servidores externos. Isso pode ser útil quando os servidores conetados não estão respondendo adequadamente.

Passos

1. Introduza o seguinte comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Exibir informações sobre os servidores recém-redescobertos: `vserver cifs domain discovered-servers show -vserver vserver_name`

Exemplo

O exemplo a seguir redefine e redescobre servidores para máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address    Status
--------------- -------- ---------- ----------- ------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4       OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5       OK
example.com     MS-DC    adequate   DC-1        1.1.3.4       OK
example.com     MS-DC    adequate   DC-2        1.1.3.5       OK
```

Informações relacionadas

Exibindo informações sobre servidores descobertos

Parar ou iniciar o servidor CIFS

Gerenciar a descoberta do controlador de domínio

A partir do ONTAP 9.3, você pode modificar o processo padrão pelo qual controladores de domínio (DCs) são descobertos. Isso permite limitar a descoberta ao seu site ou a um pool de DCs preferenciais, o que pode levar a melhorias de desempenho, dependendo do ambiente.

Sobre esta tarefa

Por padrão, o processo de descoberta dinâmica descobre todos os DCs disponíveis, incluindo todos os DCs preferenciais, todos os DCs no local e todos os DCs remotos. Essa configuração pode levar à latência na autenticação e ao acesso a compartilhamentos em determinados ambientes. Se você já determinou o pool de DCs que deseja usar, ou se os DCs remotos são inadequados ou inacessíveis, você pode alterar o método de descoberta.

No ONTAP 9.3 e versões posteriores, o `discovery-mode` parâmetro `cifs domain discovered-servers` do comando permite selecionar uma das seguintes opções de descoberta:

- Todos os DCs no domínio são descobertos.

- Apenas DCs no local são descobertos.

  O `default-site` parâmetro para o servidor SMB pode ser definido para usar esse modo com LIFs que não são atribuídos a um site em sites e serviços.

- A deteção de servidor não é realizada, a configuração do servidor SMB depende apenas de DCs preferenciais.

  Para utilizar este modo, tem de definir primeiro os DCs preferidos para o servidor SMB.

Antes de começar

Você deve estar no nível de privilégio avançado.

Passo

1. Especifique a opção de descoberta desejada: `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   Opções para o `mode` parâmetro:

   - `all`

     Descubra todos os DCs disponíveis (padrão).

   - `site`

     Limite a descoberta DC ao seu site.

   - `none`

     Use apenas DCs preferenciais e não execute a descoberta.

Adicione controladores de domínio preferenciais

O ONTAP descobre automaticamente controladores de domínio através do DNS. Opcionalmente, você pode adicionar um ou mais controladores de domínio à lista de controladores de domínio preferenciais para um domínio específico.

Sobre esta tarefa

Se já existir uma lista de controlador de domínio preferencial para o domínio especificado, a nova lista será mesclada com a lista existente.

Passo

1. Para adicionar à lista de controladores de domínio preferenciais, digite o seguinte comando `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

   `-vserver` *`vserver_name`* Especifica o nome da máquina virtual de storage (SVM).

   `-domain` *`domain_name`* Especifica o nome totalmente qualificado do ative Directory do domínio ao qual pertencem os controladores de domínio especificados.

`-preferred-dc IP_address`,... especifica um ou mais endereços IP dos controladores de domínio preferidos, como uma lista delimitada por vírgulas, por ordem de preferência.

Exemplo

O comando a seguir adiciona controladores de domínio 172.17.102.25 e 172.17.102.24 à lista de controladores de domínio preferenciais que o servidor SMB no SVM VS1 usa para gerenciar o acesso externo ao domínio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

Informações relacionadas

Comandos para gerenciar controladores de domínio preferenciais

Comandos para gerenciar controladores de domínio preferenciais

Você precisa saber os comandos para adicionar, exibir e remover controladores de domínio preferenciais.

Se você quiser…	Use este comando…
Adicione um controlador de domínio preferido	`vserver cifs domain preferred-dc add`
Exibir controladores de domínio preferenciais	`vserver cifs domain preferred-dc show`
Remova um controlador de domínio preferido	`vserver cifs domain preferred-dc remove`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

Adicionando controladores de domínio preferenciais

Ative as conexões SMB2 aos controladores de domínio

A partir do ONTAP 9.1, você pode habilitar o SMB versão 2,0 para se conetar a um controlador de domínio. Isso é necessário se você desativou o SMB 1,0 em controladores de domínio. A partir do ONTAP 9.2, o SMB2 é ativado por predefinição.

Sobre esta tarefa

A `smb2-enabled-for-dc-connections` opção de comando ativa o padrão do sistema para o lançamento do ONTAP que você está usando. O padrão do sistema para o ONTAP 9.1 está ativado para o SMB 1,0 e desativado para o SMB 2,0. O padrão do sistema para o ONTAP 9.2 está habilitado para o SMB 1,0 e habilitado para o SMB 2,0. Se o controlador de domínio não puder negociar o SMB 2,0 inicialmente, ele usará o SMB 1,0.

O SMB 1,0 pode ser desativado do ONTAP para um controlador de domínio. No ONTAP 9.1, se o SMB 1,0 tiver sido desativado, o SMB 2,0 deve ser ativado para se comunicar com um controlador de domínio.

Saiba mais sobre:

- "Verificando versões SMB ativadas".
- "Versões e funcionalidade SMB compatíveis".

> Se `-smb1-enabled-for-dc-connections` estiver definido como `false` enquanto `-smb1-enabled` estiver definido como `true`, o ONTAP nega conexões SMB 1,0 como cliente, mas continua a aceitar conexões SMB 1,0 de entrada como servidor.

Passos

1. Antes de alterar as configurações de segurança SMB, verifique quais versões SMB estão ativadas: `vserver cifs security show`
2. Role a lista para baixo para ver as versões SMB.
3. Execute o comando apropriado, usando a `smb2-enabled-for-dc-connections` opção.

Se você quiser que SMB2 seja…	Digite o comando…
Ativado	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc-connections true`
Desativado	`vserver cifs security modify -vserver` *`vserver_name`* `-smb2-enabled-for-dc-connections false`

Ative conexões criptografadas para controladores de domínio

A partir do ONTAP 9.8, você pode especificar que as conexões aos controladores de domínio sejam criptografadas.

Sobre esta tarefa

O ONTAP requer criptografia para comunicações de controlador de domínio (DC) quando a `-encryption-required-for-dc-connection` opção está definida como `true`; o padrão é `false`. Quando a opção está definida, apenas o protocolo SMB3 será utilizado para ligações ONTAP-DC, uma vez que a encriptação é suportada apenas pelo SMB3.

Quando as comunicações CC criptografadas são necessárias, a `-smb2-enabled-for-dc-connections` opção é ignorada, porque o ONTAP negocia somente conexões SMB3. Se um DC não suportar SMB3 e criptografia, o ONTAP não se conetará a ele.

Passo

1. Ative a comunicação encriptada com o DC: `vserver cifs security modify -vserver` *`svm_name`* `-encryption-required-for-dc-connection true`

Use sessões nulas para acessar o armazenamento em ambientes não Kerberos

Use sessões nulas para acessar o armazenamento na visão geral de ambientes não Kerberos

O acesso de sessão nula fornece permissões para recursos de rede, como dados do sistema de armazenamento de dados, e para serviços baseados em cliente executados no sistema local. Uma sessão nula ocorre quando um processo de cliente usa a conta "system" para acessar um recurso de rede. A configuração de sessão nula é específica para autenticação não Kerberos.

Como o sistema de armazenamento fornece acesso nulo à sessão

Como compartilhamentos de sessão nulos não exigem autenticação, os clientes que exigem acesso de sessão null devem ter seus endereços IP mapeados no sistema de armazenamento.

Por padrão, os clientes de sessão nula não mapeados podem acessar determinados serviços do sistema ONTAP, como enumeração de compartilhamento, mas eles são restritos a acessar quaisquer dados do sistema de storage.

> O ONTAP suporta os valores de configuração do Registro anônimo do Windows com a `-restrict-anonymous` opção. Isso permite controlar até que ponto os usuários nulos não mapeados podem exibir ou acessar recursos do sistema. Por exemplo, você pode desativar a enumeração de compartilhamento e o acesso ao compartilhamento IPC (o compartilhamento de pipe nomeado oculto). As `vserver cifs options modify` páginas de manual e `vserver cifs options show` fornecem mais informações sobre a `-restrict-anonymous` opção.

A menos que configurado de outra forma, um cliente executando um processo local que solicita acesso ao sistema de armazenamento por meio de uma sessão nula é membro apenas de grupos não restritivos, como "'todos'". Para limitar o acesso de sessão nula a recursos selecionados do sistema de armazenamento, você pode querer criar um grupo ao qual todos os clientes de sessão nula pertencem; a criação deste grupo permite restringir o acesso ao sistema de armazenamento e definir permissões de recursos do sistema de armazenamento que se aplicam especificamente a clientes de sessão nula.

O ONTAP fornece uma sintaxe de mapeamento no `vserver name-mapping` conjunto de comandos para especificar o endereço IP dos clientes que têm acesso permitido aos recursos do sistema de armazenamento usando uma sessão de usuário nula. Depois de criar um grupo para usuários nulos, você pode especificar restrições de acesso para recursos do sistema de armazenamento e permissões de recursos que se aplicam somente a sessões nulas. O usuário nulo é identificado como logon anônimo. Os usuários nulos não têm acesso a nenhum diretório home.

Qualquer usuário nulo que acesse o sistema de armazenamento a partir de um endereço IP mapeado recebe permissões de usuário mapeadas. Considere as precauções apropriadas para evitar o acesso não autorizado aos sistemas de armazenamento mapeados com usuários nulos. Para máxima proteção, coloque o sistema de armazenamento e todos os clientes que necessitem de acesso nulo ao sistema de armazenamento de utilizadores numa rede separada, para eliminar a possibilidade de "spoofing" de endereço IP.

Informações relacionadas

Configurando restrições de acesso para usuários anônimos

Conceder acesso a usuários nulos a compartilhamentos de sistema de arquivos

Você pode permitir o acesso aos recursos do seu sistema de armazenamento por clientes de sessão nulos, atribuindo um grupo a ser usado por clientes de sessão nulos e

registrando os endereços IP de clientes de sessão nulos para adicionar à lista de clientes com permissão para acessar dados usando sessões nulas.

Passos

1. Use o `vserver name-mapping create` comando para mapear o usuário nulo para qualquer usuário válido do Windows, com um qualificador IP.

   O comando a seguir mapeia o usuário nulo para user1 com um nome de host válido google.com:

   ```
   vserver name-mapping create –direction win-unix  -position 1 –pattern
   “ANONYMOUS LOGON” –replacement user1 – hostname google.com
   ```

   O comando a seguir mapeia o usuário nulo para user1 com um endereço IP válido 10.238.2.54/32:

   ```
   vserver name-mapping create –direction win-unix  -position 2 –pattern
   “ANONYMOUS LOGON” –replacement user1 –address 10.238.2.54/32
   ```

2. Use o `vserver name-mapping show` comando para confirmar o mapeamento de nomes.

   ```
   vserver name-mapping show

   Vserver:   vs1
   Direction: win-unix
   Position Hostname         IP Address/Mask
   -------- --------         ----------------
   1       -                 10.72.40.83/32      Pattern: anonymous logon
                                              Replacement: user1
   ```

3. Use o `vserver cifs options modify –win-name-for-null-user` comando para atribuir a associação do Windows ao usuário nulo.

   Essa opção é aplicável somente quando há um mapeamento de nome válido para o usuário nulo.

   ```
   vserver cifs options modify -win-name-for-null-user user1
   ```

4. Use o `vserver cifs options show` comando para confirmar o mapeamento do usuário nulo para o usuário ou grupo do Windows.

   ```
   vserver cifs options show

   Vserver :vs1

   Map Null User to Windows User of Group: user1
   ```

Gerencie aliases NetBIOS para servidores SMB

Gerenciar aliases NetBIOS para servidores SMB

Os aliases NetBIOS são nomes alternativos para o servidor SMB que os clientes SMB podem usar ao se conetar ao servidor SMB. A configuração de aliases NetBIOS para um servidor SMB pode ser útil quando você está consolidando dados de outros servidores de arquivos para o servidor SMB e deseja que o servidor SMB responda aos nomes dos servidores de arquivos originais.

Você pode especificar uma lista de aliases NetBIOS ao criar o servidor SMB ou a qualquer momento depois de criar o servidor SMB. Você pode adicionar ou remover aliases NetBIOS da lista a qualquer momento. Você pode se conetar ao servidor SMB usando qualquer um dos nomes na lista de alias do NetBIOS.

Informações relacionadas

Exibindo informações sobre NetBIOS sobre conexões TCP

Adicione uma lista de aliases NetBIOS ao servidor SMB

Se você quiser que os clientes SMB se conetem ao servidor SMB usando um alias, você pode criar uma lista de aliases NetBIOS ou adicionar aliases NetBIOS a uma lista existente de aliases NetBIOS.

Sobre esta tarefa

- O nome de alias NetBIOS pode ter 15 até carateres de comprimento.
- Você pode configurar até 200 aliases NetBIOS no servidor SMB.
- Não são permitidos os seguintes carateres:
- ( ) [ ] | ; : " , > / ?

Passos

1. Adicione os aliases NetBIOS
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - Você pode especificar um ou mais aliases NetBIOS usando uma lista delimitada por vírgulas.
   - Os aliases NetBIOS especificados são adicionados à lista existente.
   - Uma nova lista de aliases NetBIOS é criada se a lista estiver vazia no momento.
2. Verifique se os aliases NetBIOS foram adicionados corretamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Informações relacionadas

Removendo aliases NetBIOS da lista de alias NetBIOS

Exibindo a lista de aliases NetBIOS em servidores CIFS

Remova os aliases NetBIOS da lista de alias NetBIOS

Se você não precisar de aliases NetBIOS específicos para um servidor CIFS, você poderá remover esses aliases NetBIOS da lista. Você também pode remover todos os aliases NetBIOS da lista.

Sobre esta tarefa

Você pode remover mais de um alias NetBIOS usando uma lista delimitada por vírgulas. Você pode remover todos os aliases NetBIOS em um servidor CIFS especificando - como o valor para o `-netbios-aliases` parâmetro.

Passos

1. Execute uma das seguintes ações:

Se você quiser remover…	Digite…
Aliases NetBIOS específicos da lista	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
Todos os aliases NetBIOS da lista	`vserver cifs remove-netbios-aliases -vserver` *`vserver_name`* `-netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verifique se os aliases NetBIOS especificados foram removidos: `vserver cifs show -vserver` *`vserver_name`* `-display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

Exiba a lista de aliases NetBIOS em servidores CIFS

Você pode exibir a lista de aliases NetBIOS. Isso pode ser útil quando você deseja determinar a lista de nomes sobre os quais clientes SMB podem fazer conexões com o servidor CIFS.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite…
Os aliases NetBIOS de um servidor CIFS	`vserver cifs show -display-netbios -aliases`
A lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS	`vserver cifs show -instance`

O exemplo a seguir exibe informações sobre os aliases NetBIOS de um servidor CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

O exemplo a seguir exibe a lista de aliases NetBIOS como parte das informações detalhadas do servidor CIFS:

```
vserver cifs show -instance
```

```
                                    Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_SERVER
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                           Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Consulte a página de manual para obter mais informações.

Informações relacionadas

Adicionando uma lista de aliases NetBIOS ao servidor CIFS

Determine se os clientes SMB estão conetados usando aliases NetBIOS

Você pode determinar se os clientes SMB estão conetados usando aliases NetBIOS e, em caso afirmativo, qual alias NetBIOS é usado para fazer a conexão. Isso pode ser útil ao solucionar problemas de conexão.

Sobre esta tarefa

Você deve usar o `-instance` parâmetro para exibir o alias NetBIOS (se houver) associado a uma conexão SMB. Se o nome do servidor CIFS ou um endereço IP for usado para fazer a conexão SMB, a saída para o `NetBIOS Name` campo é - (hífen).

Passo

1. Execute a ação desejada:

Se você quiser exibir informações do NetBIOS para…	Digite…
Conexões SMB	`vserver cifs session show -instance`
Conexões usando um alias NetBIOS especificado:	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

O exemplo a seguir exibe informações sobre o alias NetBIOS usado para fazer a conexão SMB com o Session ID 1:

```
vserver cifs session show -session-id 1 -instance
```

```
                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
                 Workstation: 10.2.2.50
    Authentication Mechanism: NTLMv2
                Windows User: EXAMPLE\user1
                   UNIX User: user1
                 Open Shares: 2
                  Open Files: 2
                  Open Other: 0
              Connected Time: 1d 1h 10m 5s
                   Idle Time: 22s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: ALIAS1
       SMB Encryption Status: Unencrypted
```

Gerenciar diversas tarefas de servidor SMB

Pare ou inicie o servidor CIFS

Você pode parar o servidor CIFS em uma SVM, que pode ser útil na execução de tarefas enquanto os usuários não acessam dados por compartilhamentos SMB. Você pode reiniciar o acesso SMB iniciando o servidor CIFS. Ao parar o servidor CIFS, você também pode modificar os protocolos permitidos na máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Pare o servidor CIFS	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	Inicie o servidor CIFS
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` especifica se o comando deve ser executado em primeiro plano ou em segundo plano. Se você não inserir esse parâmetro, ele será definido como `true`, e o comando será executado em primeiro plano.

2. Verifique se o status administrativo do servidor CIFS está correto usando o `vserver cifs show` comando.

Exemplo

Os comandos a seguir iniciam o servidor CIFS no SVM VS1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

Informações relacionadas

Exibindo informações sobre servidores descobertos

Redefinir e redescobrir servidores

Mova servidores CIFS para diferentes OUs

O processo de criação do servidor CIFS usa a unidade organizacional padrão (ou) CN de computadores durante a configuração, a menos que você especifique uma ou diferente. Você pode mover servidores CIFS para diferentes OUs após a configuração.

Passos

1. No servidor Windows, abra a árvore **usuários e computadores do ative Directory**.
2. Localize o objeto do ative Directory da máquina virtual de storage (SVM).
3. Clique com o botão direito do rato no objeto e selecione **mover**.
4. Selecione a UO que você deseja associar ao SVM

Resultados

O objeto SVM é colocado na UO selecionada.

Modifique o domínio DNS dinâmico na SVM antes de mover o servidor SMB

Se desejar que o servidor DNS integrado ao ative Directory Registre dinamicamente os Registros DNS do servidor SMB no DNS ao mover o servidor SMB para outro domínio, você deve modificar DNS dinâmico (DDNS) na máquina virtual de armazenamento (SVM) antes de mover o servidor SMB.

Antes de começar

Os serviços de nomes DNS devem ser modificados no SVM para usar o domínio DNS que contém os

Registros de localização do serviço para o novo domínio que conterá a conta de computador do servidor SMB. Se você estiver usando DDNS seguro, você deve usar servidores de nomes DNS integrados ao ative Directory.

Sobre esta tarefa

Embora o DDNS (se configurado no SVM) adicione automaticamente os Registros DNS para LIFs de dados ao novo domínio, os Registros DNS para o domínio original não são excluídos automaticamente do servidor DNS original. Você deve excluí-los manualmente.

Para concluir as modificações do DDNS antes de mover o servidor SMB, consulte o seguinte tópico:

"Configurar serviços DNS dinâmicos"

Ingressar em um SVM em um domínio do active Directory

É possível associar uma máquina virtual de armazenamento (SVM) a um domínio do ative Directory sem excluir o servidor SMB existente, modificando o domínio usando o `vserver cifs modify` comando. Você pode ingressar novamente no domínio atual ou ingressar em um novo.

Antes de começar

- O SVM já deve ter uma configuração de DNS.
- A configuração DNS do SVM deve ser capaz de servir o domínio de destino.

  Os servidores DNS têm de conter os registos de localização de serviço (SRV) para os servidores LDAP de domínio e controlador de domínio.

Sobre esta tarefa

- O status administrativo do servidor CIFS deve ser definido como "próprio" para prosseguir com a modificação de domínio do ative Directory.
- Se o comando for concluído com êxito, o status administrativo será automaticamente definido como "'up"'.
- Ao ingressar em um domínio, esse comando pode levar vários minutos para ser concluído.

Passos

1. Junte-se ao SVM ao domínio do servidor CIFS: `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   Para obter mais informações, consulte a página man para o `vserver cifs modify` comando. Se você precisar reconfigurar o DNS para o novo domínio, consulte a página de manual do `vserver dns modify` comando.

   Para criar uma conta de máquina do ative Directory para o servidor SMB, você deve fornecer o nome e a senha de uma conta do Windows com Privileges suficiente para adicionar computadores ao `ou=` *`example`* `ou` contentor dentro do *`example`* domínio .com.

   A partir do ONTAP 9.7, o administrador do AD pode fornecer um URI para um arquivo keytab como alternativa para fornecer um nome e uma senha para uma conta privilegiada do Windows. Quando receber o URI, inclua-o `-keytab-uri` no parâmetro com os `vserver cifs` comandos.

2. Verifique se o servidor CIFS está no domínio desejado do ative Directory: `vserver cifs show`

Exemplo

No exemplo a seguir, o servidor SMB "'CIFSSERVER1"" no SVM VS1 junta o domínio example.com usando autenticação keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE           domain
```

Exibir informações sobre NetBIOS sobre conexões TCP

Você pode exibir informações sobre conexões NetBIOS sobre TCP (NBT). Isso pode ser útil ao solucionar problemas relacionados ao NetBIOS.

Passo

1. Use o `vserver cifs nbtstat` comando para exibir informações sobre NetBIOS sobre conexões TCP.

   O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Exemplo

O exemplo a seguir mostra as informações do serviço de nomes NetBIOS exibidas para "'cluster1":

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

Comandos para gerenciar servidores SMB

Você precisa saber os comandos para criar, exibir, modificar, parar, iniciar e excluir servidores SMB. Há também comandos para redefinir e redescobrir servidores, alterar ou redefinir senhas de conta de máquina, agendar alterações para senhas de conta de máquina e adicionar ou remover aliases NetBIOS.

Se você quiser…	Use este comando…
Crie um servidor SMB	`vserver cifs create`
Exibir informações sobre um servidor SMB	`vserver cifs show`
Modifique um servidor SMB	`vserver cifs modify`
Mova um servidor SMB para outro domínio	`vserver cifs modify`

Parar um servidor SMB	`vserver cifs stop`
Inicie um servidor SMB	`vserver cifs start`
Excluir um servidor SMB	`vserver cifs delete`
Redefinir e redescobrir servidores para o servidor SMB	`vserver cifs domain discovered-servers reset-servers`
Altere a senha da conta de máquina do servidor SMB	`vserver cifs domain password change`
Redefina a senha da conta da máquina do servidor SMB	`vserver cifs domain password change`
Agendar alterações automáticas de senha para a conta de máquina do servidor SMB	`vserver cifs domain password schedule modify`
Adicione aliases NetBIOS para o servidor SMB	`vserver cifs add-netbios-aliases`
Remova os aliases NetBIOS para o servidor SMB	`vserver cifs remove-netbios-aliases`

Consulte a página de manual de cada comando para obter mais informações.

Informações relacionadas

"O que acontece com usuários e grupos locais ao excluir servidores SMB"

Ative o serviço de nomes NetBIOS

Começando com ONTAP 9, o serviço de nomes NetBIOS (NBNS, às vezes chamado de Serviço de nomes de Internet do Windows ou WINS) é desativado por padrão. Anteriormente, as máquinas virtuais de armazenamento (SVMs) habilitadas por CIFS enviavam transmissões de Registro de nomes, independentemente de o WINS estar habilitado em uma rede. Para limitar tais transmissões a configurações em que o NBNS é necessário, você deve habilitar o NBNS explicitamente para novos servidores CIFS.

Antes de começar

- Se você já estiver usando NBNS e atualizar para o ONTAP 9, não é necessário concluir esta tarefa. NBNS continuará a funcionar como antes.
- O NBNS é ativado por UDP (porta 137).
- NBNS sobre IPv6 não é suportado.

Passos

1. Defina o nível de privilégio como avançado.

```
set -privilege advanced
```

2. Ative NBNS em um servidor CIFS.

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. Retorne ao nível de privilégio de administrador.

```
set -privilege admin
```

Use o IPv6 para acesso SMB e serviços SMB

Requisitos para usar IPv6

Antes de poder usar o IPv6 no servidor SMB, você precisa saber quais versões do ONTAP e SMB o suportam e quais são os requisitos de licença.

Requisitos de licença do ONTAP

Nenhuma licença especial é necessária para o IPv6 quando o SMB é licenciado. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a IPv6 em todas as versões do protocolo SMB.

O serviço de nomes NetBIOS (NBNS) em IPv6 não é suportado.

Suporte para IPv6 com acesso SMB e serviços CIFS

Se você quiser usar o IPv6 em seu servidor CIFS, você precisa estar ciente de como o ONTAP suporta o IPv6 para acesso SMB e comunicação de rede para serviços CIFS.

Suporte ao cliente e servidor Windows

O ONTAP fornece suporte para servidores e clientes Windows que suportam IPv6. A seguir descreve o suporte ao cliente e servidor Microsoft Windows IPv6:

- O Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e posterior suportam o IPv6 para serviços de partilha de ficheiros SMB e ative Directory, incluindo DNS, LDAP, CLDAP e Kerberos.

  Se os endereços IPv6 estiverem configurados, o Windows 7 e o Windows Server 2008 e versões posteriores usam o IPv6 por padrão para serviços do ative Directory. Tanto a autenticação NTLM como Kerberos através de conexões IPv6 são suportadas.

Todos os clientes Windows suportados pelo ONTAP podem se conetar a compartilhamentos SMB usando endereços IPv6.

Para obter as informações mais recentes sobre quais clientes Windows ONTAP suportam, consulte "Matriz de interoperabilidade".

Os domínios NT não são suportados para IPv6.

Suporte adicional a serviços CIFS

Além do suporte IPv6 para compartilhamentos de arquivos SMB e serviços do ative Directory, o ONTAP oferece suporte IPv6 para o seguinte:

- Serviços do lado do cliente, incluindo pastas offline, perfis de roaming, redirecionamento de pastas e versões anteriores
- Serviços do lado do servidor, incluindo diretórios base dinâmicos (recurso Home Directory), links simbólicos e Widelinks, BranchCache, descarga de cópia ODX, referências automáticas de nós e versões anteriores
- Serviços de gerenciamento de acesso a arquivos, incluindo o uso de usuários e grupos locais do Windows para controle de acesso e gerenciamento de direitos, configuração de permissões de arquivos e políticas de auditoria usando a CLI, rastreamento de segurança, gerenciamento de bloqueios de arquivos e monitoramento de atividades SMB
- Auditoria multiprotocolo nas
- FPolicy
- Compartilhamentos continuamente disponíveis, protocolo de testemunha e VSS remoto (usado com configurações Hyper-V em SMB)

Serviço de nomes e suporte de serviços de autenticação

A comunicação com os seguintes serviços de nome é suportada com o IPv6:

- Controladores de domínio
- Servidores DNS
- Servidores LDAP
- Servidores KDC
- Servidores NIS

Como os servidores CIFS usam o IPv6 para se conetar a servidores externos

Para criar uma configuração que atenda aos seus requisitos, você deve estar ciente de como os servidores CIFS usam o IPv6 ao fazer conexões com servidores externos.

- Seleção do endereço de origem

  Se for feita uma tentativa de ligação a um servidor externo, o endereço de origem selecionado tem de ser do mesmo tipo que o endereço de destino. Por exemplo, se estiver conetando a um endereço IPv6, a máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS deve ter um LIF de dados ou LIF de gerenciamento que tenha um endereço IPv6 para usar como endereço de origem. Da mesma forma, se estiver conetando a um endereço IPv4, o SVM precisa ter um LIF de dados ou um LIF de gerenciamento

que tenha um endereço IPv4 para usar como endereço de origem.

- Para servidores dinamicamente descobertos usando DNS, a descoberta do servidor é executada da seguinte forma:
  - Se o IPv6 estiver desativado no cluster, apenas serão detetados IPv4 endereços de servidores.
  - Se IPv6 estiver ativado no cluster, os endereços de servidor IPv4 e IPv6 serão descobertos. Qualquer tipo pode ser usado dependendo da adequação do servidor ao qual o endereço pertence e da disponibilidade de dados IPv6 ou IPv4 ou LIFs de gerenciamento. A descoberta dinâmica de servidor é usada para descobrir controladores de domínio e seus serviços associados, como LSA, NETLOGON, Kerberos e LDAP.
- Conetividade do servidor DNS

  Se o SVM usa IPv6 ao se conetar a um servidor DNS depende da configuração dos serviços de nome DNS. Se os serviços DNS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes DNS pode usar endereços IPv4 para que as conexões com servidores DNS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes DNS.

- Conetividade do servidor LDAP

  Se o SVM usa IPv6 ao se conetar a um servidor LDAP depende da configuração do cliente LDAP. Se o cliente LDAP estiver configurado para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração do cliente LDAP pode usar endereços IPv4 para que as conexões com servidores LDAP continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar a configuração do cliente LDAP.

  > A configuração do cliente LDAP é usada ao configurar o LDAP para serviços de nome de usuário, grupo e netgroup UNIX.

- Conetividade do servidor NIS

  Se o SVM usa IPv6 ao conetar-se a um servidor NIS depende da configuração dos serviços de nome NIS. Se os serviços NIS estiverem configurados para usar endereços IPv6, as conexões serão feitas usando IPv6. Se desejar, a configuração dos serviços de nomes NIS pode usar endereços IPv4 para que as conexões com servidores NIS continuem a usar endereços IPv4. Combinações de endereços IPv4 e IPv6 podem ser especificadas ao configurar serviços de nomes NIS.

  > Os serviços de nomes NIS são usados para armazenar e gerenciar objetos de nome de usuário, grupo, netgroup e host UNIX.

Informações relacionadas

Habilitação do IPv6 para SMB (somente administradores de cluster)

Monitoramento e exibição de informações sobre IPv6 sessões SMB

Ativar o IPv6 para SMB (somente administradores de cluster)

As redes IPv6 não estão ativadas durante a configuração do cluster. Um administrador de cluster deve habilitar o IPv6 após a conclusão da configuração do cluster para usar o IPv6 para SMB. Quando o administrador do cluster ativa o IPv6, ele é ativado para todo o cluster.

Passo

1. Ativar IPv6: `network options ipv6 modify -enabled true`

   Para obter mais informações sobre como ativar o IPv6 no cluster e configurar LIFs IPv6, consulte o *Network Management Guide*.

   IPv6 está ativado. LIFs de dados IPv6 para acesso SMB podem ser configurados.

Informações relacionadas

Monitoramento e exibição de informações sobre IPv6 sessões SMB

"Gerenciamento de rede"

Desativar IPv6 para SMB

Mesmo que IPv6 esteja habilitado no cluster usando uma opção de rede, você não pode desabilitar IPv6 para SMB usando o mesmo comando. Em vez disso, o ONTAP desativa o IPv6 quando o administrador do cluster desativa a última interface habilitada para IPv6 no cluster. Você deve se comunicar com o administrador do cluster sobre o gerenciamento de suas interfaces IPv6 habilitadas.

Para obter mais informações sobre a desativação do IPv6 no cluster, consulte o *Network Management Guide*.

Informações relacionadas

"Gerenciamento de rede"

Monitore e exiba informações sobre IPv6 sessões SMB

Você pode monitorar e exibir informações sobre sessões SMB conetadas usando redes IPv6G. Essas informações são úteis para determinar quais clientes estão se conetando usando o IPv6, bem como outras informações úteis sobre sessões SMB do IPv6.

Passo

1. Execute a ação desejada:

Se você quiser determinar se…	Digite o comando…
As sessões de SMB a uma máquina virtual de storage (SVM) são conetadas usando o IPv6	`vserver cifs session show -vserver` *`vserver_name`* `-instance`
IPv6 é usado para sessões SMB através de um endereço LIF especificado	`vserver cifs session show -vserver` *`vserver_name`* `-lif-address` *`LIF_IP_address`* `-instance` *`LIF_IP_address`* É o endereço IPv6 do LIF de dados.

Configure o acesso a arquivos usando SMB

Configurar estilos de segurança

Como os estilos de segurança afetam o acesso aos dados

Estilos de segurança e seus efeitos

Existem quatro estilos de segurança diferentes: UNIX, NTFS, misto e unificado. Cada estilo de segurança tem um efeito diferente sobre como as permissões são tratadas para os dados. Você deve entender os diferentes efeitos para garantir que você selecione o estilo de segurança apropriado para seus propósitos.

É importante entender que os estilos de segurança não determinam quais tipos de clientes podem ou não acessar dados. Os estilos de segurança determinam apenas o tipo de permissões que o ONTAP usa para controlar o acesso aos dados e que tipo de cliente pode modificar essas permissões.

Por exemplo, se um volume usa estilo de segurança UNIX, os clientes SMB ainda podem acessar dados (desde que autentiquem e autorizem adequadamente) devido à natureza multiprotocolo do ONTAP. No entanto, o ONTAP usa permissões UNIX que somente clientes UNIX podem modificar usando ferramentas nativas.

Estilo de segurança	Clientes que podem modificar permissões	Permissões que os clientes podem usar	Estilo de segurança eficaz resultante	Clientes que podem acessar arquivos
UNIX	NFS	NFSv3 bits de modo	UNIX	NFS e SMB
		ACLs NFSv4.x		
NTFS	SMB	ACLs NTFS	NTFS	
Misto	NFS ou SMB	NFSv3 bits de modo	UNIX	
		NFSv4.ACLs		
		ACLs NTFS	NTFS	
Unificado (somente para volumes infinitos, no ONTAP 9.4 e versões anteriores).	NFS ou SMB	NFSv3 bits de modo	UNIX	
		ACLs NFSv4,1		
		ACLs NTFS	NTFS	

Os volumes FlexVol suportam estilos de segurança UNIX, NTFS e mistos. Quando o estilo de segurança é misto ou unificado, as permissões efetivas dependem do tipo de cliente que modificou as permissões pela última vez porque os usuários definem o estilo de segurança individualmente. Se o último cliente que modificou permissões fosse um cliente NFSv3, as permissões são bits do modo UNIX NFSv3. Se o último cliente foi um cliente NFSv4, as permissões são NFSv4 ACLs. Se o último cliente foi um cliente SMB, as permissões são ACLs do Windows NTFS.

O estilo de segurança unificado só está disponível com volumes infinitos, que não são mais suportados no ONTAP 9.5 e versões posteriores. Para obter mais informações, Visão geral do gerenciamento do FlexGroup volumesconsulte .

A partir do ONTAP 9.2, o `show-effective-permissions` parâmetro para o `vserver security file-`

`directory` comando permite exibir permissões efetivas concedidas a um usuário Windows ou UNIX no caminho especificado de arquivo ou pasta. Além disso, o parâmetro opcional `-share-name` permite exibir a permissão de compartilhamento efetivo.

> O ONTAP define inicialmente algumas permissões de arquivo padrão. Por padrão, o estilo de segurança eficaz em todos os dados em UNIX, volumes mistos e de estilo de segurança unificado é UNIX e o tipo de permissões efetivas é bits de modo UNIX (0755 a menos que especificado de outra forma) até ser configurado por um cliente como permitido pelo estilo de segurança padrão. Por padrão, o estilo de segurança eficaz em todos os dados em volumes de estilo de segurança NTFS é NTFS e tem uma ACL que permite o controle total para todos.

Onde e quando definir estilos de segurança

Os estilos de segurança podem ser definidos em volumes FlexVol (raiz ou volumes de dados) e qtrees. Os estilos de segurança podem ser definidos manualmente no momento da criação, herdados automaticamente ou alterados posteriormente.

Decida qual estilo de segurança usar em SVMs

Para ajudá-lo a decidir qual estilo de segurança usar em um volume, você deve considerar dois fatores. O fator principal é o tipo de administrador que gerencia o sistema de arquivos. O fator secundário é o tipo de usuário ou serviço que acessa os dados no volume.

Ao configurar o estilo de segurança em um volume, você deve considerar as necessidades do seu ambiente para garantir que você selecione o melhor estilo de segurança e evite problemas com o gerenciamento de permissões. As seguintes considerações podem ajudá-lo a decidir:

Estilo de segurança	Escolha se…
UNIX	• O sistema de arquivos é gerenciado por um administrador UNIX. • A maioria dos usuários são clientes NFS. • Um aplicativo que acessa os dados usa um usuário UNIX como a conta de serviço.
NTFS	• O sistema de arquivos é gerenciado por um administrador do Windows. • A maioria dos usuários são clientes SMB. • Um aplicativo que acessa os dados usa um usuário do Windows como a conta de serviço.
Misto	O sistema de arquivos é gerenciado por administradores UNIX e Windows e os usuários consistem em clientes NFS e SMB.

Como a herança de estilo de segurança funciona

Se você não especificar o estilo de segurança ao criar um novo FlexVol volume ou uma qtree, ele herdará seu estilo de segurança de maneiras diferentes.

Os estilos de segurança são herdados da seguinte maneira:

- Um FlexVol volume herda o estilo de segurança do volume raiz do SVM.
- Uma qtree herda o estilo de segurança do seu que contém FlexVol volume.
- Um arquivo ou diretório herda o estilo de segurança dele contendo FlexVol volume ou qtree.

Como o ONTAP preserva as permissões UNIX

Quando os arquivos em um FlexVol volume que atualmente têm permissões UNIX são editados e salvos por aplicativos do Windows, o ONTAP pode preservar as permissões UNIX.

Quando os aplicativos em clientes do Windows editam e salvam arquivos, eles leem as propriedades de segurança do arquivo, criam um novo arquivo temporário, aplicam essas propriedades ao arquivo temporário e dão ao arquivo temporário o nome do arquivo original.

Quando os clientes Windows executam uma consulta para as propriedades de segurança, eles recebem uma ACL construída que representa exatamente as permissões UNIX. O único propósito desta ACL construída é preservar as permissões UNIX do arquivo, pois os arquivos são atualizados por aplicativos do Windows para garantir que os arquivos resultantes tenham as mesmas permissões UNIX. O ONTAP não define nenhuma ACLs NTFS usando a ACL construída.

Gerenciar permissões UNIX usando a guia Segurança do Windows

Se você quiser manipular permissões UNIX de arquivos ou pastas em volumes mistos de estilo de segurança ou qtrees em SVMs, você pode usar a guia Segurança em clientes Windows. Como alternativa, você pode usar aplicativos que podem consultar e definir ACLs do Windows.

- Modificação de permissões UNIX

  Você pode usar a guia Segurança do Windows para exibir e alterar permissões UNIX para um volume ou qtree misto de estilo de segurança. Se você usar a guia principal de Segurança do Windows para alterar permissões UNIX, primeiro remova o ACE existente que deseja editar (isso define os bits de modo como 0) antes de fazer as alterações. Como alternativa, você pode usar o editor avançado para alterar permissões.

  Se as permissões de modo forem usadas, você pode alterar diretamente as permissões de modo para o UID listado, GID e outros (todos os outros com uma conta no computador). Por exemplo, se o UID exibido tiver permissões r-x, você pode alterar as permissões UID para rwx.

- Alterando permissões UNIX para permissões NTFS

  Você pode usar a guia Segurança do Windows para substituir objetos de segurança UNIX por objetos de segurança do Windows em um volume de estilo de segurança misto ou qtree onde os arquivos e pastas têm um estilo de segurança eficaz UNIX.

Você deve primeiro remover todas as entradas de permissão UNIX listadas antes de poder substituí-las pelos objetos de Usuário e Grupo do Windows desejados. Em seguida, você pode configurar ACLs baseadas em NTFS nos objetos Usuário e Grupo do Windows. Removendo todos os objetos de segurança UNIX e adicionando apenas usuários e grupos do Windows a um arquivo ou pasta em um volume ou qtree misto de estilo de segurança, você altera o estilo de segurança efetivo no arquivo ou pasta de UNIX para NTFS.

Ao alterar permissões em uma pasta, o comportamento padrão do Windows é propagar essas alterações para todas as subpastas e arquivos. Portanto, você deve alterar a opção de propagação para a configuração desejada se não quiser propagar uma alteração no estilo de segurança para todas as pastas, subpastas e arquivos filhos.

Configurar estilos de segurança em volumes raiz do SVM

Você configura o estilo de segurança do volume raiz da máquina virtual de storage (SVM) para determinar o tipo de permissões usado para dados no volume raiz do SVM.

Passos

1. Use o `vserver create` comando com o `-rootvolume-security-style` parâmetro para definir o estilo de segurança.

   As opções possíveis para o estilo de segurança do volume raiz são `unix`, `ntfs` ou `mixed`.

2. Exiba e verifique a configuração, incluindo o estilo de segurança do volume raiz do SVM criado: `vserver show -vserver vserver_name`

Configurar estilos de segurança no FlexVol volumes

Você configura o estilo de segurança do FlexVol volume para determinar o tipo de permissões usadas para dados nos volumes do FlexVol da máquina virtual de storage (SVM).

Passos

1. Execute uma das seguintes ações:

Se o FlexVol volume…	Use o comando…
Ainda não existe	`volume create` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.
Já existe	`volume modify` e inclua o `-security-style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança do FlexVol volume são `unix`, `ntfs` ou `mixed`.

   Se você não especificar um estilo de segurança ao criar um FlexVol volume, o volume herdará o estilo de segurança do volume raiz.

   Para obter mais informações sobre os `volume create` comandos ou `volume modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança do FlexVol volume criado, digite o seguinte comando:

   `volume show -volume volume_name -instance`

Configurar estilos de segurança no qtrees

Você configura o estilo de segurança do volume de qtree para determinar o tipo de permissões usadas para dados no qtrees.

Passos

1. Execute uma das seguintes ações:

Se a qtree…	Use o comando…
Ainda não existe	`volume qtree create` e inclua o `-security -style` parâmetro para especificar o estilo de segurança.
Já existe	`volume qtree modify` e inclua o `-security -style` parâmetro para especificar o estilo de segurança.

   As opções possíveis para o estilo de segurança de qtree são `unix`, `ntfs`, ou `mixed`.

   Se você não especificar um estilo de segurança ao criar uma qtree, o estilo de segurança padrão será `mixed`.

   Para obter mais informações sobre os `volume qtree create` comandos ou `volume qtree modify`, "Gerenciamento de storage lógico"consulte .

2. Para exibir a configuração, incluindo o estilo de segurança da qtree que você criou, digite o seguinte comando: `volume qtree show -qtree qtree_name -instance`

Crie e gerencie volumes de dados em namespaces nas

Criar e gerenciar volumes de dados na visão geral dos namespaces nas

Para gerenciar o acesso a arquivos em um ambiente nas, você precisa gerenciar volumes de dados e pontos de junção na máquina virtual de storage (SVM). Isso inclui Planejar sua arquitetura de namespace, criar volumes com ou sem pontos de junção, montar ou desmontar volumes e exibir informações sobre volumes de dados e namespaces de servidor NFS ou CIFS.

Crie volumes de dados com pontos de junção especificados

Pode especificar o ponto de junção quando cria um volume de dados. O volume resultante é montado automaticamente no ponto de junção e está imediatamente disponível para configurar para acesso nas.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.

> Os seguintes carateres não podem ser usados no caminho de junção: * *
>
> Além disso, o comprimento do caminho de junção não pode ter mais de 255 carateres.

Passos

1. Crie o volume com um ponto de junção: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path` *`junction_path`*

   O caminho de junção deve começar com a raiz (/) e pode conter diretórios e volumes juntados. O caminho de junção não precisa conter o nome do volume. Os caminhos de junção são independentes do nome do volume.

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados criado. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   O caminho de junção é insensível a maiúsculas e minúsculas; `/ENG` é o mesmo que `/eng`. Se você criar um compartilhamento CIFS, o Windows tratará o caminho de junção como se ele fosse sensível a maiúsculas e minúsculas. Por exemplo, se a junção for `/ENG`, o caminho de um compartilhamento CIFS deve começar com `/ENG`, não `/eng`.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado com o ponto de junção desejado: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemplo

O exemplo a seguir cria um volume chamado "home4" localizado na SVM VS1 que tem um caminho de junção `/eng/home` :

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

Crie volumes de dados sem especificar pontos de junção

Você pode criar um volume de dados sem especificar um ponto de junção. O volume resultante não é montado automaticamente e não está disponível para configuração para acesso nas. É necessário montar o volume antes de configurar compartilhamentos SMB ou exportações NFS para esse volume.

Antes de começar

O agregado no qual você deseja criar o volume já deve existir.

Passos

1. Crie o volume sem um ponto de junção usando o seguinte comando: `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   Especificar um estilo de segurança de volume é opcional. Se você não especificar um estilo de segurança, o ONTAP criará o volume com o mesmo estilo de segurança aplicado ao volume raiz da máquina virtual de storage (SVM). No entanto, o estilo de segurança do volume raiz pode não ser o estilo de segurança que você deseja aplicar ao volume de dados. A recomendação é especificar o estilo de segurança quando você cria o volume para minimizar problemas de acesso a arquivos difíceis de solucionar.

   Há muitos parâmetros opcionais que você pode usar para personalizar um volume de dados. Para saber mais sobre eles, consulte as páginas de manual do `volume create` comando.

2. Verifique se o volume foi criado sem um ponto de junção: `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

Exemplo

O exemplo a seguir cria um volume chamado "vendas" localizado no SVM VS1 que não está montado em um ponto de junção:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

Montar ou desmontar volumes existentes no namespace nas

Um volume deve ser montado no namespace nas antes de poder configurar o acesso do cliente nas aos dados contidos nos volumes de máquina virtual de storage (SVM). Você pode montar um volume em um ponto de junção se ele não estiver montado no

momento. Você também pode desmontar volumes.

Sobre esta tarefa

Se você desmontar e colocar um volume off-line, todos os dados dentro do ponto de junção, incluindo dados em volumes com pontos de junção contidos no namespace do volume não montado, ficarão inacessíveis para clientes nas.

> Para interromper o acesso de cliente nas a um volume, não é suficiente simplesmente desmontar o volume. Você deve colocar o volume off-line ou tomar outras medidas para garantir que os caches de manipulação de arquivos do lado do cliente sejam invalidados. Para obter mais informações, consulte o seguinte artigo da base de dados de Conhecimento: "Os clientes NFSv3 ainda têm acesso a um volume depois de serem removidos do namespace no ONTAP"

Quando você desmontar e colocar um volume off-line, os dados dentro do volume não são perdidos. Além disso, políticas de exportação de volume existentes e compartilhamentos SMB criados no volume ou em diretórios e pontos de junção dentro do volume não montado são retidos. Se você remontar o volume não montado, os clientes nas poderão acessar os dados contidos no volume usando políticas de exportação e compartilhamentos SMB existentes.

Passos

1. Execute a ação desejada:

Se você quiser…	Digite os comandos…
Monte um volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

Desmontar um volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. Verifique se o volume está no estado de montagem desejado:

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

Exemplos

O exemplo a seguir monta um volume chamado "vendas" localizado na SVM "VS1" no ponto de junção ""/vendas":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

O exemplo a seguir desmonta e coloca offline um volume chamado "data" localizado na SVM ""VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

Apresentar informações sobre a montagem do volume e o ponto de junção

Você pode exibir informações sobre volumes montados para máquinas virtuais de armazenamento (SVMs) e os pontos de junção para os quais os volumes são montados. Você também pode determinar quais volumes não estão montados em um ponto de junção. Use essas informações para entender e gerenciar seu namespace SVM.

Passos

1. Execute a ação desejada:

Se você quiser exibir…	Digite o comando…
Informações resumidas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -junction`
Informações detalhadas sobre volumes montados e não montados no SVM	`volume show -vserver vserver_name -volume volume_name -instance`

Se você quiser exibir…	Digite o comando…
Informações específicas sobre volumes montados e não montados no SVM	a. Se necessário, você pode exibir campos válidos para o `-fields` parâmetro usando o seguinte comando: `volume show -fields ?` b. Exiba as informações desejadas usando o `-fields` parâmetro: Volume show -vserver vserver_name -fieldname,…

Exemplos

O exemplo a seguir exibe um resumo dos volumes montados e não montados no SVM VS1:

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

O exemplo a seguir exibe informações sobre campos especificados para volumes localizados no SVM VS2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

Configurar mapeamentos de nomes

Configure a visão geral dos mapeamentos de nomes

O ONTAP usa mapeamento de nomes para mapear identidades CIFS para identidades UNIX, identidades Kerberos para identidades UNIX e identidades UNIX para identidades CIFS. Ele precisa dessas informações para obter credenciais de usuário e fornecer acesso adequado aos arquivos, independentemente de estarem se conetando a partir de um cliente NFS ou de um cliente CIFS.

Há duas exceções em que você não precisa usar o mapeamento de nomes:

- Você configura um ambiente UNIX puro e não planeja usar o acesso CIFS ou o estilo de segurança NTFS em volumes.
- Em vez disso, você configura o usuário padrão a ser usado.

  Nesse cenário, o mapeamento de nomes não é necessário porque, em vez de mapear cada credencial de cliente individual, todas as credenciais de cliente são mapeadas para o mesmo usuário padrão.

Observe que você pode usar o mapeamento de nomes somente para usuários, não para grupos.

No entanto, você pode mapear um grupo de usuários individuais para um usuário específico. Por exemplo, você pode mapear todos os usuários do AD que começam ou terminam com a palavra VENDAS para um

usuário UNIX específico e para o UID do usuário.

Como o mapeamento de nomes funciona

Quando o ONTAP tem que mapear credenciais para um usuário, ele primeiro verifica o banco de dados de mapeamento de nomes local e o servidor LDAP para um mapeamento existente. Verifique uma ou ambas e em que ordem é determinada pela configuração do serviço de nomes do SVM.

- Para mapeamento do Windows para UNIX

  Se nenhum mapeamento for encontrado, o ONTAP verifica se o nome de usuário do Windows em minúsculas é um nome de usuário válido no domínio UNIX. Se isso não funcionar, ele usará o usuário UNIX padrão desde que esteja configurado. Se o usuário UNIX padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

- Para mapeamento UNIX para Windows

  Se nenhum mapeamento for encontrado, o ONTAP tentará encontrar uma conta do Windows que corresponda ao nome UNIX no domínio SMB. Se isso não funcionar, ele usará o usuário SMB padrão, desde que esteja configurado. Se o usuário CIFS padrão não estiver configurado e o ONTAP também não puder obter um mapeamento dessa maneira, o mapeamento falhará e um erro será retornado.

As contas de máquina são mapeadas para o usuário UNIX padrão especificado por padrão. Se nenhum usuário UNIX padrão for especificado, mapeamentos de contas de máquina falharão.

- A partir do ONTAP 9.5, você pode mapear contas de máquina para usuários que não sejam o usuário UNIX padrão.
- No ONTAP 9.4 e anteriores, você não pode mapear contas de máquina para outros usuários.

  Mesmo que os mapeamentos de nomes para contas de máquinas sejam definidos, os mapeamentos serão ignorados.

Procura multidomínio para mapeamentos de nome de usuário do UNIX para o Windows

O ONTAP oferece suporte a pesquisas de vários domínios ao mapear usuários UNIX para usuários do Windows. Todos os domínios confiáveis descobertos são pesquisados por correspondências ao padrão de substituição até que um resultado correspondente seja retornado. Como alternativa, você pode configurar uma lista de domínios confiáveis preferenciais, que é usada em vez da lista de domínios confiáveis descobertos e é pesquisada em ordem até que um resultado correspondente seja retornado.

Como as relações de confiança de domínio afetam as pesquisas de mapeamento de nomes de usuário do Windows

Para entender como o mapeamento de nomes de usuário de vários domínios funciona, você deve entender como as relações de confiança de domínio funcionam com o ONTAP. As relações de confiança do ative Directory com o domínio home do servidor CIFS podem ser uma confiança bidirecional ou podem ser um dos dois tipos de confiança unidirecionais, uma confiança de entrada ou uma confiança de saída. O domínio inicial é o domínio ao qual pertence o servidor CIFS na SVM.

- *Confiança bidirecional*

  Com trusts bidirecionais, ambos os domínios confiam uns nos outros. Se o domínio home do servidor CIFS tiver uma confiança bidirecional com outro domínio, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável e vice-versa.

  As pesquisas de mapeamento de nome de usuário do UNIX para o Windows podem ser realizadas apenas em domínios com confiança bidirecional entre o domínio inicial e o outro domínio.

- *Outbound Trust*

  Com uma confiança de saída, o domínio home confia no outro domínio. Nesse caso, o domínio home pode autenticar e autorizar um usuário pertencente ao domínio confiável de saída.

  Um domínio com uma confiança de saída com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

- *Confiança inbound*

  Com uma confiança de entrada, o outro domínio confia no domínio home do servidor CIFS. Neste caso, o domínio inicial não pode autenticar ou autorizar um usuário pertencente ao domínio confiável de entrada.

  Um domínio com uma confiança de entrada com o domínio inicial é *not* pesquisado ao executar pesquisas de mapeamento de nomes de usuário do UNIX para o Windows.

Como os curingas (*) são usados para configurar pesquisas de vários domínios para mapeamento de nomes

As pesquisas de mapeamento de nomes de vários domínios são facilitadas pelo uso de curingas na seção domínio do nome de usuário do Windows. A tabela a seguir ilustra como usar curingas na parte de domínio de uma entrada de mapeamento de nomes para habilitar pesquisas de vários domínios:

Padrão	Substituição	Resultado
raiz	• administrador	O usuário UNIX "'root'" é mapeado para o usuário chamado "'administrador'". Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente chamado "administrador" seja encontrado.

Padrão	Substituição	Resultado
*	• *	Os usuários UNIX válidos são mapeados para os usuários do Windows correspondentes. Todos os domínios confiáveis são pesquisados em ordem até que o primeiro usuário correspondente com esse nome seja encontrado. O padrão* é válido apenas para mapeamento de nomes do UNIX para o Windows, e não para o contrário.

Como as pesquisas de nomes de vários domínios são realizadas

Você pode escolher um dos dois métodos para determinar a lista de domínios confiáveis usados para pesquisas de nomes de vários domínios:

- Use a lista de confiança bidirecional descoberta automaticamente compilada pelo ONTAP
- Use a lista de domínio confiável preferida que você compila

Se um usuário UNIX for mapeado para um usuário do Windows com um curinga usado para a seção de domínio do nome de usuário, o usuário do Windows será pesquisado em todos os domínios confiáveis da seguinte forma:

- Se uma lista de domínio confiável preferencial estiver configurada, o usuário mapeado do Windows será pesquisado somente nesta lista de pesquisa, em ordem.
- Se uma lista preferencial de domínios confiáveis não estiver configurada, o usuário do Windows será pesquisado em todos os domínios confiáveis bidirecionais do domínio doméstico.
- Se não houver domínios bidirecionalmente confiáveis para o domínio home, o usuário será pesquisado no domínio home.

Se um usuário UNIX for mapeado para um usuário do Windows sem uma seção de domínio no nome de usuário, o usuário do Windows será pesquisado no domínio inicial.

Regras de conversão de mapeamento de nomes

Um sistema ONTAP mantém um conjunto de regras de conversão para cada SVM. Cada regra consiste em duas partes: Um *pattern* e um *replacement*. As conversões começam no início da lista apropriada e executam uma substituição com base na primeira regra de correspondência. O padrão é uma expressão regular estilo UNIX. A substituição é uma cadeia de carateres contendo sequências de escape que representam subexpressões do padrão, como no programa UNIX `sed`.

Crie um mapeamento de nomes

Você pode usar o `vserver name-mapping create` comando para criar um mapeamento de nomes. Use mapeamentos de nomes para permitir que os usuários do Windows acessem volumes de estilo de segurança UNIX e o inverso.

Sobre esta tarefa

Para cada SVM, o ONTAP oferece suporte a até 12.500 mapeamentos de nomes para cada direção.

Passo

1. Criar um mapeamento de nomes: `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > As `-pattern` declarações e `-replacement` podem ser formuladas como expressões regulares. Você também pode usar a `-replacement` instrução para negar explicitamente um mapeamento para o usuário usando a cadeia de substituição nula `" "` (o caractere de espaço). Consulte a `vserver name-mapping create` página de manual para obter detalhes.

   Quando os mapeamentos do Windows para UNIX são criados, todos os clientes SMB que tenham conexões abertas ao sistema ONTAP no momento em que os novos mapeamentos são criados devem fazer logout e fazer login novamente para ver os novos mapeamentos.

Exemplos

O comando a seguir cria um mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do UNIX para o Windows na posição 1 na lista de prioridades. O mapeamento mapeia o usuário UNIX johnd para o usuário do Windows Eng.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. O mapeamento é um mapeamento do Windows para o UNIX na posição 1 na lista de prioridades. Aqui o padrão e a substituição incluem expressões regulares. O mapeamento mapeia cada usuário CIFS no domínio ENG para usuários no domínio LDAP associado ao SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

O comando a seguir cria outro mapeamento de nomes no SVM chamado VS1. Aqui, o padrão inclui "" como um elemento no nome de usuário do Windows que deve ser escapado. O mapeamento mapeia as operações do usuário do Windows para o usuário do UNIX John_OPS.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

Configure o usuário padrão

Você pode configurar um usuário padrão para usar se todas as outras tentativas de mapeamento falharem para um usuário ou se não quiser mapear usuários individuais entre UNIX e Windows. Alternativamente, se você quiser que a autenticação de usuários não mapeados falhe, você não deve configurar um usuário padrão.

Sobre esta tarefa

Para autenticação CIFS, se você não quiser mapear cada usuário do Windows para um usuário UNIX individual, você pode especificar um usuário UNIX padrão.

Para autenticação NFS, se você não quiser mapear cada usuário UNIX para um usuário individual do Windows, você pode especificar um usuário padrão do Windows.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o seguinte comando…
Configure o usuário UNIX padrão	`vserver cifs options modify -default -unix-user` *user_name*
Configure o usuário padrão do Windows	`vserver nfs modify -default-win-user` *user_name*

Comandos para gerenciar mapeamentos de nomes

Existem comandos ONTAP específicos para gerenciar mapeamentos de nomes.

Se você quiser…	Use este comando…
Crie um mapeamento de nomes	`vserver name-mapping create`
Insira um mapeamento de nomes em uma posição específica	`vserver name-mapping insert`
Exibir mapeamentos de nomes	`vserver name-mapping show`

Se você quiser…	Use este comando…
Troque a posição de dois mapeamentos de nomes Uma troca não é permitida quando o mapeamento de nomes é configurado com uma entrada de qualificador ip.	`vserver name-mapping swap`
Modificar um mapeamento de nomes	`vserver name-mapping modify`
Eliminar um mapeamento de nomes	`vserver name-mapping delete`
Valide o mapeamento de nomes correto	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

Consulte a página de manual de cada comando para obter mais informações.

Configurar pesquisas de mapeamento de nomes de vários domínios

Ative ou desative pesquisas de mapeamento de nomes de vários domínios

Com pesquisas de mapeamento de nomes de vários domínios, você pode usar um cartão selvagem (**) na parte de domínio de um nome do Windows ao configurar o usuário UNIX para o mapeamento de nome de usuário do Windows. O uso de um cartão selvagem (**) na parte do domínio do nome permite que o ONTAP pesquise todos os domínios que tenham uma confiança bidirecional com o domínio que contém a conta do computador do servidor CIFS.

Sobre esta tarefa

Como alternativa à pesquisa de todos os domínios bidirecionalmente confiáveis, você pode configurar uma lista de domínios confiáveis preferenciais. Quando uma lista de domínios confiáveis preferenciais é configurada, o ONTAP usa a lista de domínios confiáveis preferenciais em vez dos domínios confiáveis bidirecionais descobertos para realizar pesquisas de mapeamento de nomes de vários domínios.

- As pesquisas de mapeamento de nomes de vários domínios são ativadas por padrão.
- Esta opção está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você deseja que as pesquisas de mapeamento de nomes de vários domínios sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Redefinir e redescobrir domínios confiáveis

Você pode forçar a redescoberta de todos os domínios confiáveis. Isso pode ser útil quando os servidores de domínio confiáveis não estão respondendo adequadamente ou as relações de confiança foram alteradas. Somente domínios com confiança bidirecional com o domínio home, que é o domínio que contém a conta de computador do servidor CIFS, são descobertos.

Passo

1. Redefina e redescubra domínios confiáveis usando o `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

Informações relacionadas

Exibindo informações sobre domínios confiáveis descobertos

Exibir informações sobre domínios confiáveis descobertos

Você pode exibir informações sobre os domínios confiáveis descobertos para o domínio doméstico do servidor CIFS, que é o domínio que contém a conta de computador do servidor CIFS. Isso pode ser útil quando você quiser saber quais domínios confiáveis são descobertos e como eles são solicitados na lista de domínios confiáveis descobertos.

Sobre esta tarefa

Apenas os domínios com confiança bidirecional com o domínio home são descobertos. Como o controlador de domínio (DC) do domínio home retorna a lista de domínios confiáveis em uma ordem determinada pelo DC, a ordem dos domínios dentro da lista não pode ser prevista. Ao exibir a lista de domínios confiáveis, você pode determinar a ordem de pesquisa para pesquisas de mapeamento de nomes de vários domínios.

As informações de domínio confiável exibidas são agrupadas por nó e máquina virtual de armazenamento (SVM).

Passo

1. Exiba informações sobre domínios confiáveis descobertos usando o `vserver cifs domain trusts show` comando.

   `vserver cifs domain trusts show -vserver vs1`

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

Informações relacionadas

Redefinir e redescobrir domínios confiáveis

Adicione, remova ou substitua domínios confiáveis em listas de domínios confiáveis preferenciais

Pode adicionar ou remover domínios fidedignos da lista de domínios fidedignos preferidos para o servidor SMB ou pode modificar a lista atual. Se você configurar uma lista de domínio confiável preferencial, essa lista será usada em vez dos domínios confiáveis bidirecionais descobertos ao executar pesquisas de mapeamento de nomes de vários domínios.

Sobre esta tarefa

- Se você estiver adicionando domínios confiáveis a uma lista existente, a nova lista será mesclada com a lista existente com as novas entradas colocadas no final Os domínios confiáveis são pesquisados na ordem em que aparecem na lista de domínios confiáveis.
- Se você estiver removendo domínios confiáveis da lista existente e não especificar uma lista, toda a lista de domínio confiável para a máquina virtual de armazenamento especificada (SVM) será removida.
- Se você modificar a lista existente de domínios confiáveis, a nova lista substituirá a lista existente.

Você deve inserir apenas domínios bidirecionalmente confiáveis na lista de domínios confiáveis preferidos. Mesmo que você possa inserir domínios confiáveis de saída ou entrada na lista de domínios preferidos, eles não são usados ao realizar pesquisas de mapeamento de nomes de vários domínios. O ONTAP pula a entrada do domínio unidirecional e passa para o próximo domínio confiável bidirecional na lista.

Passo

1. Execute uma das seguintes ações:

Se você quiser fazer o seguinte com a lista de domínios confiáveis preferenciais…	Use o comando…
Adicione domínios confiáveis à lista	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
Remova domínios confiáveis da lista	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
Modifique a lista existente	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

Exemplos

O comando a seguir adiciona dois domínios confiáveis (cifs1.example.com e cifs2.example.com) à lista de domínios confiáveis preferida usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir remove dois domínios confiáveis da lista usada pelo SVM VS1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

O comando a seguir modifica a lista de domínio confiável usada pelo SVM VS1. A nova lista substitui a lista original:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

Informações relacionadas

Exibindo informações sobre a lista de domínio confiável preferencial

Exibir informações sobre a lista de domínios confiáveis preferencial

Você pode exibir informações sobre quais domínios confiáveis estão na lista de domínios confiáveis preferenciais e a ordem em que eles são pesquisados se as pesquisas de mapeamento de nomes de vários domínios estiverem ativadas. Você pode configurar uma lista de domínio confiável preferida como alternativa ao uso da lista de domínio confiável descoberta automaticamente.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre o seguinte…	Use o comando…
Todos os domínios confiáveis preferenciais no cluster agrupados por máquina virtual de armazenamento (SVM)	`vserver cifs domain name-mapping-search show`
Todos os domínios confiáveis preferenciais para um SVM especificado	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

O comando a seguir exibe informações sobre todos os domínios confiáveis preferenciais no cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

Informações relacionadas

Adicionar, remover ou substituir domínios confiáveis em listas de domínios confiáveis preferenciais

Crie e configure compartilhamentos SMB

Crie e configure a visão geral de compartilhamentos SMB

Para que usuários e aplicativos possam acessar dados no servidor CIFS em SMB, você deve criar e configurar compartilhamentos SMB, que é um ponto de acesso nomeado em um volume. Você pode personalizar compartilhamentos especificando parâmetros de compartilhamento e propriedades de compartilhamento. Você pode modificar um compartilhamento existente a qualquer momento.

Quando você cria um compartilhamento SMB, o ONTAP cria uma ACL padrão para as permissões de compartilhamento com controle total para todos.

Os compartilhamentos SMB estão vinculados ao servidor CIFS na máquina virtual de storage (SVM). Os compartilhamentos de SMB serão excluídos se o SVM for excluído ou se o servidor CIFS ao qual ele está associado for excluído do SVM. Se você recriar o servidor CIFS na SVM, será necessário recriar os compartilhamentos SMB.

Informações relacionadas

Gerencie o acesso a arquivos usando SMB

"Configuração SMB para Microsoft Hyper-V e SQL Server"

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Quais são os compartilhamentos administrativos padrão

Quando você cria um servidor CIFS na máquina virtual de storage (SVM), os compartilhamentos administrativos padrão são criados automaticamente. Você deve entender o que são esses compartilhamentos padrão e como eles são usados.

O ONTAP cria os seguintes compartilhamentos administrativos padrão quando você cria o servidor CIFS:

> A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

- ipc
- (Somente ONTAP 9.7 e versões anteriores)
- c

Como os compartilhamentos que terminam com o caractere dólar são compartilhamentos ocultos, os compartilhamentos administrativos padrão não são visíveis em meu computador, mas você pode visualizá-los usando pastas compartilhadas.

Como os compartilhamentos padrão do ipc e do admin são usados

As ações do ONTAP são usadas pelos administradores do Windows e não podem ser usadas pelos administradores do Windows para acessar dados residentes no SVM.

- compartilhar

  A ação ipc é um recurso que compartilha os pipes nomeados que são essenciais para a comunicação entre programas. O compartilhamento ipc é usado durante a administração remota de um computador e ao visualizar os recursos compartilhados de um computador. Não é possível alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs do compartilhamento ipc. Você também não pode renomear ou excluir o compartilhamento ipc.

- Compartilhar (somente ONTAP 9.7 e anteriores)

  > A partir do ONTAP 9.8, o compartilhamento admin não é mais criado por padrão.

  O compartilhamento admin é usado durante a administração remota do SVM. O caminho desse recurso é sempre o caminho para a raiz do SVM. Você não pode alterar as configurações de compartilhamento, propriedades de compartilhamento ou ACLs para o compartilhamento admin. Você também não pode renomear ou excluir o compartilhamento admin.

Como o compartilhamento padrão c

O compartilhamento de CAD é um compartilhamento administrativo que o cluster ou o administrador do SVM pode usar para acessar e gerenciar o volume raiz do SVM.

A seguir estão as caraterísticas da participação:

- O caminho para esse compartilhamento é sempre o caminho para o volume raiz da SVM e não pode ser modificado.
- A ACL padrão para o compartilhamento c

  Este utilizador é o administrador. Por padrão, o administrador do BUILTIN pode mapear para o compartilhamento e exibição, criar, modificar ou excluir arquivos e pastas no diretório raiz mapeado. Cuidado deve ser exercido ao gerenciar arquivos e pastas neste diretório.

- Você pode alterar a ACL do compartilhamento.
- Você pode alterar as configurações de compartilhamento e as propriedades de compartilhamento.
- Não é possível eliminar a partilha c
- O administrador do SVM pode acessar o restante do namespace SVM a partir do compartilhamento mapeado por meio do cruzamento das junções do namespace.
- O compartilhamento c pode ser acessado usando o Console de Gerenciamento da Microsoft.

Informações relacionadas

Configurando permissões avançadas de arquivos NTFS usando a guia Segurança do Windows

Requisitos de nomenclatura para compartilhamento de SMB

Você deve manter os requisitos de nomenclatura do compartilhamento do ONTAP em mente ao criar compartilhamentos SMB no seu servidor SMB.

As convenções de nomes de compartilhamento para ONTAP são as mesmas que para o Windows e incluem os seguintes requisitos:

- O nome de cada compartilhamento deve ser exclusivo para o servidor SMB.
- Nomes de compartilhamento não diferenciam maiúsculas de minúsculas.
- O comprimento máximo do nome da partilha é de 80 carateres.
- Nomes de compartilhamento Unicode são suportados.
- Nomes de compartilhamento que terminam com o caractere dólar são compartilhamentos ocultos.
- Para o ONTAP 9.7 e anteriores, os compartilhamentos administrativos são criados automaticamente em todos os servidores CIFS e são nomes de compartilhamento reservados. A partir do ONTAP 9.8, o compartilhamento admin não é mais criado automaticamente.
- Você não pode usar o nome de compartilhamento ONTAP_ADMIN ao criar um compartilhamento.
- Nomes de compartilhamento que contêm espaços são suportados:
  - Você não pode usar um espaço como o primeiro caractere ou como o último caractere em um nome de compartilhamento.
  - Você deve incluir nomes de compartilhamento contendo um espaço entre aspas.

    As aspas simples são consideradas parte do nome da partilha e não podem ser utilizadas no lugar das aspas.

- Os seguintes carateres especiais são suportados quando você nomeia compartilhamentos SMB:

! A % e ' _ - . Clique em "OK"

- Os seguintes carateres especiais não são suportados quando você nomeia compartilhamentos SMB:
  - " / : ; | > , ? *

Requisitos de sensibilidade de caso de diretório ao criar compartilhamentos em um ambiente multiprotocolo

Se você criar compartilhamentos em um SVM em que o esquema de nomenclatura 8,3 seja usado para distinguir entre nomes de diretórios onde haja apenas diferenças de casos entre os nomes, você deve usar o nome 8,3 no caminho de compartilhamento para garantir que o cliente se conete ao caminho de diretório desejado.

No exemplo a seguir, dois diretórios chamados "testdir" e "TESTDIR" foram criados em um cliente Linux. O caminho de junção do volume que contém os diretórios é `/home`. A primeira saída é de um cliente Linux e a segunda saída é de um cliente SMB.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Ao criar um compartilhamento no segundo diretório, você deve usar o nome 8,3 no caminho de compartilhamento. Neste exemplo, o caminho de compartilhamento para o primeiro diretório é `/home/testdir` e o caminho de compartilhamento para o segundo diretório é `/home/TESTDI~1`.

Use propriedades de compartilhamento SMB

Use a visão geral das propriedades de compartilhamento SMB

Você pode personalizar as propriedades dos compartilhamentos SMB.

As propriedades de compartilhamento disponíveis são as seguintes:

Compartilhar propriedades	Descrição
`oplocks`	Esta propriedade especifica que o compartilhamento usa bloqueios oportunistas, também conhecidos como cache do lado do cliente.
`browsable`	Esta propriedade permite que os clientes Windows naveguem na partilha.

Compartilhar propriedades	Descrição
`showsnapshot`	Essa propriedade especifica que as cópias Snapshot podem ser visualizadas e atravessadas por clientes.
`changenotify`	Esta propriedade especifica que o compartilhamento suporta solicitações Change Notify. Para compartilhamentos em um SVM, esta é uma propriedade inicial padrão.
`attributecache`	Essa propriedade permite que o cache de atributos de arquivo no compartilhamento SMB forneça acesso mais rápido aos atributos. O padrão é desabilitar o cache de atributos. Esta propriedade só deve ser ativada se houver clientes conetando-se a compartilhamentos sobre SMB 1,0. Essa propriedade de compartilhamento não se aplica se os clientes estiverem se conetando a compartilhamentos em SMB 2.x ou SMB 3,0.
`continuously-available`	Esta propriedade permite que clientes SMB que a suportam para abrir arquivos de forma persistente. Os arquivos abertos desta maneira são protegidos contra eventos disruptivos, como failover e giveback.
`branchcache`	Esta propriedade especifica que o compartilhamento permite que os clientes solicitem hashes BranchCache nos arquivos desse compartilhamento. Esta opção é útil somente se você especificar "'per-share'" como o modo operacional na configuração do CIFS BranchCache.
`access-based-enumeration`	Esta propriedade especifica que *Access Based Enumeração* (ABE) está ativada neste compartilhamento. As pastas compartilhadas filtradas por ABE são visíveis para um usuário com base nos direitos de acesso desse usuário individual, impedindo a exibição de pastas ou outros recursos compartilhados que o usuário não tem direitos de acesso.

Compartilhar propriedades	Descrição
`namespace-caching`	Esta propriedade especifica que os clientes SMB que se conetam a esse compartilhamento podem armazenar em cache os resultados da enumeração de diretórios retornados pelos servidores CIFS, o que pode fornecer melhor desempenho. Por padrão, os clientes SMB 1 não armazenam em cache os resultados da enumeração de diretórios. Como os clientes SMB 2 e SMB 3 armazenam resultados de enumeração de diretório em cache por padrão, especificar essa propriedade de compartilhamento fornece benefícios de desempenho apenas para conexões de cliente SMB 1.
`encrypt-data`	Esta propriedade especifica que a criptografia SMB deve ser usada ao acessar esse compartilhamento. Os clientes SMB que não suportam encriptação ao aceder a dados SMB não poderão aceder a esta partilha.

Adicione ou remova propriedades de compartilhamento em um compartilhamento SMB existente

Você pode personalizar um compartilhamento SMB existente adicionando ou removendo propriedades de compartilhamento. Isso pode ser útil se você quiser alterar a configuração de compartilhamento para atender às mudanças nos requisitos do seu ambiente.

Antes de começar

O compartilhamento cujas propriedades você deseja modificar deve existir.

Sobre esta tarefa

Diretrizes para adicionar propriedades de compartilhamento:

- Você pode adicionar uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Quaisquer propriedades de compartilhamento que você especificou anteriormente permanecem em vigor.

  As propriedades recém-adicionadas são anexadas à lista existente de propriedades de compartilhamento.
- Se você especificar um novo valor para as propriedades de compartilhamento que já são aplicadas ao compartilhamento, o valor recém-especificado substituirá o valor original.
- Não é possível remover propriedades de compartilhamento usando o `vserver cifs share properties add` comando.

  Você pode usar o `vserver cifs share properties remove` comando para remover propriedades de compartilhamento.

Diretrizes para remover propriedades de compartilhamento:

- Você pode remover uma ou mais propriedades de compartilhamento usando uma lista delimitada por vírgulas.
- Todas as propriedades de compartilhamento que você especificou anteriormente, mas não as removem, permanecem em vigor.

Passos

1. Introduza o comando adequado:

Se você quiser…	Digite o comando…
Adicione propriedades de compartilhamento	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remover propriedades de compartilhamento	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verifique as configurações da propriedade de compartilhamento: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplos

O comando a seguir adiciona a `showsnapshot` propriedade share a uma ação chamada "hare1" no SVM VS1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

O comando a seguir remove a `browsable` propriedade share de um compartilhamento chamado "hare2" no SVM VS1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Informações relacionadas

Comandos para gerenciar compartilhamentos SMB

Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força

Quando você cria um compartilhamento da linha de comando ONTAP para dados com segurança efetiva UNIX, você pode especificar que todos os arquivos criados por usuários SMB nesse compartilhamento pertencem ao mesmo grupo, conhecido como *force-group*, que deve ser um grupo predefinido no banco de dados de grupos UNIX. O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos.

Especificar um grupo de força é significativo apenas se o compartilhamento estiver em um UNIX ou em uma qtree misto. Não há necessidade de definir um grupo de força para compartilhamentos em um volume NTFS ou qtree porque o acesso a arquivos nesses compartilhamentos é determinado pelas permissões do Windows, não GIDs UNIX.

Se um grupo de força tiver sido especificado para uma ação, o seguinte se tornará verdadeiro para a partilha:

- Os usuários SMB no grupo de força que acessam esse compartilhamento são temporariamente alterados para o GID do grupo de força.

  Este GID permite que eles acessem arquivos neste compartilhamento que não são acessíveis normalmente com seu GID principal ou UID.

- Todos os arquivos neste compartilhamento criados por usuários SMB pertencem ao mesmo grupo de força, independentemente do GID principal do proprietário do arquivo.

Quando os usuários SMB tentam acessar um arquivo criado pelo NFS, os GIDs principais dos usuários SMB determinam os direitos de acesso.

O grupo force não afeta a forma como os usuários NFS acessam arquivos neste compartilhamento. Um arquivo criado por NFS adquire o GID do proprietário do arquivo. A determinação das permissões de acesso é baseada no UID e GID principal do usuário NFS que está tentando acessar o arquivo.

O uso de um grupo de força torna mais fácil garantir que os arquivos possam ser acessados por usuários SMB pertencentes a vários grupos. Por exemplo, se você quiser criar um compartilhamento para armazenar as páginas da Web da empresa e dar acesso de gravação a usuários nos departamentos de Engenharia e Marketing, você pode criar um compartilhamento e dar acesso de gravação a um grupo de força chamado "'webgroup1". Devido ao grupo force, todos os arquivos criados por usuários SMB neste compartilhamento

são de propriedade do grupo "'webgroup1". Além disso, os usuários recebem automaticamente o GID do grupo "'webgroup1" ao acessar o compartilhamento. Como resultado, todos os usuários podem escrever para esse compartilhamento sem que você precise gerenciar os direitos de acesso dos usuários nos departamentos de Engenharia e Marketing.

Informações relacionadas

Criando um compartilhamento SMB com a configuração de compartilhamento de grupo de força

Crie um compartilhamento SMB com a configuração de compartilhamento de grupo de força

Você pode criar um compartilhamento SMB com a configuração de compartilhamento de grupo de força se desejar que os usuários de SMB que acessam dados em volumes ou qtrees com segurança de arquivos UNIX sejam considerados pelo ONTAP como pertencentes ao mesmo grupo UNIX.

Passo

1. Crie o compartilhamento SMB: `vserver cifs share create -vserver` *`vserver_name`* `-share -name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   Se o caminho UNC (`\\servername\sharename\filepath`) do compartilhamento contiver mais de 256 carateres (excluindo o " " " inicial`\\` no caminho UNC), a guia **Segurança** na caixa Propriedades do Windows não estará disponível. Este é um problema de cliente do Windows em vez de um problema de ONTAP. Para evitar esse problema, não crie compartilhamentos com caminhos UNC com mais de 256 carateres.

   Se você quiser remover o grupo de força depois que o compartilhamento é criado, você pode modificar o compartilhamento a qualquer momento e especificar uma string vazia ("") como o valor para o `-force -group-for-create` parâmetro. Se você remover o grupo de força modificando o compartilhamento, todas as conexões existentes a esse compartilhamento continuarão tendo o grupo de força definido anteriormente como GID principal.

Exemplo

O comando a seguir cria um compartilhamento "webpages" que é acessível na Web no `/corp/companyinfo` diretório no qual todos os arquivos criados pelos usuários SMB são atribuídos ao grupo webgroup1:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Informações relacionadas

Otimize o acesso do usuário SMB com a configuração de compartilhamento de grupo de força

Exibir informações sobre compartilhamentos SMB usando o MMC

Você pode exibir informações sobre compartilhamentos SMB no SVM e executar algumas tarefas de gerenciamento usando o Console de Gerenciamento da Microsoft (MMC). Antes de poder visualizar os compartilhamentos, você precisa conetar o MMC ao SVM.

Sobre esta tarefa

Você pode executar as seguintes tarefas em compartilhamentos contidos em SVMs usando o MMC:

- Ver compartilhamentos
- Ver sessões ativas
- Exibir arquivos abertos
- Enumerar a lista de sessões, ficheiros e ligações em árvore no sistema
- Feche os ficheiros abertos no sistema
- Feche as sessões abertas
- Criar/gerenciar compartilhamentos

> As visualizações exibidas pelos recursos anteriores são específicas de nós e não específicas de cluster. Portanto, quando você usa o MMC para se conetar ao nome do host do servidor SMB (ou seja, cifs01.domain.local), você é encaminhado, com base em como configurou o DNS, para um único LIF dentro do cluster.

As seguintes funções não são suportadas no MMC para ONTAP:

- Criando novos usuários/grupos locais
- Gerir/visualizar utilizadores/grupos locais existentes
- Visualização de eventos ou registos de desempenho
- Armazenamento
- Serviços e aplicações

Nos casos em que a operação não é suportada, você pode ter `remote procedure call failed` erros.

"Perguntas frequentes: Usando o Windows MMC com ONTAP"

Passos

1. Para abrir o MMC de Gerenciamento de computador em qualquer servidor Windows, no **Painel de Controle**, selecione **Ferramentas administrativas** > **Gerenciamento de computador**.
2. Selecione **Ação** > **ligar a outro computador**.

   A caixa de diálogo Selecionar computador é exibida.
3. Digite o nome do sistema de armazenamento ou clique em **Procurar** para localizar o sistema de armazenamento.
4. Clique em **OK**.

   O MMC se coneta ao SVM.
5. No painel de navegação, clique em **pastas compartilhadas** > **compartilhamentos**.

   Uma lista de compartilhamentos no SVM é exibida no painel de exibição direito.
6. Para exibir as propriedades de compartilhamento de um compartilhamento, clique duas vezes no compartilhamento para abrir a caixa de diálogo **Propriedades**.
7. Se você não puder se conetar ao sistema de armazenamento usando o MMC, você poderá adicionar o usuário ao grupo BUILTIN ou BUILTIN/Power Users usando um dos seguintes comandos no sistema de armazenamento:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Comandos para gerenciar compartilhamentos SMB

Use os `vserver cifs share` comandos e `vserver cifs share properties` para gerenciar compartilhamentos SMB.

Se você quiser…	Use este comando…
Crie um compartilhamento SMB	`vserver cifs share create`
Exibir compartilhamentos SMB	`vserver cifs share show`
Modificar um compartilhamento SMB	`vserver cifs share modify`
Excluir um compartilhamento SMB	`vserver cifs share delete`
Adicione propriedades de compartilhamento a um compartilhamento existente	`vserver cifs share properties add`
Remover propriedades de compartilhamento de um compartilhamento existente	`vserver cifs share properties remove`
Exibir informações sobre as propriedades de compartilhamento	`vserver cifs share properties show`

Consulte a página de manual de cada comando para obter mais informações.

Proteja o acesso a arquivos usando ACLs de compartilhamento SMB

Diretrizes para gerenciar ACLs de nível de compartilhamento SMB

Você pode alterar ACLs de nível de compartilhamento para dar aos usuários mais ou menos direitos de acesso ao compartilhamento. Você pode configurar ACLs de nível de compartilhamento usando usuários e grupos do Windows ou usuários e grupos UNIX.

Por padrão, a ACL de nível de compartilhamento dá controle total ao grupo padrão chamado Everyone. Controle total na ACL significa que todos os usuários no domínio e todos os domínios confiáveis têm acesso total ao compartilhamento. Você pode controlar o nível de acesso de uma ACL de nível de compartilhamento usando o "Console de Gerenciamento Microsoft (MMC) em um cliente Windows ou na linha de comando ONTAP".

As diretrizes a seguir se aplicam quando você usa o MMC:

- Os nomes de usuário e grupo especificados devem ser nomes do Windows.
- Você pode especificar apenas permissões do Windows.

As diretrizes a seguir se aplicam quando você usa a linha de comando ONTAP:

- Os nomes de usuário e grupo especificados podem ser nomes do Windows ou nomes UNIX.

  Se um tipo de usuário e grupo não for especificado ao criar ou modificar ACLs, o tipo padrão será usuários e grupos do Windows.

- Você pode especificar apenas permissões do Windows.

Criar listas de controle de acesso de compartilhamento SMB

A configuração de permissões de compartilhamento criando listas de controle de acesso (ACLs) para compartilhamentos SMB permite controlar o nível de acesso a um compartilhamento para usuários e grupos.

Sobre esta tarefa

Você pode configurar ACLs de nível de compartilhamento usando nomes de usuário ou grupo do Windows locais ou de domínio ou nomes de usuário ou grupo UNIX.

Antes de criar uma nova ACL, você deve excluir a ACL de compartilhamento padrão `Everyone / Full Control` , que representa um risco de segurança.

No modo de grupo de trabalho, o nome de domínio local é o nome do servidor SMB.

Passos

1. Exclua a ACL de compartilhamento padrão: 'Vserver cifs share access-control delete -vserver <vserver_name> -share <share_name> -user-or-group everyone'
2. Configure a nova ACL:

Se você quiser configurar ACLs usando um…	Digite o comando…
Usuário do Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`
Grupo Windows	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`

Se você quiser configurar ACLs usando um…	Digite o comando…
Utilizador UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
Grupo UNIX	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. Verifique se a ACL aplicada ao compartilhamento está correta usando o `vserver cifs share access-control show` comando.

Exemplo

O comando a seguir `Change` concede permissões ao grupo Windows "'equipe de vendas'" para o compartilhamento "vendas" no vs1.example.com.º SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

O comando a seguir `Read` dá permissão ao grupo UNIX "Engineering" para o compartilhamento "eng" no SVM "vs2.example.com":

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$         BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng        engineering              unix-group  Read
```

Os comandos a seguir `Change` dão permissão ao grupo local do Windows chamado "Tiger Team" e `Full_Control` permissão ao usuário local do Windows chamado "Sue Chang" para o compartilhamento "datavol5" no SVM "VS1":

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- -------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

Comandos para gerenciar listas de controle de acesso de compartilhamento SMB

Você precisa saber os comandos para gerenciar listas de controle de acesso (ACLs) SMB, o que inclui criar, exibir, modificar e excluir.

Se você quiser…	Use este comando…
Crie uma nova ACL	`vserver cifs share access-control create`
Exibir ACLs	`vserver cifs share access-control show`
Modificar uma ACL	`vserver cifs share access-control modify`
Eliminar uma ACL	`vserver cifs share access-control delete`

Proteja o acesso aos arquivos usando permissões de arquivo

Configure permissões avançadas de arquivos NTFS usando a guia Segurança do Windows

Você pode configurar permissões de arquivo NTFS padrão em arquivos e pastas usando a guia **Segurança do Windows** na janela Propriedades do Windows.

Antes de começar

O administrador que executa esta tarefa deve ter permissões NTFS suficientes para alterar permissões nos objetos selecionados.

Sobre esta tarefa

A configuração de permissões de arquivos NTFS é feita em um host do Windows adicionando entradas a listas de controle de acesso discricionárias (DACLs) NTFS associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS. Essas tarefas são tratadas automaticamente pela GUI do Windows.

Passos

1. No menu **Ferramentas** no Windows Explorer, selecione **Mapear unidade de rede**.
2. Preencha a caixa de diálogo **Map Network Drive**:

   a. Selecione uma letra **Drive**.

   b. Na caixa **pasta**, digite o nome do servidor CIFS que contém o compartilhamento que contém os dados aos quais você deseja aplicar permissões e o nome do compartilhamento.

   Se o nome do servidor CIFS for "'CIFS_SERVER'" e o compartilhamento for chamado "hare1", você deverá digitar `\\CIFS_SERVER\share1`.

   > Você pode especificar o endereço IP da interface de dados para o servidor CIFS em vez do nome do servidor CIFS.

   c. Clique em **Finish**.

A unidade selecionada está montada e pronta com a janela do Windows Explorer exibindo arquivos e pastas contidos no compartilhamento.

3. Selecione o arquivo ou diretório para o qual você deseja definir permissões de arquivo NTFS.
4. Clique com o botão direito do rato no ficheiro ou diretório e selecione **Propriedades**.
5. Selecione a guia **Segurança**.

   A guia **Segurança** exibe a lista de usuários e grupos para os quais a permissão NTFS está definida. A caixa **Permissions for** exibe uma lista de permissões de permissão e negação em vigor para cada usuário ou grupo selecionado.

6. Clique em **Avançado**.

   A janela Propriedades do Windows exibe informações sobre permissões de arquivo existentes atribuídas a usuários e grupos.

7. Clique em **alterar permissões**.

   A janela permissões é aberta.

8. Execute as ações desejadas:

Se você quiser…	Faça o seguinte…
Configurar permissões NTFS avançadas para um novo utilizador ou grupo	a. Clique em **Add**. b. Na caixa **Digite o nome do objeto a ser selecionado**, digite o nome do usuário ou grupo que deseja adicionar. c. Clique em **OK**.
Alterar permissões NTFS avançadas de um usuário ou grupo	a. Na caixa **entradas de permissões:**, selecione o usuário ou grupo cujas permissões avançadas você deseja alterar. b. Clique em **Editar**.
Remover permissões NTFS avançadas para um usuário ou grupo	a. Na caixa **entradas de permissões:**, selecione o usuário ou grupo que deseja remover. b. Clique em **Remover**. c. Avance para o passo 13.

   Se você estiver adicionando permissões NTFS avançadas em um novo usuário ou grupo ou alterando permissões avançadas NTFS em um usuário ou grupo existente, a caixa Entrada de permissão para <Object> será aberta.

9. Na caixa **Apply to**, selecione como você deseja aplicar esta entrada de permissão de arquivo NTFS.

   Se você estiver configurando permissões de arquivo NTFS em um único arquivo, a caixa **Apply to** não estará ativa. A configuração **apply to** é padrão para **this object only**.

10. Na caixa **Permissions**, selecione as caixas **allow** ou **deny** para as permissões avançadas que você deseja definir neste objeto.

    ◦ Para permitir o acesso especificado, selecione a caixa **permitir**.

- Para não permitir o acesso especificado, selecione a caixa **Negar**. Você pode definir permissões nos seguintes direitos avançados:
- * Controle total*

  Se você escolher esse direito avançado, todos os outros direitos avançados serão escolhidos automaticamente (permitir ou negar direitos).

- * Traverse pasta / executar arquivo *
- **Lista de pastas / dados de leitura**
- **Leia atributos**
- **Leia atributos estendidos**
- * Criar arquivos / escrever dados *
- * Criar pastas / anexar dados*
- * Escrever atributos*
- **Escreva atributos estendidos**
- **Excluir subpastas e arquivos**
- **Excluir**
- **Permissões de leitura**
- **Alterar permissões**
- **Assuma a propriedade**

  Se qualquer uma das caixas de permissão avançada não for selecionável, é porque as permissões são herdadas do objeto pai.

11. Se você quiser que subpastas e arquivos desse objeto herdem essas permissões, marque a caixa **aplicar essas permissões a objetos e/ou contentores dentro desse contentor somente**.
12. Clique em **OK**.
13. Depois de terminar de adicionar, remover ou editar permissões NTFS, especifique a configuração de herança para este objeto:

    - Selecione a caixa **incluir permissões herdadas a partir da caixa pai** deste objeto.

      Este é o padrão.

    - Selecione a caixa **Substituir todas as permissões de objeto filho por permissões herdadas deste objeto**.

      Esta configuração não está presente na caixa permissões se você estiver definindo permissões de arquivo NTFS em um único arquivo.

Tenha cuidado ao selecionar esta definição. Esta configuração remove todas as permissões existentes em todos os objetos filho e as substitui pelas configurações de permissão deste objeto. Você pode remover inadvertidamente as permissões que você não queria que fossem removidas. É especialmente importante ao definir permissões em um volume ou qtree misto de estilo de segurança. Se objetos filho tiverem um estilo de segurança eficaz UNIX, propagar permissões NTFS para esses objetos filho resulta na alteração do ONTAP desses objetos do estilo de segurança UNIX para o estilo de segurança NTFS e todas as permissões UNIX nesses objetos filho serão substituídas por permissões NTFS.

- Selecione ambas as caixas.
- Selecione nenhuma das caixas.

14. Clique em **OK** para fechar a caixa **permissões**.
15. Clique em **OK** para fechar a caixa **Configurações avançadas de segurança para o <Object>**.

Para obter mais informações sobre como definir permissões NTFS avançadas, consulte a documentação do Windows.

Informações relacionadas

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Configurar permissões de arquivos NTFS usando a CLI do ONTAP

Você pode configurar permissões de arquivos NTFS em arquivos e diretórios usando a CLI do ONTAP. Isso permite configurar permissões de arquivos NTFS sem precisar se conetar aos dados usando um compartilhamento SMB em um cliente Windows.

Você pode configurar permissões de arquivo NTFS adicionando entradas a listas de controle de acesso discricionário NTFS (DACLs) associadas a um descritor de segurança NTFS. O descritor de segurança é então aplicado a arquivos e diretórios NTFS.

Você só pode configurar permissões de arquivo NTFS usando a linha de comando. Você não pode configurar ACLs NFSv4 usando a CLI.

Passos

1. Crie um descritor de segurança NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. Adicione DACLs ao descritor de segurança NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
```

```
{this-folder|sub-folders|files}
```

3. Crie uma política de segurança de arquivo/diretório.

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

Como as permissões de arquivo UNIX fornecem controle de acesso ao acessar arquivos por SMB

Um FlexVol volume pode ter um dos três tipos de estilo de segurança: NTFS, UNIX ou misto. Você pode acessar dados sobre SMB independentemente do estilo de segurança; no entanto, permissões de arquivo UNIX apropriadas são necessárias para acessar dados com segurança efetiva UNIX.

Quando os dados são acessados por SMB, há vários controles de acesso usados para determinar se um usuário está autorizado a executar uma ação solicitada:

- Permissões de exportação

  Configurar permissões de exportação para o acesso SMB é opcional.

- Permissões de compartilhamento
- Permissões de arquivo

  Os seguintes tipos de permissões de arquivo podem ser aplicados aos dados nos quais o usuário deseja executar uma ação:

  - NTFS
  - ACLs do UNIX NFSv4
  - Bits do modo UNIX

Para dados com ACLs NFSv4 ou bits de modo UNIX definidos, as permissões de estilo UNIX são usadas para determinar os direitos de acesso aos dados. O administrador do SVM precisa definir a permissão de arquivo apropriada para garantir que os usuários tenham os direitos para executar a ação desejada.

Os dados em um volume misto de estilo de segurança podem ter um estilo de segurança eficaz NTFS ou UNIX. Se os dados tiverem um estilo de segurança eficaz UNIX, as permissões NFSv4 ou os bits de modo UNIX serão usados ao determinar os direitos de acesso aos dados.

Acesso seguro a arquivos usando o controle de acesso dinâmico (DAC)

Proteja o acesso a ficheiros utilizando a visão geral do controlo de acesso dinâmico (DAC)

Você pode proteger o acesso usando o Controle de Acesso Dinâmico e criando políticas de acesso centrais no ative Directory e aplicando-as a arquivos e pastas em SVMs por meio de objetos de Diretiva de Grupo aplicados (GPOs). Você pode configurar a auditoria para usar eventos de preparação de políticas de acesso central para ver os efeitos das alterações nas políticas de acesso central antes de aplicá-las.

Adições às credenciais CIFS

Antes do Controle de Acesso Dinâmico, uma credencial CIFS incluía a identidade de um responsável de segurança (o usuário) e a associação de grupo do Windows. Com o Dynamic Access Control, mais três tipos de informações são adicionados à identidade do dispositivo, às declarações do dispositivo e às declarações do usuário:

- Identidade do dispositivo

  O analógico das informações de identidade do usuário, exceto se for a identidade e associação de grupo do dispositivo do qual o usuário está fazendo login.

- Reclamações do dispositivo

  Afirmações sobre um dispositivo principal de segurança. Por exemplo, uma alegação de dispositivo pode ser que ela seja membro de uma ou específica.

- Reclamações do utilizador

  Afirmações sobre um responsável de segurança do usuário. Por exemplo, uma alegação de usuário pode ser que sua conta do AD seja membro de uma ou específica.

Políticas de acesso central

As políticas de acesso central para arquivos permitem que as organizações implantem e gerenciem centralmente políticas de autorização que incluem expressões condicionais usando grupos de usuários, reivindicações de usuários, declarações de dispositivos e propriedades de recursos.

Por exemplo, para acessar dados de alto impactos nos negócios, um usuário precisa ser um funcionário em tempo integral e ter acesso apenas aos dados de um dispositivo gerenciado. As políticas de acesso central são definidas no ative Directory e distribuídas para servidores de arquivos através do mecanismo GPO.

Preparação de políticas de acesso central com auditoria avançada

As políticas de acesso central podem ser "envelhecidas", caso em que são avaliadas de forma "'What-if'" durante as verificações de acesso ao arquivo. Os resultados do que teria acontecido se a política estivesse em vigor e como isso difere do que está configurado atualmente são registrados como um evento de auditoria. Dessa forma, os administradores podem usar logs de eventos de auditoria para estudar o impactos de uma alteração de política de acesso antes de realmente colocar a política em jogo. Depois de avaliar o impactos de uma alteração de política de acesso, a política pode ser implantada via GPOs nos SVMs desejados.

Informações relacionadas

GPOs compatíveis

Aplicando objetos de Diretiva de Grupo a servidores CIFS

Ativar ou desativar o suporte de GPO num servidor CIFS

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Configuração de políticas de acesso central para proteger dados em servidores CIFS

Exibindo informações sobre a segurança do controle de acesso dinâmico

"Auditoria de SMB e NFS e rastreamento de segurança"

Funcionalidade de controlo de acesso dinâmico suportada

Se você quiser usar o controle de acesso dinâmico (DAC) em seu servidor CIFS, você precisa entender como o ONTAP suporta a funcionalidade de controle de acesso dinâmico em ambientes do ative Directory.

Suportado para controlo de acesso dinâmico

O ONTAP suporta a seguinte funcionalidade quando o controlo de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Reclamações no sistema de arquivos	Reivindicações são pares simples de nome e valor que afirmam alguma verdade sobre um usuário. As credenciais do usuário contêm informações de reclamação, e os descritores de segurança nos arquivos podem executar verificações de acesso que incluem verificações de reclamações. Isso dá aos administradores um nível mais alto de controle sobre quem pode acessar arquivos.
Expressões condicionais para verificações de acesso a arquivos	Ao modificar os parâmetros de segurança de um arquivo, os usuários podem adicionar expressões condicionais arbitrariamente complexas ao descritor de segurança do arquivo. A expressão condicional pode incluir verificações para reclamações.
Controle central do acesso a arquivos através de políticas de acesso central	As políticas de acesso central são um tipo de ACL armazenada no ative Directory que pode ser marcada para um arquivo. O acesso ao arquivo só é concedido se as verificações de acesso do descritor de segurança no disco e da diretiva de acesso central marcada permitirem o acesso. Isso dá aos administradores a capacidade de controlar o acesso a arquivos de um local central (AD) sem ter que modificar o descritor de segurança no disco.
Preparação da política de acesso central	Adiciona a capacidade de testar alterações de segurança sem afetar o acesso real aos arquivos, "definindo" uma alteração nas políticas de acesso central e vendo o efeito da alteração em um relatório de auditoria.
Suporte para exibir informações sobre a segurança da diretiva de acesso central usando a CLI do ONTAP	Estende o `vserver security file-directory show` comando para exibir informações sobre políticas de acesso centrais aplicadas.

Funcionalidade	Comentários
Rastreamento de segurança que inclui políticas de acesso central	Estende a `vserver security trace` família de comandos para exibir resultados que incluem informações sobre políticas de acesso central aplicadas.

Não suportado para o controlo de acesso dinâmico

O ONTAP não suporta a seguinte funcionalidade quando o controlo de acesso dinâmico está ativado no servidor CIFS:

Funcionalidade	Comentários
Classificação automática de objetos do sistema de arquivos NTFS	Esta é uma extensão para a infra-estrutura de classificação de ficheiros do Windows que não é suportada no ONTAP.
Auditoria avançada que não a preparação de políticas de acesso central	Somente o estadiamento da política de acesso central é suportado para auditoria avançada.

Considerações ao usar o Controle de Acesso Dinâmico e políticas de Acesso Central com servidores CIFS

Há certas considerações que você deve ter em mente ao usar o controle de acesso dinâmico (DAC) e as políticas de acesso central para proteger arquivos e pastas em servidores CIFS.

O acesso NFS pode ser negado ao root se a regra de política se aplicar ao usuário do domínio/administrador

Em determinadas circunstâncias, o acesso NFS à raiz pode ser negado quando a segurança da diretiva de acesso central é aplicada aos dados que o usuário raiz está tentando acessar. O problema ocorre quando a política de acesso central contém uma regra que é aplicada ao domínio/administrador e a conta raiz é mapeada para a conta de domínio/administrador.

Em vez de aplicar uma regra ao utilizador de domínio/administrador, deve aplicar a regra a um grupo com Privileges administrativo, como o grupo de domínio/administradores. Desta forma, pode mapear a raiz para a conta de domínio/administrador sem que a raiz seja afetada por este problema.

O grupo BUILTIN/Administradores do servidor CIFS tem acesso a recursos quando a diretiva de acesso central aplicado não é encontrada no ative Directory

É possível que os recursos contidos no servidor CIFS tenham políticas de acesso central aplicadas a eles, mas quando o servidor CIFS usa o SID da política de acesso central para tentar recuperar informações do ative Directory, o SID não corresponde a nenhum SIDs de política de acesso central existente no ative Directory. Nestas circunstâncias, o servidor CIFS aplica a política de recuperação padrão local para esse recurso.

A política de recuperação padrão local permite o acesso do grupo BUILTIN/Administradores do servidor CIFS a esse recurso.

Ativar ou desativar a descrição geral do controlo de Acesso Dinâmico

A opção que permite utilizar o controlo de Acesso Dinâmico (DAC) para proteger objetos no servidor CIFS está desativada por predefinição. Você deve ativar a opção se quiser usar o Controle de Acesso Dinâmico no servidor CIFS. Se decidir mais tarde que não pretende utilizar o controlo de Acesso Dinâmico para proteger objetos armazenados no servidor CIFS, pode desativar a opção.

Sobre esta tarefa

Uma vez que o Controle de Acesso Dinâmico esteja ativado, o sistema de arquivos pode conter ACLs com entradas relacionadas ao Controle de Acesso Dinâmico. Se o controlo de Acesso Dinâmico estiver desativado, as entradas atuais do controlo de Acesso Dinâmico serão ignoradas e as novas não serão permitidas.

Esta opção está disponível apenas no nível de privilégio avançado.

Passo

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que o Controle de Acesso Dinâmico seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Configuração de políticas de acesso central para proteger dados em servidores CIFS

Gerencie ACLs que contêm ACEs de controle de acesso dinâmico quando o controle de acesso dinâmico estiver desativado

Se você tiver recursos que têm ACLs aplicadas com ACEs de controle de acesso dinâmico e desativar o controle de acesso dinâmico na máquina virtual de armazenamento (SVM), remova os ACEs de controle de acesso dinâmico antes de gerenciar os ACEs de controle de acesso não dinâmico nesse recurso.

Sobre esta tarefa

Depois de o controlo de acesso dinâmico ser desativado, não é possível remover os ACEs de controlo de acesso não dinâmico existentes nem adicionar novos ACEs de controlo de acesso não dinâmico até ter removido os ACEs de controlo de acesso dinâmico existentes.

Você pode usar qualquer ferramenta usada normalmente para gerenciar ACLs para executar essas etapas.

Passos

1. Determine quais ACEs do controle de acesso dinâmico são aplicados ao recurso.
2. Remova os ACEs de controle de acesso dinâmico do recurso.
3. Adicione ou remova ACEs não-Dynamic Access Control conforme desejado do recurso.

Configurar políticas de acesso central para proteger dados em servidores CIFS

Há várias etapas que você deve seguir para proteger o acesso aos dados no servidor CIFS usando políticas de acesso central, incluindo habilitar o DAC (Dynamic Access Control) no servidor CIFS, configurar políticas de acesso central no ative Directory, aplicar as políticas de acesso central a contentores do ative Directory com GPOs e habilitar GPOs no servidor CIFS.

Antes de começar

- O ative Directory deve ser configurado para usar políticas de acesso central.
- Você precisa ter acesso suficiente nos controladores de domínio do ative Directory para criar políticas de acesso centrais e para criar e aplicar GPOs aos contêineres que contêm os servidores CIFS.
- Você precisa ter acesso administrativo suficiente na máquina virtual de storage (SVM) para executar os comandos necessários.

Sobre esta tarefa

As políticas de acesso central são definidas e aplicadas a objetos de diretiva de grupo (GPOs) no active Directory. Você pode consultar a Biblioteca Microsoft TechNet para obter instruções sobre como configurar políticas de acesso central e GPOs.

"Microsoft TechNet Library"

Passos

1. Ative o controle de acesso dinâmico na SVM se ele ainda não estiver habilitado usando o `vserver cifs options modify` comando.

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. Habilite os objetos de diretiva de grupo (GPOs) no servidor CIFS se eles ainda não estiverem habilitados usando o `vserver cifs group-policy modify` comando.

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. Crie regras de acesso central e políticas de acesso central no ative Directory.
4. Crie um objeto de diretiva de grupo (GPO) para implantar as políticas de acesso central no ative Directory.
5. Aplique o GPO ao recipiente onde a conta do computador do servidor CIFS está localizada.
6. Atualize manualmente os GPOs aplicados ao servidor CIFS usando o `vserver cifs group-policy update` comando.

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. Verifique se a diretiva de acesso central GPO é aplicada aos recursos no servidor CIFS usando o `vserver cifs group-policy show-applied` comando.

   O exemplo a seguir mostra que a Diretiva de domínio padrão tem duas diretivas de acesso central

aplicadas ao servidor CIFS:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
------------------------------
    GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
```

```
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Ativar ou desativar o controlo de acesso dinâmico

Apresentar informações sobre a segurança do controlo de acesso dinâmico

Pode apresentar informações sobre a segurança do controlo de acesso dinâmico (DAC) em volumes NTFS e em dados com segurança eficaz NTFS em volumes mistos de estilo de segurança. Isso inclui informações sobre ACEs condicionais, ACEs de recursos e ACEs de política de acesso central. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
Onde a saída é exibida com SIDs de grupo e usuário	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
Sobre segurança de arquivos e diretórios para arquivos e diretórios onde a máscara de bits hexadecimal é traduzida para o formato textual	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

Exemplos

O exemplo a seguir exibe informações de segurança do Dynamic Access Control sobre o caminho `/vol1` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

Informações relacionadas

Exibindo informações sobre as configurações do GPO

Exibindo informações sobre políticas de acesso central

Exibindo informações sobre as regras da política de acesso central

Considerações de reversão para o Controle de Acesso Dinâmico

Você deve estar ciente do que acontece ao reverter para uma versão do ONTAP que não suporta o controle de acesso dinâmico (DAC) e o que você deve fazer antes e depois de reverter.

Se você quiser reverter o cluster para uma versão do ONTAP que não suporte o Controle de Acesso Dinâmico e o Controle de Acesso Dinâmico estiver ativado em uma ou mais máquinas virtuais de armazenamento (SVMs), faça o seguinte antes de reverter:

- Você deve desativar o Controle de Acesso Dinâmico em todos os SVMs que o tenham ativado no cluster.
- É necessário modificar qualquer configuração de auditoria no cluster que contenha o `cap-staging` tipo de evento para usar somente o `file-op` tipo de evento.

Você deve entender e agir sobre algumas considerações importantes de reversão para arquivos e pastas com ACEs de Controle de Acesso Dinâmico:

- Se o cluster for revertido, os ACEs de Controle de Acesso Dinâmico existentes não serão removidos; no entanto, eles serão ignorados nas verificações de acesso ao arquivo.
- Uma vez que os ACEs do controlo de Acesso Dinâmico são ignorados após a reversão, o acesso aos ficheiros será alterado nos ficheiros com ACEs do controlo de Acesso Dinâmico.

  Isso poderia permitir que os usuários acessem arquivos que eles anteriormente não podiam, ou não poderiam acessar arquivos que anteriormente poderiam.

- Você deve aplicar ACEs não-Dynamic Access Control aos arquivos afetados para restaurar seu nível anterior de segurança.

  Isso pode ser feito antes de reverter ou imediatamente após a reversão ser concluída.

> Uma vez que os ACEs do controlo de Acesso Dinâmico são ignorados após a reversão, não é necessário removê-los ao aplicar ACEs do controlo de Acesso não Dinâmico aos ficheiros afetados. No entanto, se desejado, você pode removê-los manualmente.

Onde encontrar informações adicionais sobre como configurar e usar o Controle de Acesso Dinâmico e as políticas de Acesso Central

Recursos adicionais estão disponíveis para ajudá-lo a configurar e usar o controle de acesso dinâmico e as políticas de acesso central.

Você pode encontrar informações sobre como configurar o Controle de Acesso Dinâmico e as políticas de Acesso Central no ative Directory na Biblioteca Microsoft TechNet.

"Microsoft TechNet: Visão geral do cenário Dynamic Access Control"

"Microsoft TechNet: Cenário de Política de Acesso Central"

As referências a seguir podem ajudá-lo a configurar o servidor SMB para usar e dar suporte ao Controle de Acesso Dinâmico e às políticas de Acesso Central:

- **Usando GPOs no servidor SMB**

  Aplicando objetos de Diretiva de Grupo a servidores SMB

- **Configurando a auditoria nas no servidor SMB**

  "Auditoria de SMB e NFS e rastreamento de segurança"

Acesso SMB seguro usando políticas de exportação

Como as políticas de exportação são usadas com o acesso SMB

Se as políticas de exportação para acesso SMB estiverem habilitadas no servidor SMB, as políticas de exportação serão usadas ao controlar o acesso a volumes SVM por clientes SMB. Para acessar dados, você pode criar uma política de exportação que permita o acesso SMB e, em seguida, associá-la aos volumes que contêm compartilhamentos SMB.

Uma política de exportação tem uma ou mais regras aplicadas a ela que especifica quais clientes têm permissão de acesso aos dados e quais protocolos de autenticação são suportados para acesso somente leitura e gravação. Você pode configurar políticas de exportação para permitir o acesso por SMB a todos os clientes, uma sub-rede de clientes ou um cliente específico e para permitir a autenticação usando autenticação Kerberos, autenticação NTLM ou autenticação Kerberos e NTLM ao determinar o acesso somente leitura e gravação aos dados.

Depois de processar todas as regras de exportação aplicadas à política de exportação, o ONTAP pode determinar se o cliente recebe acesso e que nível de acesso é concedido. As regras de exportação se aplicam a máquinas cliente, não a usuários e grupos do Windows. As regras de exportação não substituem a autenticação e autorização baseadas em grupo e no utilizador do Windows. As regras de exportação fornecem outra camada de segurança de acesso, além das permissões de compartilhamento e acesso a arquivos.

Você associa exatamente uma política de exportação a cada volume para configurar o acesso do cliente ao volume. Cada SVM pode conter várias políticas de exportação. Isso permite que você faça o seguinte para SVMs com vários volumes:

- Atribua diferentes políticas de exportação a cada volume do SVM para controle de acesso de cliente individual a cada volume no SVM.
- Atribua a mesma política de exportação a vários volumes do SVM para controle de acesso de cliente idêntico sem precisar criar uma nova política de exportação para cada volume.

Cada SVM tem pelo menos uma política de exportação chamada "falha", que não contém regras. Não é possível excluir esta política de exportação, mas você pode renomeá-la ou modificá-la. Por padrão, cada volume no SVM está associado à política de exportação padrão. Se as políticas de exportação para acesso SMB estiverem desativadas no SVM, a política de exportação "falha" não terá efeito no acesso SMB.

Você pode configurar regras que fornecem acesso a hosts NFS e SMB e associar essa regra a uma política de exportação, que pode ser associada ao volume que contém dados ao qual hosts NFS e SMB precisam acessar. Alternativamente, se houver alguns volumes em que apenas clientes SMB exigem acesso, você poderá configurar uma política de exportação com regras que só permitem acesso usando o protocolo SMB e que usa apenas Kerberos ou NTLM (ou ambos) para autenticação para acesso somente leitura e gravação. A política de exportação é então associada aos volumes em que apenas o acesso SMB é desejado.

Se as políticas de exportação para SMB estiverem ativadas e um cliente fizer uma solicitação de acesso não permitida pela política de exportação aplicável, a solicitação falhará com uma mensagem de permissão negada. Se um cliente não corresponder a nenhuma regra na política de exportação do volume, o acesso será negado. Se uma política de exportação estiver vazia, todos os acessos serão implicitamente negados. Isso é verdade mesmo se as permissões de compartilhamento e arquivo permitissem o acesso. Isso significa que você deve configurar sua política de exportação para permitir minimamente o seguinte em volumes que contêm compartilhamentos SMB:

- Permitir o acesso a todos os clientes ou ao subconjunto apropriado de clientes
- Permitir acesso através de SMB
- Permitir acesso apropriado somente leitura e gravação usando a autenticação Kerberos ou NTLM (ou ambas)

Saiba mais "configuração e gerenciamento de políticas de exportação"sobre .

Como funcionam as regras de exportação

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente a um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente.

Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação. A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

Você pode configurar regras de exportação para determinar permissões de acesso do cliente usando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação, por exemplo, NFSv4 ou SMB.
- Um identificador de cliente, por exemplo, nome de host ou endereço IP.

  O tamanho máximo para o `-clientmatch` campo é de 4096 carateres.

- O tipo de segurança usado pelo cliente para autenticar, por exemplo, Kerberos v5, NTLM ou AUTH_SYS.

Se uma regra especificar vários critérios, o cliente deve corresponder a todos eles para que a regra seja aplicada.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv3 e o cliente tem o endereço IP 10,1.17,37.

Mesmo que o protocolo de acesso do cliente corresponda, o endereço IP do cliente está em uma sub-rede diferente da especificada na regra de exportação. Portanto, a correspondência do cliente falha e esta regra não se aplica a este cliente.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

A solicitação de acesso do cliente é enviada usando o protocolo NFSv4 e o cliente tem o endereço IP 10,1.16,54.

O protocolo de acesso do cliente corresponde e o endereço IP do cliente está na sub-rede especificada. Portanto, a correspondência do cliente é bem-sucedida e esta regra se aplica a este cliente. O cliente obtém acesso de leitura e gravação independentemente do seu tipo de segurança.

Exemplo

A política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

O cliente nº 1 tem o endereço IP 10,1.16,207, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com Kerberos v5.

O cliente nº 2 tem o endereço IP 10,1.16,211, envia uma solicitação de acesso usando o protocolo NFSv3 e autenticado com AUTH_SYS.

O protocolo de acesso do cliente e o endereço IP correspondem a ambos os clientes. O parâmetro somente leitura permite o acesso somente leitura a todos os clientes, independentemente do tipo de segurança com o qual eles autenticaram. Portanto, ambos os clientes recebem acesso somente leitura. No entanto, somente o cliente nº 1 obtém acesso de leitura e gravação porque usou o tipo de segurança aprovado Kerberos v5 para autenticar. O cliente nº 2 não obtém acesso de leitura e gravação.

Exemplos de regras de política de exportação que restringem ou permitem acesso através de SMB

Os exemplos mostram como criar regras de política de exportação que restringem ou permitem o acesso ao SMB em um SVM que tenha políticas de exportação para acesso ao SMB ativadas.

As políticas de exportação para o acesso SMB estão desativadas por predefinição. Você precisa configurar regras de política de exportação que restrinjam ou permitam acesso ao SMB somente se você tiver ativado políticas de exportação para acesso ao SMB.

Regra de exportação apenas para acesso SMB

O comando a seguir cria uma regra de exportação no SVM chamado "'VS1" que tem a seguinte configuração:

- Nome da política: cifs1
- Número de índice: 1

- Correspondência de cliente: Corresponde apenas a clientes na rede 192.168.1.0/24
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Para clientes que usam autenticação NTLM ou Kerberos
- Acesso de leitura-gravação: Para clientes que usam a autenticação Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

Regra de exportação para SMB e acesso NFS

O comando a seguir cria uma regra de exportação no SVM chamado"' VS1" que tem a seguinte configuração:

- Nome da política: cifsnfs1
- Número de índice: 2
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Acesso SMB e NFS
- Acesso somente leitura: Para todos os clientes
- Acesso de leitura e gravação: Para clientes que usam Kerberos (NFS e SMB) ou autenticação NTLM (SMB)
- Mapeamento para ID de usuário UNIX 0 (zero): Mapeado para ID de usuário 65534 (que normalmente mapeia para o nome de usuário ninguém)
- Acesso suid e sgid: Permite

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

Regra de exportação para acesso SMB usando apenas NTLM

O comando a seguir cria uma regra de exportação no SVM chamado "'VS1" que tem a seguinte configuração:

- Nome da política: ntlm1
- Número de índice: 1
- Correspondência do cliente: Corresponde a todos os clientes
- Protocolo: Ativa apenas o acesso SMB
- Acesso somente leitura: Somente para clientes que usam NTLM
- Acesso de leitura e gravação: Apenas para clientes que utilizam NTLM

Se você configurar a opção somente leitura ou a opção leitura-gravação para acesso somente NTLM, você deverá usar entradas baseadas em endereço IP na opção correspondência do cliente. Caso contrário, você recebe `access denied` erros. Isso ocorre porque o ONTAP usa os nomes principais do Serviço Kerberos (SPN) ao usar um nome de host para verificar os direitos de acesso do cliente. A autenticação NTLM não suporta nomes SPN.

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

Ativar ou desativar políticas de exportação para acesso SMB

Você pode ativar ou desativar políticas de exportação para acesso SMB em máquinas virtuais de armazenamento (SVMs). O uso de políticas de exportação para controlar o acesso SMB a recursos é opcional.

Antes de começar

A seguir estão os requisitos para ativar políticas de exportação para SMB:

- O cliente deve ter um Registro "PTR" no DNS antes de criar as regras de exportação para esse cliente.
- Um conjunto adicional de Registros "'A'" e "'PTR'" para nomes de host é necessário se o SVM fornecer acesso a clientes NFS e o nome de host que você deseja usar para acesso NFS for diferente do nome do servidor CIFS.

Sobre esta tarefa

Ao configurar um novo servidor CIFS na SVM, o uso de políticas de exportação para acesso SMB é desativado por padrão. Você pode habilitar políticas de exportação para acesso SMB se quiser controlar o acesso com base no protocolo de autenticação ou em endereços IP de cliente ou nomes de host. Você pode ativar ou desativar políticas de exportação para acesso SMB a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ativar ou desativar políticas de exportação:
   - Ativar políticas de exportação: `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - Desativar políticas de exportação: `vserver cifs options modify -vserver` *`vserver_name`* `-is-exportpolicy-enabled false`
3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir permite o uso de políticas de exportação para controlar o acesso de clientes SMB a recursos no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Além de proteger o acesso usando a segurança nativa em nível de arquivo e exportar e compartilhar, você pode configurar o Storage-Level Access Guard, uma terceira camada de segurança aplicada pelo ONTAP no nível de volume. O Storage-Level Access Guard se aplica ao acesso de todos os protocolos nas ao objeto de storage ao qual ele é aplicado.

Apenas as permissões de acesso NTFS são suportadas. Para que o ONTAP execute verificações de segurança em usuários UNIX para obter acesso a dados em volumes para os quais o Guarda de Acesso em nível de storage foi aplicado, o usuário do UNIX deve mapear para um usuário do Windows na SVM que possua o volume.

Comportamento do Access Guard no nível de storage

- O Storage-Level Access Guard aplica-se a todos os arquivos ou a todos os diretórios em um objeto de armazenamento.

  Como todos os arquivos ou diretórios em um volume estão sujeitos às configurações do Storage-Level Access Guard, a herança através da propagação não é necessária.

- Você pode configurar o Storage-Level Access Guard para se aplicar apenas a arquivos, apenas a diretórios ou a arquivos e diretórios dentro de um volume.
  - Segurança de arquivos e diretórios

    Aplica-se a cada diretório e arquivo dentro do objeto de armazenamento. Esta é a configuração padrão.

  - Segurança de arquivos

    Aplica-se a todos os arquivos dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de diretórios.

  - Segurança do diretório

    Aplica-se a todos os diretórios dentro do objeto de armazenamento. A aplicação dessa segurança não afeta o acesso ou a auditoria de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

- Se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard.

  Ele é aplicado no nível do objeto de armazenamento e armazenado nos metadados usados para determinar as permissões efetivas.

- A segurança no nível do storage não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX).

  Ele foi desenvolvido para ser modificado apenas por administradores de storage.

- Você pode aplicar o Storage-Level Access Guard a volumes com NTFS ou estilo de segurança misto.
- Você pode aplicar o Storage-Level Access Guard a volumes com estilo de segurança UNIX, desde que o SVM que contém o volume tenha um servidor CIFS configurado.
- Quando os volumes são montados sob um caminho de junção de volume e se o Storage-Level Access Guard estiver presente nesse caminho, ele não será propagado para volumes montados sob ele.
- O descritor de segurança do Access Guard em nível de storage é replicado com a replicação de dados do SnapMirror e com replicação SVM.
- Há dispensação especial para scanners de vírus.

  Acesso excecional é permitido a esses servidores para exibir arquivos e diretórios, mesmo que o Storage-Level Access Guard negue acesso ao objeto.

- As notificações FPolicy não são enviadas se o acesso for negado devido ao Storage-Level Access Guard.

Verificações de ordem de acesso

O acesso a um arquivo ou diretório é determinado pelo efeito combinado das permissões de exportação ou compartilhamento, as permissões de guarda de acesso em nível de armazenamento definidas em volumes e as permissões de arquivo nativo aplicadas a arquivos e/ou diretórios. Todos os níveis de segurança são avaliados para determinar quais as permissões efetivas de um arquivo ou diretório. As verificações de acesso de segurança são realizadas na seguinte ordem:

1. Permissões de compartilhamento SMB ou nível de exportação NFS
2. Proteção de acesso no nível de storage
3. Listas de controle de acesso (ACLs) de arquivos/pastas NTFS, ACLs NFSv4 ou bits de modo UNIX

Casos de uso para usar o Storage-Level Access Guard

O Storage-Level Access Guard fornece segurança adicional no nível de armazenamento, que não é visível do lado do cliente; portanto, ele não pode ser revogado por nenhum dos usuários ou administradores de seus desktops. Há certos casos de uso em que a capacidade de controlar o acesso no nível de storage é benéfica.

Os casos de uso típicos para esse recurso incluem os seguintes cenários:

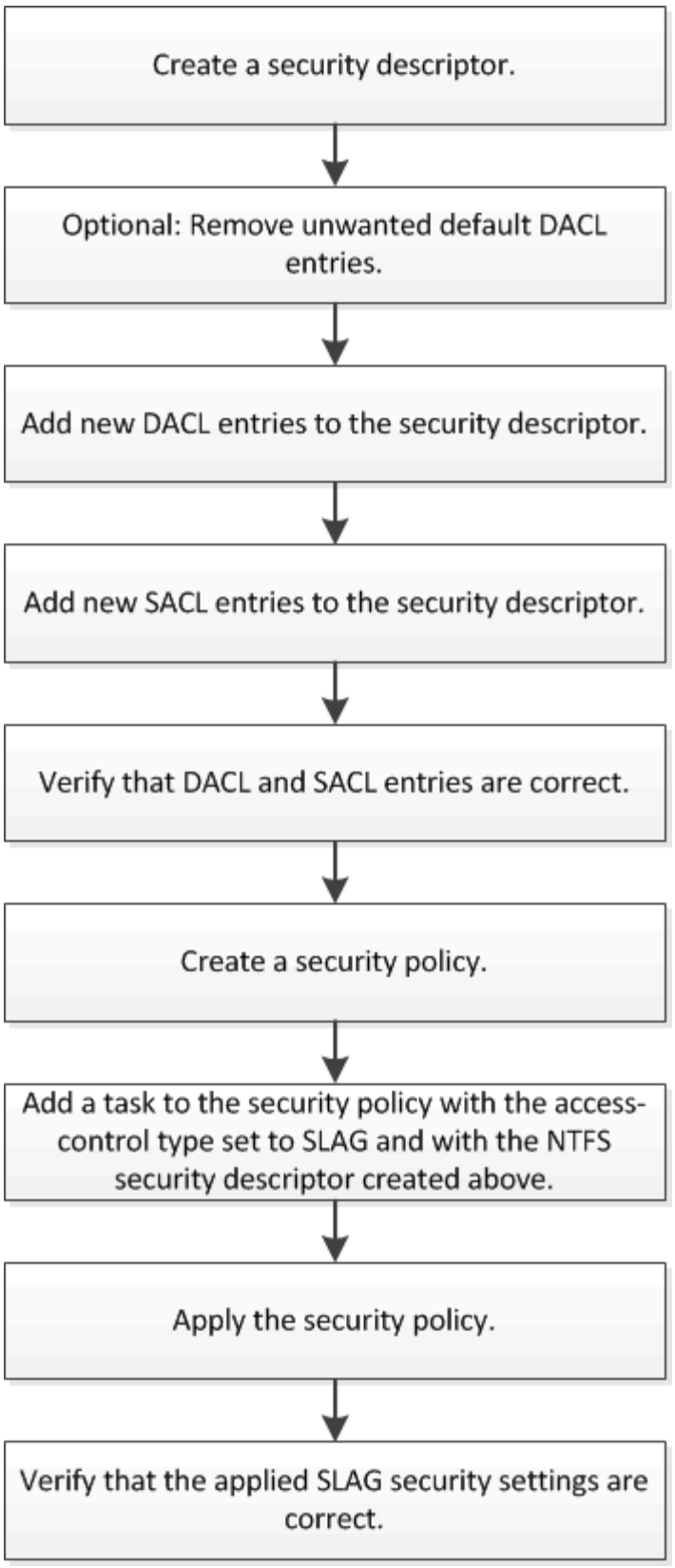
- Proteção da propriedade intelectual através da auditoria e controlo do acesso de todos os utilizadores ao

nível do armazenamento

- Armazenamento para empresas de serviços financeiros, incluindo bancos e grupos de negociação
- Serviços governamentais dos EUA com storage de arquivos separado para departamentos individuais
- Universidades protegendo todos os arquivos dos alunos

Fluxo de trabalho para configurar o Storage-Level Access Guard

O fluxo de trabalho para configurar o guarda de acesso em nível de armazenamento (SLAG) usa os mesmos comandos CLI do ONTAP que você usa para configurar permissões de arquivos NTFS e políticas de auditoria. Em vez de configurar o acesso a arquivos e diretórios em um destino designado, você configura O SLAG no volume designado de máquina virtual de armazenamento (SVM).



Informações relacionadas

Configurando o Storage-Level Access Guard

Configurar o Storage-Level Access Guard

Há uma série de etapas que você precisa seguir para configurar o Storage-Level Access Guard em um volume ou qtree. O Storage-Level Access Guard fornece um nível de segurança de acesso definido no nível de armazenamento. Ele fornece segurança que se aplica a todos os acessos de todos os protocolos nas ao objeto de storage ao qual foi aplicado.

Passos

1. Crie um descritor de segurança usando o `vserver security file-directory ntfs create` comando.

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   Um descritor de segurança é criado com as quatro entradas de controle de acesso (ACEs) padrão a seguir:

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Se você não quiser usar as entradas padrão ao configurar o Storage-Level Access Guard, você pode removê-las antes de criar e adicionar seus próprios ACEs ao descritor de segurança.

2. Remova qualquer um dos ACEs DACL padrão do descritor de segurança que você não deseja configurar

com segurança Storage-Level Access Guard:

a. Remova quaisquer ACEs DACL indesejados usando o `vserver security file-directory ntfs dacl remove` comando.

   Neste exemplo, três ACEs DACL padrão são removidos do descritor de segurança: BUILTIN/Administrators, BUILTIN/Users e CREATOR OWNER.

   ```
   vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
   -access-type allow -account builtin\users vserver security file-directory
   ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
   builtin\administrators vserver security file-directory ntfs dacl remove
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
   ```

b. Verifique se os ACEs DACL que você não deseja usar para a segurança Storage-Level Access Guard são removidos do descritor de segurança usando o `vserver security file-directory ntfs dacl show` comando.

   Neste exemplo, a saída do comando verifica se três ACEs DACL padrão foram removidos do descritor de segurança, deixando apenas a entrada DACA ACE padrão DA AUTORIDADE NT/SISTEMA:

   ```
   vserver security file-directory ntfs dacl show -vserver vs1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. Adicione uma ou mais entradas DACL a um descritor de segurança usando o `vserver security file-directory ntfs dacl add` comando.

   Neste exemplo, dois ACEs DACL são adicionados ao descritor de segurança:

   ```
   vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
   -access-type allow -account example\engineering -rights full-control -apply-to
   this-folder,sub-folders,files vserver security file-directory ntfs dacl add
   -vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
   -rights read -apply-to this-folder,sub-folders,files
   ```

4. Adicione uma ou mais entradas SACL a um descritor de segurança usando o `vserver security file-directory ntfs sacl add` comando.

   Neste exemplo, dois ACEs SACL são adicionados ao descritor de segurança:

   ```
   vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
   ```

```
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verifique se os ACEs DACL e SACL estão configurados corretamente utilizando os `vserver security file-directory ntfs dacl show` comandos e `vserver security file-directory ntfs sacl show`, respetivamente.

   Neste exemplo, o comando a seguir exibe informações sobre entradas DACL para descritor de segurança "D1":

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   ```

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       EXAMPLE\Domain Users
                        allow    read           this-folder, sub-folders,
   files
       EXAMPLE\engineering
                        allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   Neste exemplo, o comando a seguir exibe informações sobre entradas SACL para descritor de segurança "D1":

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   ```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. Crie uma política de segurança usando o `vserver security file-directory policy create` comando.

   O exemplo a seguir cria uma política chamada "policy1":

   ```
   vserver security file-directory policy create -vserver vs1 -policy-name
   policy1
   ```

7. Verifique se a política está corretamente configurada usando o `vserver security file-directory policy show` comando.

   ```
   vserver security file-directory policy show
   ```

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança usando o `vserver security file-directory policy task add` comando com o `-access-control` parâmetro definido como `slag`.

   Mesmo que uma política possa conter mais de uma tarefa Storage-Level Access Guard, você não pode configurar uma política para conter tarefas de diretório de arquivo e Guarda de acesso no nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

   Neste exemplo, uma tarefa é adicionada à política chamada "'policy1", que é atribuída ao descritor de segurança "'D1'". Ele é atribuído ao `/datavol1` caminho com o tipo de controle de acesso definido como "lag".

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. Verifique se a tarefa está configurada corretamente usando o `vserver security file-directory`

`policy task show` comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name
policy1
```

```
 Vserver: vs1
  Policy: policy1

   Index  File/Folder  Access           Security  NTFS       NTFS
Security
          Path         Control          Type      Mode       Descriptor
Name
   -----  -----------  ---------------  --------  ----------
---------------
   1      /datavol1    slag             ntfs      propagate  sd1
```

10. Aplique a política de segurança Storage-Level Access Guard usando o `vserver security file-directory apply` comando.

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    O trabalho para aplicar a política de segurança está agendado.

11. Verifique se as configurações de segurança do Access Guard no nível de armazenamento aplicado estão corretas usando o `vserver security file-directory show` comando.

    Neste exemplo, a saída do comando mostra que a segurança do Storage-Level Access Guard foi aplicada ao volume NTFS `/datavol1` . Mesmo que a DACL padrão que permite o controle total para todos permaneça, a segurança do Storage-Level Access Guard restringe (e audita) o acesso aos grupos definidos nas configurações do Storage-Level Access Guard.

    ```
    vserver security file-directory show -vserver vs1 -path /datavol1
    ```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

Gerenciamento da segurança de arquivos NTFS, políticas de auditoria NTFS e Guarda de acesso em nível de armazenamento em SVMs usando a CLI

Fluxo de trabalho para configurar o Storage-Level Access Guard

Exibindo informações sobre o Storage-Level Access Guard

Remoção do Storage-Level Access Guard

Matriz DE ESCÓRIA eficaz

Você pode configurar O SLAG em um volume ou uma qtree ou ambos. A matriz DE ESCÓRIA define em que volume ou qtree é a configuração DE ESCÓRIA aplicável em vários cenários listados na tabela.

	ESCÓRIA de volume num AFS	**ESCÓRIA de volume em uma cópia Snapshot**	**ESCÓRIA de Qtree em um AFS**	**ESCÓRIA de Qtree em uma cópia Snapshot**
Acesso de volume num sistema de ficheiros de acesso (AFS)	SIM	NÃO	N/A.	N/A.
Acesso de volume em uma cópia Snapshot	SIM	NÃO	N/A.	N/A.
Acesso Qtree em um AFS (quando ESCÓRIA está presente na qtree)	NÃO	NÃO	SIM	NÃO
Acesso Qtree em um AFS (quando ESCÓRIA não está presente em qtree)	SIM	NÃO	NÃO	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA está presente no qtree AFS)	NÃO	NÃO	SIM	NÃO
Acesso Qtree na cópia Snapshot (quando A ESCÓRIA não está presente na qtree AFS)	SIM	NÃO	NÃO	NÃO

Exibir informações sobre o Storage-Level Access Guard

O Storage-Level Access Guard é uma terceira camada de segurança aplicada em um volume ou qtree. As configurações do Access Guard no nível de armazenamento não podem ser visualizadas usando a janela Propriedades do Windows. Você deve usar a CLI do ONTAP para exibir informações sobre a segurança do Guarda de acesso em nível de armazenamento, que pode ser usada para validar sua configuração ou para

solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para o volume ou qtree cujas informações de segurança do Storage-Level Access Guard você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

Passo

1. Exibir as configurações de segurança do Access Guard no nível de armazenamento com o nível de detalhe desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemplos

O exemplo a seguir exibe informações de segurança do Access Guard no nível de armazenamento para o volume de estilo de segurança NTFS com o caminho `/datavol1` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

O exemplo a seguir exibe as informações do Access Guard no nível de storage sobre o volume de estilo de segurança misto no caminho `/datavol5` do SVM VS1. O nível superior deste volume tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Remova o Storage-Level Access Guard

Você pode remover o Storage-Level Access Guard em um volume ou qtree se não quiser mais definir a segurança de acesso no nível de armazenamento. A remoção do Storage-Level Access Guard não modifica ou remove a segurança regular do arquivo NTFS e do diretório.

Passos

1. Verifique se o volume ou a qtree tem o Storage-Level Access Guard configurado usando o `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. Remova o Storage-Level Access Guard usando o `vserver security file-directory remove-slag` comando.

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. Verifique se o Storage-Level Access Guard foi removido do volume ou qtree usando o `vserver security file-directory show` comando.

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

Gerencie o acesso a arquivos usando SMB

Use usuários e grupos locais para autenticação e autorização

Como o ONTAP usa usuários e grupos locais

Conceitos de usuários e grupos locais

Você deve saber o que são usuários e grupos locais e algumas informações básicas sobre eles, antes de determinar se deseja configurar e usar usuários e grupos locais em seu ambiente.

- **Usuário local**

  Uma conta de usuário com um identificador de segurança exclusivo (SID) que tem visibilidade somente na máquina virtual de armazenamento (SVM) na qual é criada. As contas de usuário locais têm um conjunto de atributos, incluindo nome de usuário e SID. Uma conta de usuário local autentica localmente no servidor CIFS usando autenticação NTLM.

  As contas de usuário têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges a um usuário.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.

- **Grupo local**

  Um grupo com um SID exclusivo tem visibilidade somente na SVM em que ele é criado. Grupos contêm um conjunto de membros. Os membros podem ser usuários locais, usuários de domínio, grupos de domínio e contas de máquinas de domínio. Os grupos podem ser criados, modificados ou excluídos.

  Os grupos têm vários usos:

  - Usado para conceder *Gerenciamento de Direitos de Usuário* Privileges aos seus membros.
  - Usado para controlar o acesso em nível de compartilhamento e em nível de arquivo aos recursos de arquivo e pasta que o SVM possui.
- **Domínio local**

  Um domínio que tem escopo local, limitado pelo SVM. O nome do domínio local é o nome do servidor CIFS. Os usuários e grupos locais estão contidos no domínio local.

- **Identificador de segurança (SID)**

  Um SID é um valor numérico de comprimento variável que identifica os princípios de segurança do estilo Windows. Por exemplo, um SID típico assume a seguinte forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- * Autenticação NTLM*

  Um método de segurança do Microsoft Windows usado para autenticar usuários em um servidor CIFS.

- **Banco de dados replicado em cluster (RDB)**

  Um banco de dados replicado com uma instância em cada nó em um cluster. Os objetos de usuário local e grupo são armazenados no RDB.

Razões para criar usuários locais e grupos locais

Há várias razões para criar usuários locais e grupos locais na sua máquina virtual de storage (SVM). Por exemplo, você pode acessar um servidor SMB usando uma conta de usuário local se os controladores de domínio (DCs) não estiverem disponíveis, talvez queira usar grupos locais para atribuir Privileges ou se o servidor SMB estiver em um grupo de trabalho.

Você pode criar uma ou mais contas de usuário locais pelos seguintes motivos:

- Seu servidor SMB está em um grupo de trabalho e os usuários de domínio não estão disponíveis.

  Os utilizadores locais são necessários nas configurações do grupo de trabalho.

- Você deseja a capacidade de autenticar e fazer login no servidor SMB se os controladores de domínio não estiverem disponíveis.

  Os usuários locais podem se autenticar com o servidor SMB usando a autenticação NTLM quando o controlador de domínio está inativo ou quando problemas de rede impedem que o servidor SMB entre em Contato com o controlador de domínio.

- Você deseja atribuir *User Rights Management* Privileges a um usuário local.

User Rights Management é a capacidade de um administrador de servidor SMB controlar quais direitos os usuários e grupos têm no SVM. Você pode atribuir Privileges a um usuário atribuindo o Privileges à conta do usuário ou tornando o usuário membro de um grupo local que tenha esses Privileges.

Você pode criar um ou mais grupos locais pelos seguintes motivos:

- O servidor SMB está em um grupo de trabalho e os grupos de domínio não estão disponíveis.

  Os grupos locais não são necessários nas configurações do grupo de trabalho, mas podem ser úteis para gerenciar o Access Privileges para usuários locais do grupo de trabalho.

- Você deseja controlar o acesso aos recursos de arquivos e pastas usando grupos locais para controle de compartilhamento e acesso a arquivos.
- Você deseja criar grupos locais com *User Rights Management* Privileges personalizado.

  Alguns grupos de utilizadores incorporados têm Privileges predefinidos. Para atribuir um conjunto personalizado de Privileges, você pode criar um grupo local e atribuir o Privileges necessário a esse grupo. Em seguida, você pode adicionar usuários locais, usuários de domínio e grupos de domínio ao grupo local.

Informações relacionadas

Como funciona a autenticação de usuário local

Lista de Privileges suportados

Como funciona a autenticação de usuário local

Antes que um usuário local possa acessar dados em um servidor CIFS, o usuário deve criar uma sessão autenticada.

Como o SMB é baseado em sessão, a identidade do usuário pode ser determinada apenas uma vez, quando a sessão é configurada pela primeira vez. O servidor CIFS usa autenticação baseada em NTLM ao autenticar usuários locais. Tanto o NTLMv1 como o NTLMv2 são suportados.

O ONTAP usa autenticação local em três casos de uso. Cada caso de uso depende se a parte do domínio do nome de usuário (com o formato DOMÍNIO/usuário) corresponde ao nome de domínio local do servidor CIFS (o nome do servidor CIFS):

- A parte do domínio corresponde

  Os usuários que fornecem credenciais de usuário local ao solicitar acesso aos dados são autenticados localmente no servidor CIFS.

- A parte do domínio não corresponde

  O ONTAP tenta usar a autenticação NTLM com um controlador de domínio no domínio ao qual o servidor CIFS pertence. Se a autenticação for bem-sucedida, o login será concluído. Se não for bem-sucedido, o que acontece a seguir depende do motivo pelo qual a autenticação não foi bem-sucedida.

  Por exemplo, se o usuário existir no ative Directory mas a senha for inválida ou expirada, o ONTAP não tentará usar a conta de usuário local correspondente no servidor CIFS. Em vez disso, a autenticação falha. Existem outros casos em que o ONTAP usa a conta local correspondente no servidor CIFS, se existir, para autenticação - mesmo que os nomes de domínio NetBIOS não correspondam. Por exemplo,

se existir uma conta de domínio correspondente mas estiver desativada, o ONTAP utiliza a conta local correspondente no servidor CIFS para autenticação.

- A parte do domínio não é especificada

  O ONTAP tenta pela primeira vez a autenticação como um usuário local. Se a autenticação como um usuário local falhar, o ONTAP autenticará o usuário com um controlador de domínio no domínio ao qual o servidor CIFS pertence.

Depois que a autenticação de usuário local ou de domínio for concluída com sucesso, o ONTAP constrói um token de acesso completo de usuário, que leva em conta a associação de grupo local e o Privileges.

Para obter mais informações sobre autenticação NTLM para usuários locais, consulte a documentação do Microsoft Windows.

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Como os tokens de acesso do usuário são construídos

Quando um usuário mapeia um compartilhamento, uma sessão SMB autenticada é estabelecida e um token de acesso de usuário é construído que contém informações sobre o usuário, a associação de grupo do usuário e Privileges cumulativos e o usuário UNIX mapeado.

A menos que a funcionalidade esteja desativada, as informações de usuário local e grupo também são adicionadas ao token de acesso do usuário. A forma como os tokens de acesso são construídos depende se o login é para um usuário local ou um usuário de domínio do ative Directory:

- Início de sessão do utilizador local

  Embora os usuários locais possam ser membros de diferentes grupos locais, os grupos locais não podem ser membros de outros grupos locais. O token de acesso de usuário local é composto por uma união de todos os Privileges atribuídos a grupos aos quais um usuário local específico é membro.

- Login de usuário de domínio

  Quando um usuário de domínio faz login, o ONTAP obtém um token de acesso de usuário que contém o SID do usuário e os SIDs para todos os grupos de domínio aos quais o usuário é membro. O ONTAP usa a união do token de acesso do usuário de domínio com o token de acesso fornecido por associações locais dos grupos de domínio do usuário (se houver), bem como qualquer Privileges direto atribuído ao usuário do domínio ou qualquer uma de suas associações de grupo de domínio.

Para login de usuário local e de domínio, o RID de grupo principal também é definido para o token de acesso do usuário. O RID predefinido é `Domain Users` (RID 513). Não é possível alterar a predefinição.

O processo de mapeamento de nomes do Windows para UNIX e UNIX para Windows segue as mesmas regras para contas locais e de domínio.

> Não há mapeamento automático implícito de um usuário UNIX para uma conta local. Se isso for necessário, uma regra de mapeamento explícito deve ser especificada usando os comandos de mapeamento de nomes existentes.

Diretrizes para o uso do SnapMirror em SVMs que contêm grupos locais

Você deve estar ciente das diretrizes ao configurar o SnapMirror em volumes de propriedade de SVMs que contêm grupos locais.

Não é possível usar grupos locais em ACEs aplicados a arquivos, diretórios ou compartilhamentos replicados pelo SnapMirror para outro SVM. Se você usar o recurso SnapMirror para criar um espelhamento de DR para um volume em outro SVM e o volume tiver um ACE para um grupo local, o ACE não será válido no espelhamento. Se os dados forem replicados para uma SVM diferente, eles serão migrados para um domínio local diferente. As permissões concedidas a usuários e grupos locais são válidas somente dentro do escopo do SVM no qual foram criados originalmente.

O que acontece com usuários e grupos locais ao excluir servidores CIFS

O conjunto padrão de usuários e grupos locais é criado quando um servidor CIFS é criado e eles são associados à máquina virtual de armazenamento (SVM) que hospeda o servidor CIFS. Os administradores do SVM podem criar usuários e grupos locais a qualquer momento. Você precisa estar ciente do que acontece com usuários e grupos locais quando você exclui o servidor CIFS.

Usuários e grupos locais estão associados a SVMs; portanto, eles não são excluídos quando os servidores CIFS são excluídos devido a considerações de segurança. Embora os usuários e grupos locais não sejam excluídos quando o servidor CIFS é excluído, eles ficam ocultos. Não é possível exibir ou gerenciar usuários e grupos locais até que você crie novamente um servidor CIFS no SVM.

O status administrativo do servidor CIFS não afeta a visibilidade de usuários ou grupos locais.

Como você pode usar o Microsoft Management Console com usuários e grupos locais

Você pode exibir informações sobre usuários e grupos locais no Console de Gerenciamento da Microsoft. Com esta versão do ONTAP, não é possível executar outras tarefas de gerenciamento para usuários e grupos locais a partir do Console de Gerenciamento da Microsoft.

Diretrizes para reverter

Se você pretende reverter o cluster para uma versão do ONTAP que não ofereça suporte a usuários e grupos locais e usuários e grupos locais estejam sendo usados para gerenciar o acesso a arquivos ou direitos de usuário, você deve estar ciente de certas considerações.

- Devido a razões de segurança, as informações sobre usuários locais configurados, grupos e Privileges não são excluídas quando o ONTAP é revertido para uma versão que não suporta a funcionalidade de usuários locais e grupos.
- Após a reversão para uma versão principal anterior do ONTAP, o ONTAP não usa usuários e grupos locais durante a autenticação e criação de credenciais.
- Os utilizadores e grupos locais não são removidos das ACLs de ficheiros e pastas.
- Solicitações de acesso a arquivos que dependem do acesso concedido devido às permissões concedidas a usuários ou grupos locais são negadas.

Para permitir o acesso, você deve reconfigurar as permissões de arquivo para permitir o acesso com base em objetos de domínio em vez de objetos de usuário local e grupo.

O que são os Privileges locais

Lista de Privileges suportados

O ONTAP tem um conjunto predefinido de Privileges suportados. Alguns grupos locais predefinidos têm alguns desses Privileges adicionados a eles por padrão. Você também pode adicionar ou remover Privileges dos grupos predefinidos ou criar novos usuários ou grupos locais e adicionar Privileges aos grupos criados ou aos usuários e grupos de domínio existentes.

A tabela a seguir lista os Privileges suportados na máquina virtual de armazenamento (SVM) e fornece uma lista de grupos BUILTIN com Privileges atribuídos:

Nome do privilégio	Configuração de segurança padrão	Descrição
`SeTcbPrivilege`	Nenhum	Agir como parte do sistema operacional
`SeBackupPrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Faça backup de arquivos e diretórios, substituindo quaisquer ACLs
`SeRestorePrivilege`	`BUILTIN\Administrators`, `BUILTIN\Backup Operators`	Restaure arquivos e diretórios, substituindo qualquer ACLs defina qualquer SID válido de usuário ou grupo como proprietário do arquivo
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	Assuma a propriedade de arquivos ou outros objetos
`SeSecurityPrivilege`	`BUILTIN\Administrators`	Gerenciar a auditoria Isso inclui a visualização, o dumping e a limpeza do log de segurança.
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators` `BUILTIN\Backup Operators`,, `BUILTIN\Power Users` `BUILTIN\Users`,,, `Everyone`	Verificação da travessa de derivação Os usuários com esse privilégio não são obrigados a ter permissões de avanço (x) para percorrer pastas, links simbólicos ou junções.

Informações relacionadas

- Atribuir Privileges local
- Configuração da verificação transversal de derivação

Atribuir Privileges

Você pode atribuir Privileges diretamente a usuários locais ou usuários de domínio. Como alternativa, você pode atribuir usuários a grupos locais cujos Privileges atribuídos correspondem aos recursos que você deseja que esses usuários tenham.

- Você pode atribuir um conjunto de Privileges a um grupo que você criar.

  Em seguida, adicione um utilizador ao grupo que tem o Privileges que pretende que esse utilizador tenha.

- Você também pode atribuir usuários locais e usuários de domínio a grupos predefinidos cujo Privileges padrão corresponde ao Privileges que você deseja conceder a esses usuários.

Informações relacionadas

- Adicionando Privileges a usuários ou grupos locais ou de domínio
- Removendo Privileges de usuários ou grupos locais ou de domínio
- Redefinir o Privileges para usuários e grupos locais ou de domínio
- Configuração da verificação transversal de derivação

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Há certas diretrizes que você deve ter em mente quando você usa grupos BUILTIN e a conta de administrador local. Por exemplo, você pode renomear a conta de administrador local, mas não pode excluir essa conta.

- A conta de administrador pode ser renomeada, mas não pode ser excluída.
- A conta de administrador não pode ser removida do grupo BUILTIN/Administradores.
- Os grupos DE COMPILAÇÃO podem ser renomeados, mas não podem ser excluídos.

  Depois que o grupo BUILTIN é renomeado, outro objeto local pode ser criado com o nome conhecido; no entanto, o objeto recebe um novo RID.

- Não existe uma conta de convidado local.

Informações relacionadas

Grupos BUILTIN predefinidos e Privileges padrão

Requisitos para senhas de usuários locais

Por padrão, as senhas de usuário local devem atender aos requisitos de complexidade. Os requisitos de complexidade de senha são semelhantes aos requisitos definidos na política de segurança local do Microsoft Windows *diretiva de segurança*.

A senha deve atender aos seguintes critérios:

- Deve ter pelo menos seis carateres de comprimento

- Não deve conter o nome da conta de utilizador
- Deve conter carateres de pelo menos três das quatro categorias seguintes:
  - Carateres maiúsculos em inglês (A a Z)
  - Carateres minúsculos em inglês (a a z)
  - Base 10 dígitos (0 a 9)
  - Carateres especiais:

    i. ! ( ) [ ] : ; " ' > , . ? /

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Alterando senhas de contas de usuário locais

Grupos BUILTIN predefinidos e Privileges padrão

Você pode atribuir a associação de um usuário local ou usuário de domínio a um conjunto predefinido de grupos BUILTIN fornecidos pelo ONTAP. Grupos predefinidos têm Privileges predefinidos atribuídos.

A tabela a seguir descreve os grupos predefinidos:

Grupo BUILTIN predefinido	Privileges padrão
`BUILTIN\Administrators`LIVRAR-SE 544 Quando criada pela primeira vez, a conta local `Administrator`, com um RID de 500, é automaticamente feita um membro deste grupo. Quando a máquina virtual de storage (SVM) é unida a um domínio, o `domain\Domain Admins` grupo é adicionado ao grupo. Se o SVM sair do domínio, o `domain\Domain Admins` grupo será removido do grupo.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`LIVRAR-SE 547 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo têm as seguintes caraterísticas: • Pode criar e gerenciar usuários e grupos locais. • Não é possível adicionar a si mesmos ou qualquer outro objeto ao `BUILTIN\Administrators` grupo.	`SeChangeNotifyPrivilege`

Grupo BUILTIN predefinido	Privileges padrão
`BUILTIN\Backup Operators`LIVRAR-SE 551 Quando criado pela primeira vez, este grupo não tem nenhum membro. Os membros deste grupo podem substituir as permissões de leitura e gravação em arquivos ou pastas se forem abertos com intenção de backup.	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`LIVRAR-SE 545 Quando criado pela primeira vez, este grupo não tem nenhum membro (além do grupo especial implícito `Authenticated Users`). Quando o SVM é associado a um domínio, o `domain\Domain Users` grupo é adicionado a esse grupo. Se o SVM sair do domínio, o `domain\Domain Users` grupo será removido desse grupo.	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 Este grupo inclui todos os utilizadores, incluindo convidados (mas não utilizadores anónimos). Este é um grupo implícito com uma associação implícita.	`SeChangeNotifyPrivilege`

Informações relacionadas

Diretrizes para usar grupos BUILTIN e a conta de administrador local

Lista de Privileges suportados

Configuração da verificação transversal de derivação

Ativar ou desativar a funcionalidade de utilizadores e grupos locais

Ative ou desative a visão geral da funcionalidade de usuários e grupos locais

Antes de poder utilizar utilizadores e grupos locais para o controlo de acesso de dados de estilo de segurança NTFS, a funcionalidade de grupo e utilizador local tem de estar ativada. Além disso, se você quiser usar usuários locais para autenticação SMB, a funcionalidade de autenticação de usuário local deve estar ativada.

A funcionalidade de utilizadores e grupos locais e a autenticação de utilizadores locais são ativadas por predefinição. Se eles não estiverem ativados, você deverá ativá-los antes de configurar e usar usuários e grupos locais. Você pode desativar a funcionalidade de usuários e grupos locais a qualquer momento.

Além de desabilitar explicitamente a funcionalidade de usuário local e grupo, o ONTAP desabilita a funcionalidade de usuário local e grupo se qualquer nó no cluster for revertido para uma versão do ONTAP que não ofereça suporte à funcionalidade. A funcionalidade de usuário e grupo local não é ativada até que todos os nós do cluster estejam executando uma versão do ONTAP que o suporte.

Informações relacionadas

Modificar contas de usuário locais

Modificar grupos locais

Adicione Privileges a usuários ou grupos locais ou de domínio

Ative ou desative usuários e grupos locais

Você pode ativar ou desativar usuários locais e grupos para acesso SMB em máquinas virtuais de armazenamento (SVMs). A funcionalidade de utilizadores e grupos locais está ativada por predefinição.

Sobre esta tarefa

Você pode usar usuários e grupos locais ao configurar permissões de compartilhamento SMB e arquivos NTFS e pode, opcionalmente, usar usuários locais para autenticação ao criar uma conexão SMB. Para utilizar utilizadores locais para autenticação, também tem de ativar a opção de autenticação utilizadores locais e grupos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que os usuários e grupos locais sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a funcionalidade de usuários e grupos locais no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Ativar ou desativar a autenticação de utilizador local

Ativar ou desativar contas de utilizador locais

Ativar ou desativar a autenticação de utilizador local

Você pode ativar ou desativar a autenticação de usuário local para acesso SMB em máquinas virtuais de armazenamento (SVMs). O padrão é permitir a autenticação de usuário local, o que é útil quando o SVM não pode entrar em Contato com um controlador de domínio ou se você optar por não usar controles de acesso em nível de domínio.

Antes de começar

A funcionalidade de usuários e grupos locais deve estar ativada no servidor CIFS.

Sobre esta tarefa

Você pode ativar ou desativar a autenticação de usuário local a qualquer momento. Se você quiser usar usuários locais para autenticação ao criar uma conexão SMB, também deverá ativar a opção usuários e grupos locais do servidor CIFS.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que a autenticação local seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
Desativado	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a autenticação de usuário local no SVM VS1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Como funciona a autenticação de usuário local

Ativar ou desativar utilizadores e grupos locais

Gerenciar contas de usuários locais

Modificar contas de usuário locais

Você pode modificar uma conta de usuário local se quiser alterar o nome completo ou a descrição de um usuário existente e se quiser ativar ou desativar a conta de usuário. Você também pode renomear uma conta de usuário local se o nome do usuário estiver comprometido ou se uma alteração de nome for necessária para fins administrativos.

Se você quiser…	Digite o comando…
Modifique o nome completo do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` Se o nome completo contiver um espaço, ele deve ser incluído entre aspas duplas.
Modifique a descrição do usuário local	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Ative ou desative a conta de utilizador local	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is -account-disabled {true`
false}`	Renomeie a conta de usuário local

Exemplo

O exemplo a seguir renomeia o usuário local "'CIFS_SERVER'" para "'CIFS_Server' sue_new'" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

Ativar ou desativar contas de utilizador locais

Você ativa uma conta de usuário local se quiser que o usuário possa acessar os dados contidos na máquina virtual de armazenamento (SVM) em uma conexão SMB. Você também pode desativar uma conta de usuário local se não quiser que esse usuário acesse dados do SVM em SMB.

Sobre esta tarefa

Você ativa um usuário local modificando a conta de usuário.

Passo

1. Execute a ação apropriada:

Se você quiser…	Digite o comando…
Ative a conta de utilizador	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is-account -disabled false`
Desative a conta de usuário	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* `-user-name` *user_name* `-is-account -disabled true`

Altere as senhas da conta de usuário local

Pode alterar a palavra-passe da conta de um utilizador local. Isso pode ser útil se a senha do usuário for comprometida ou se o usuário tiver esquecido a senha.

Passo

1. Altere a senha executando a ação apropriada: `vserver cifs users-and-groups local-user set-password -vserver` *vserver_name* `-user-name` *user_name*

Exemplo

O exemplo a seguir define a senha do usuário local "'CIFS_Server'" associada à máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1:

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

Informações relacionadas

Ativar ou desativar a complexidade de senha necessária para usuários SMB locais

Exibindo informações sobre as configurações de segurança do servidor CIFS

Exibir informações sobre usuários locais

Você pode exibir uma lista de todos os usuários locais em um formulário de resumo. Se você quiser determinar quais configurações de conta estão configuradas para um usuário específico, você pode exibir informações detalhadas de conta para esse usuário, bem como as informações de conta para vários usuários. Essas informações podem ajudá-lo a determinar se você precisa modificar as configurações de um usuário e também solucionar problemas de autenticação ou acesso a arquivos.

Sobre esta tarefa

As informações sobre a palavra-passe de um utilizador nunca são apresentadas.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações sobre todos os usuários na máquina virtual de storage (SVM)	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
Exibir informações detalhadas da conta para um usuário	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

Há outros parâmetros opcionais que você pode escolher quando você executa o comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os usuários locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- --------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones
```

Exibir informações sobre associações de grupos para usuários locais

Você pode exibir informações sobre os grupos locais aos quais um usuário local pertence. Você pode usar essas informações para determinar qual acesso o usuário deve ter aos arquivos e pastas. Essas informações podem ser úteis para determinar quais direitos de acesso o usuário deve ter a arquivos e pastas ou ao solucionar problemas de acesso ao arquivo.

Sobre esta tarefa

Você pode personalizar o comando para exibir apenas as informações que deseja ver.

Passo

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Exibir informações de associação de usuário local para um usuário local especificado	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
Exibir informações de associação de usuários locais para o grupo local do qual esse usuário local é membro	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
Exibir informações de associação de usuários para usuários locais associados a uma máquina virtual de armazenamento (SVM) especificada	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
Exibir informações detalhadas de todos os usuários locais em um SVM especificado	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe as informações de associação para todos os usuários locais no SVM VS1; o usuário "CIFS_SERVER" é membro do grupo "BUILTIN" Administradores, e "'CIFS_Server'" é membro do grupo "'CIFS_Server' G1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

Eliminar contas de utilizador locais

Você pode excluir contas de usuários locais da máquina virtual de storage (SVM) se elas não forem mais necessárias para a autenticação SMB local para o servidor CIFS ou para determinar os direitos de acesso aos dados contidos no SVM.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir usuários locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse usuário não são ajustados.

- Todas as referências a usuários locais são removidas dos bancos de dados de associação e Privileges.
- Usuários padrão e bem conhecidos, como Administrador, não podem ser excluídos.

Passos

1. Determine o nome da conta de usuário local que você deseja excluir: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. Eliminar o utilizador local: `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. Verifique se a conta de usuário foi excluída: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exclui o usuário local "'CIFS_Server'" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

Gerenciar grupos locais

Modificar grupos locais

Você pode modificar grupos locais existentes alterando a descrição de um grupo local existente ou renomeando o grupo.

Se você quiser…	Use o comando…
Modifique a descrição do grupo local	`vserver cifs users-and-groups local-group modify -vserver` *vserver_name* `-group-name` *group_name* `-description text` Se a descrição contém um espaço, então ele deve ser fechado dentro de aspas duplas.
Renomeie o grupo local	`vserver cifs users-and-groups local-group rename -vserver` *vserver_name* `-group-name` *group_name* `-new-group-name` *new_group_name*

Exemplos

O exemplo a seguir renomeia o grupo local "'CIFS_SERVER' Engineering" para "'CIFS_Server' Engineering_new'":

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

O exemplo a seguir modifica a descrição do grupo local "'CIFS_SERVER' Engineering":

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

Exibir informações sobre grupos locais

É possível exibir uma lista de todos os grupos locais configurados no cluster ou em uma máquina virtual de armazenamento (SVM) especificada. Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos para dados contidos no SVM ou problemas de direitos de usuário (privilégios) no SVM.

Passo

1. Execute uma das seguintes ações:

Se você quiser informações sobre…	Digite o comando…
Todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show`
Todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

   Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O exemplo a seguir exibe informações sobre todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

Gerenciar a associação ao grupo local

Você pode gerenciar a associação de grupo local adicionando e removendo usuários locais ou de domínio ou adicionando e removendo grupos de domínio. Isso é útil se você quiser controlar o acesso a dados com base nos controles de acesso colocados no grupo ou se quiser que os usuários tenham o Privileges associado a esse grupo.

Sobre esta tarefa

Diretrizes para adicionar membros a um grupo local:

- Você não pode adicionar usuários ao grupo especial *todos*.
- O grupo local deve existir antes de poder adicionar um utilizador a ele.
- O utilizador tem de existir antes de poder adicionar o utilizador a um grupo local.
- Não é possível adicionar um grupo local a outro grupo local.
- Para adicionar um usuário ou grupo de domínio a um grupo local, o Data ONTAP deve ser capaz de resolver o nome para um SID.

Diretrizes para remover membros de um grupo local:

- Você não pode remover membros do grupo especial *todos*.
- O grupo do qual você deseja remover um membro deve existir.
- O ONTAP deve ser capaz de resolver os nomes dos membros que você deseja remover do grupo para um SID correspondente.

Passo

1. Adicione ou remova um membro em um grupo.

Se você quiser…	Em seguida, use o comando…
Adicione um membro a um grupo	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio para adicionar ao grupo local especificado.
Remova um membro de um grupo	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` Você pode especificar uma lista delimitada por vírgulas de usuários locais, usuários de domínio ou grupos de domínio a serem removidos do grupo local especificado.

O exemplo a seguir adiciona um usuário local "'SMB_SERVER'" e um grupo de domínio "'AD_Dom_eng'" ao grupo local "'SMB_SERVER' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

O exemplo a seguir remove os usuários locais "'SMB_SERVER'" e "'SMB_SERVER' james' do grupo local

"'SMB_Server' Engineering" no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informações relacionadas

Exibindo informações sobre membros de grupos locais

Exibir informações sobre membros de grupos locais

É possível exibir uma lista de todos os membros de grupos locais configurados no cluster ou em uma máquina virtual de armazenamento especificada (SVM). Essas informações podem ser úteis ao solucionar problemas de acesso a arquivos ou problemas de direitos de usuário (privilégios).

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite o comando…
Membros de todos os grupos locais no cluster	`vserver cifs users-and-groups local-group show-members`
Membros de todos os grupos locais no SVM	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações sobre membros de todos os grupos locais no SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

Eliminar um grupo local

Você poderá excluir um grupo local da máquina virtual de storage (SVM) se não for mais necessário para determinar direitos de acesso a dados associados a esse SVM ou se não for mais necessário atribuir direitos de usuário (Privileges) a membros do grupo.

Sobre esta tarefa

Tenha em mente o seguinte ao excluir grupos locais:

- O sistema de ficheiros não foi alterado.

  Os descritores de segurança do Windows em arquivos e diretórios que se referem a esse grupo não são ajustados.

- Se o grupo não existir, um erro será retornado.
- O grupo especial *todos* não pode ser excluído.
- Grupos internos, como *BUILTIN__BUILTIN/Users*, não podem ser excluídos.

Passos

1. Determine o nome do grupo local que você deseja excluir exibindo a lista de grupos locais no SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminar o grupo local: `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. Verifique se o grupo foi excluído: `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exclui o grupo local "CIFS_SERVER" associado ao SVM VS1:

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ---------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

Atualizar nomes de usuários e grupos de domínio em bancos de dados locais

Você pode adicionar usuários e grupos de domínio aos grupos locais de um servidor CIFS. Esses objetos de domínio são registrados em bancos de dados locais no cluster. Se um objeto de domínio for renomeado, os bancos de dados locais devem ser atualizados manualmente.

Sobre esta tarefa

Você deve especificar o nome da máquina virtual de armazenamento (SVM) na qual deseja atualizar nomes de domínio.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute a ação apropriada:

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito e que falharam na atualização	`vserver cifs users-and-groups update-names -vserver` *vserver_name*

Se você quiser atualizar usuários e grupos de domínio e…	Use este comando…
Exibir usuários e grupos de domínio que foram atualizados com êxito	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
Exiba apenas os usuários e grupos de domínio que não conseguem atualizar	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
Suprimir todas as informações de status sobre atualizações	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir atualiza os nomes de usuários e grupos de domínio associados à máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Para a última atualização, há uma cadeia de nomes dependente que precisa ser atualizada:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

Gerenciar Privileges local

Adicione Privileges a usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio adicionando o Privileges. O Privileges adicionado substitui o Privileges padrão atribuído a qualquer um desses objetos. Isso fornece segurança aprimorada, permitindo que você personalize o que o Privileges um usuário ou grupo tem.

Antes de começar

O usuário ou grupo local ou domínio ao qual o Privileges será adicionado já deve existir.

Sobre esta tarefa

Adicionar um privilégio a um objeto substitui o Privileges padrão para esse usuário ou grupo. Adicionar um privilégio não remove Privileges adicionados anteriormente.

Você deve ter em mente o seguinte ao adicionar o Privileges a usuários ou grupos locais ou de domínio:

- Você pode adicionar um ou mais Privileges.
- Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Adicione um ou mais Privileges a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados são aplicados ao objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir adiciona o "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do Privileges ao usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

Remova o Privileges de usuários ou grupos locais ou de domínio

Você pode gerenciar os direitos de usuário para usuários ou grupos locais ou de domínio removendo o Privileges. Isso fornece segurança aprimorada, permitindo que você

personalize o Privileges máximo que os usuários e grupos têm.

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Você deve ter em mente o seguinte ao remover o Privileges de usuários ou grupos locais ou de domínio:

- Você pode remover um ou mais Privileges.
- Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio.

  O comando pode falhar se o ONTAP não conseguir entrar em Contato com o controlador de domínio.

Passos

1. Remova um ou mais Privileges de um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group -name _name_ -privileges _privilege_[,...]`
2. Verifique se os Privileges desejados foram removidos do objeto: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O exemplo a seguir remove o Privileges "SeTcbPrivilege" e o "SeTakeOwnershipPrivilege" do usuário ""SERVIDOR_Sue"" na máquina virtual de armazenamento (SVM, anteriormente conhecida como CIFS) VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

Redefinir o Privileges para usuários e grupos locais ou de domínio

Você pode redefinir o Privileges para usuários e grupos locais ou de domínio. Isso pode ser útil quando você fez modificações no Privileges para um usuário ou grupo local ou de domínio e essas modificações não são mais desejadas ou necessárias.

Sobre esta tarefa

A redefinição do Privileges para um usuário ou grupo local ou de domínio remove quaisquer entradas de privilégio para esse objeto.

Passos

1. Redefina o Privileges em um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verifique se os Privileges são redefinidos no objeto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Exemplos

O exemplo a seguir redefine o Privileges no usuário "CIFS_SERVER" na máquina virtual de armazenamento (SVM, anteriormente conhecida como SVM) VS1. Por padrão, os usuários normais não têm o Privileges associado às suas contas:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

O exemplo a seguir redefine o Privileges para o grupo "Administradores", removendo efetivamente a entrada de privilégio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- ------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Exibir informações sobre substituições de privilégios

Você pode exibir informações sobre Privileges personalizados atribuídos a grupos ou

contas de usuário locais ou de domínio. Essas informações ajudam a determinar se os direitos de usuário desejados são aplicados.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações sobre…	Digite este comando…
Privileges personalizado para todos os usuários e grupos de domínio e locais na máquina virtual de storage (SVM)	`vserver cifs users-and-groups privilege show -vserver vserver_name`
Privileges personalizado para um domínio específico ou usuário local e grupo no SVM	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

Há outros parâmetros opcionais que você pode escolher quando você executar este comando. Consulte a página de manual para obter mais informações.

Exemplo

O comando a seguir exibe todos os Privileges explicitamente associados a usuários e grupos locais ou de domínio para o SVM VS1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configure a verificação de desvio transversal

Configure a visão geral da verificação da travessia de derivação

A verificação de desvio transversal é um direito de usuário (também conhecido como *privilégio*) que determina se um usuário pode percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões no diretório atravessado. Você deve entender o que acontece ao permitir ou desativar a verificação de desvio transversal e como configurar a verificação de desvio transversal para usuários em máquinas virtuais de armazenamento (SVMs).

O que acontece ao permitir ou ao desativar a verificação transversal de desvio

- Se permitido, quando um usuário tenta acessar um arquivo, o ONTAP não verifica a permissão de avanço para os diretórios intermediários ao determinar se deve conceder ou negar acesso ao arquivo.
- Se não for permitido, o ONTAP verifica a permissão de avanço (execução) para todos os diretórios no

caminho para o arquivo.

Se qualquer um dos diretórios intermediários não tiver o "X" (permissão de avanço), o ONTAP nega o acesso ao arquivo.

Configure a verificação de desvio transversal

Você pode configurar a verificação de desvio transversal usando a CLI do ONTAP ou configurando políticas de grupo do ative Directory com esse direito de usuário.

O `SeChangeNotifyPrivilege` privilégio controla se os usuários têm permissão para ignorar a verificação transversal.

- Adicioná-lo a usuários ou grupos SMB locais na SVM ou a usuários ou grupos de domínio permite a verificação de desvio transversal.
- Removê-lo de usuários ou grupos SMB locais no SVM ou de usuários ou grupos de domínio não permite a verificação de desvio transversal.

Por padrão, os seguintes grupos BUILTIN no SVM têm o direito de ignorar a verificação transversal:

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

Se você não quiser permitir que membros de um desses grupos ignorem a verificação transversal, você deve remover esse privilégio do grupo.

Você deve ter em mente o seguinte ao configurar a verificação de desvio transversal para usuários e grupos SMB locais no SVM usando a CLI:

- Se você quiser permitir que membros de um grupo de domínio ou local personalizado ignorem a verificação transversal, você deve adicionar o `SeChangeNotifyPrivilege` privilégio a esse grupo.
- Se você quiser permitir que um usuário local ou de domínio individual ignore a verificação transversal e que o usuário não seja membro de um grupo com esse privilégio, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a essa conta de usuário.
- Você pode desativar a verificação de desvio transversal para usuários ou grupos locais ou de domínio removendo o `SeChangeNotifyPrivilege` privilégio a qualquer momento.

> Para desativar a verificação de desvio de travers para usuários ou grupos locais ou de domínio especificados, você também deve remover o `SeChangeNotifyPrivilege` privilégio do `Everyone` grupo.

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Criar listas de controle de acesso de compartilhamento SMB

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Lista de Privileges suportados

Adicione Privileges a usuários ou grupos locais ou de domínio

Permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você quiser que um usuário possa percorrer todos os diretórios no caminho para um arquivo, mesmo que o usuário não tenha permissões em um diretório atravessado, você pode adicionar o `SeChangeNotifyPrivilege` privilégio a usuários ou grupos SMB locais em máquinas virtuais de armazenamento (SVMs). Por padrão, os usuários são capazes de ignorar a verificação de rotação do diretório.

Antes de começar

- Um servidor SMB deve estar presente na SVM.
- A opção local Users and Groups SMB Server (usuários locais e grupos) deve estar ativada.
- O usuário ou grupo local ou domínio ao qual o `SeChangeNotifyPrivilege` privilégio será adicionado já deve existir.

Sobre esta tarefa

Ao adicionar Privileges a um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio contatando o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Ative a verificação de desvio transversal adicionando o `SeChangeNotifyPrivilege` privilégio a um usuário ou grupo local ou de domínio: `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O valor para o `-user-or-group-name` parâmetro é um usuário ou grupo local, ou um usuário ou grupo de domínio.

2. Verifique se o usuário ou grupo especificado tem a verificação transversal de desvio ativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir permite que os usuários que pertencem ao grupo "'EXAMPLE'" ignorem a verificação da rotação do diretório adicionando o `SeChangeNotifyPrivilege` privilégio ao grupo:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

Informações relacionadas

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Não permitir que usuários ou grupos ignorem a verificação da rotação do diretório

Se você não quiser que um usuário percorra todos os diretórios no caminho para um arquivo porque o usuário não tem permissões no diretório atravessado, você pode remover o `SeChangeNotifyPrivilege` privilégio de usuários SMB locais ou grupos em máquinas virtuais de armazenamento (SVMs).

Antes de começar

O usuário ou grupo local ou domínio do qual o Privileges será removido já deve existir.

Sobre esta tarefa

Ao remover o Privileges de um usuário ou grupo de domínio, o ONTAP pode validar o usuário ou grupo de domínio entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Não permitir a verificação da travessa de derivação: `vserver cifs users-and-groups privilege remove-privilege -vserver` *`vserver_name`* `-user-or-group-name` *`name`* `-privileges SeChangeNotifyPrivilege`

   O comando remove o `SeChangeNotifyPrivilege` privilégio do usuário ou grupo local ou domínio que você especificar com o valor do `-user-or-group-name` *`name`* parâmetro.

2. Verifique se o usuário ou grupo especificado tem verificação de desvio de rotação desativada: `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

Exemplo

O comando a seguir despermite que os usuários que pertencem ao grupo "'EXAMPLE"' ignorem a verificação da rotação do diretório:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ----------------------
vs1       EXAMPLE\eng           -
```

Informações relacionadas

Permitir que usuários ou grupos ignorem a verificação de rotação do diretório

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Exibir informações sobre a visão geral das políticas de auditoria e segurança de arquivos

Você pode exibir informações sobre segurança de arquivos em arquivos e diretórios contidos em volumes em máquinas virtuais de armazenamento (SVMs). Você pode exibir informações sobre políticas de auditoria no FlexVol volumes. Se configurado, você pode exibir informações sobre as configurações de segurança do Guarda de Acesso em nível de armazenamento e Controle Dinâmico de Acesso no FlexVol volumes.

Exibindo informações sobre segurança de arquivos

Você pode exibir informações sobre a segurança de arquivos aplicada a dados contidos em volumes e qtrees (para volumes FlexVol) com os seguintes estilos de segurança:

- NTFS
- UNIX
- Misto

Exibindo informações sobre políticas de auditoria

Você pode exibir informações sobre políticas de auditoria para auditar eventos de acesso em volumes do FlexVol nos seguintes protocolos nas:

- SMB (todas as versões)
- NFSv4.x

Exibindo informações sobre a segurança do Storage-Level Access Guard (SLAG)

A segurança do Access Guard no nível de storage pode ser aplicada em volumes e objetos de qtree do FlexVol com os seguintes estilos de segurança:

- NTFS
- Misto
- UNIX (se um servidor CIFS estiver configurado na SVM que contém o volume)

Apresentar informações sobre a segurança do controlo de acesso dinâmico (DAC)

A segurança do controle de acesso dinâmico pode ser aplicada em um objeto dentro de um FlexVol volume com os seguintes estilos de segurança:

- NTFS
- Misto (se o objeto tiver segurança efetiva NTFS)

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Exibindo informações sobre o Storage-Level Access Guard

Exibir informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Você pode exibir informações sobre a segurança de arquivos e diretórios em volumes de estilo de segurança NTFS, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre os atributos dos. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Como os volumes e qtrees de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.
- A saída ACL é exibida para arquivos e pastas com segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada na raiz de volume ou qtree, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir ACLs de arquivo regulares e ACLs de Storage-Level Access Guard.
- A saída também exibe informações sobre os ACEs do Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório específico.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Se você quiser exibir informações…	Digite o seguinte comando…
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/vol4` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança com máscaras expandidas sobre o caminho `/data/engineering` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

               Vserver: vs1
             File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
```

```
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
                             .... ...0 .... .... .... .... .... .... =
System Security
```

```
                           .... .... ...1 .... .... .... .... .... =
Synchronize
                           .... .... .... 1... .... .... .... .... =
Write Owner
                           .... .... .... .1.. .... .... .... .... =
Write DAC
                           .... .... .... ..1. .... .... .... .... =
Read Control
                           .... .... .... ...1 .... .... .... .... =
Delete
                           .... .... .... .... .... ...1 .... .... =
Write Attributes
                           .... .... .... .... .... .... 1... .... =
Read Attributes
                           .... .... .... .... .... .... .1.. .... =
Delete Child
                           .... .... .... .... .... .... ..1. .... =
Execute
                           .... .... .... .... .... .... ...1 .... =
Write EA
                           .... .... .... .... .... .... .... 1... =
Read EA
                           .... .... .... .... .... .... .... .1.. =
Append
                           .... .... .... .... .... .... .... ..1. =
Write
                           .... .... .... .... .... .... .... ...1 =
Read

                         ALLOW-Everyone-0x10000000-OI|CI|IO
                           0... .... .... .... .... .... .... .... =
Generic Read
                           .0.. .... .... .... .... .... .... .... =
Generic Write
                           ..0. .... .... .... .... .... .... .... =
Generic Execute
                           ...1 .... .... .... .... .... .... .... =
Generic All
                           .... ...0 .... .... .... .... .... .... =
System Security
                           .... .... ...0 .... .... .... .... .... =
Synchronize
                           .... .... .... 0... .... .... .... .... =
Write Owner
                           .... .... .... .0.. .... .... .... .... =
Write DAC
```

```
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

O exemplo a seguir exibe informações de segurança, incluindo informações de segurança do Storage-Level Access Guard, para o volume com o caminho `/datavol1` no SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes mistos de estilo de segurança, incluindo o estilo de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou pasta você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.
- O nível superior de um volume de estilo de segurança misto pode ter segurança eficaz UNIX ou NTFS.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto as permissões de arquivo UNIX quanto as ACLs Storage-Level Access Guard.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho de arquivo ou diretório dado.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/projects` no SVM VS1 no formulário de máscara expandida. Este caminho de estilo de segurança misto tem segurança eficaz UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

               Vserver: vs1
             File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/data` no SVM VS1. Este caminho misto de estilo de segurança tem uma segurança eficaz NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

O exemplo a seguir exibe as informações de segurança sobre o volume no caminho `/datavol5` no SVM VS1. O nível superior deste volume misto de estilo de segurança tem segurança eficaz UNIX. O volume tem segurança Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Exibir informações sobre segurança de arquivos em volumes estilo de segurança UNIX

Você pode exibir informações sobre segurança de arquivos e diretórios em volumes estilo de segurança UNIX, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre proprietários e

grupos UNIX. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de acesso a arquivos.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os dados cujas informações de segurança de arquivo ou diretório você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 ao determinar direitos de acesso a arquivos.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NFSv4.

  Este campo está vazio para arquivos e diretórios que usam segurança UNIX que têm somente permissões de bit de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída de proprietário e grupo na saída ACL não se aplicam no caso de descritores de segurança NFSv4.

  Eles são apenas significativos para descritores de segurança NTFS.

- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passo

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
Com detalhes expandidos	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

O exemplo a seguir exibe as informações de segurança sobre o caminho `/home` no SVM VS1 no formulário de máscara expandida:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                           Unix User Id: 0
                          Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

Informações relacionadas

Exibindo informações sobre segurança de arquivos em volumes de estilo de segurança NTFS

Exibindo informações sobre segurança de arquivos em volumes mistos de estilo de segurança

Exibir informações sobre políticas de auditoria NTFS em volumes FlexVol usando a CLI

Você pode exibir informações sobre políticas de auditoria NTFS no FlexVol volumes, incluindo quais são os estilos de segurança e estilos de segurança eficazes, quais permissões são aplicadas e informações sobre listas de controle de acesso do sistema. Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou pastas cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança NTFS usam apenas as listas de controle de acesso do sistema NTFS (SACLs) para políticas de auditoria.
- Arquivos e pastas em um volume misto de estilo de segurança com segurança efetiva NTFS podem ter políticas de auditoria NTFS aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard está configurado pode exibir tanto o arquivo normal quanto a pasta NFSv4 SACLs e o Storage-Level Access Guard NTFS SACLs.
- Se o caminho inserido no comando for para dados com segurança efetiva NTFS, a saída também exibirá informações sobre ACEs de Controle de Acesso Dinâmico se o Controle de Acesso Dinâmico estiver configurado para o caminho do arquivo ou diretório fornecido.
- Ao exibir informações de segurança sobre arquivos e pastas com segurança efetiva NTFS, os campos de saída relacionados ao UNIX contêm informações de permissão de arquivo UNIX somente para exibição.

  Arquivos e pastas de estilo de segurança NTFS usam apenas permissões de arquivo NTFS e usuários e grupos do Windows ao determinar direitos de acesso a arquivos.

- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.

Passo

1. Exiba as configurações de diretiva de auditoria de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Como uma lista detalhada	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações da política de auditoria do caminho `/corp` no SVM VS1. O caminho tem segurança eficaz NTFS. O descritor de segurança NTFS contém uma entrada SACL DE sucesso e uma entrada de sucesso/FALHA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

O exemplo a seguir exibe as informações da política de auditoria do caminho `/datavol1` no SVM VS1. O caminho contém SACLs de arquivo e pasta regulares e SACLs de proteção de acesso em nível de armazenamento.

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Exiba informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI

Você pode exibir informações sobre as políticas de auditoria do NFSv4 em volumes do FlexVol usando a CLI do ONTAP, incluindo quais são os estilos de segurança e estilos de

segurança eficazes, quais permissões são aplicadas e informações sobre as listas de controle de acesso do sistema (SACLs). Você pode usar os resultados para validar sua configuração de segurança ou para solucionar problemas de auditoria.

Sobre esta tarefa

Você deve fornecer o nome da máquina virtual de armazenamento (SVM) e o caminho para os arquivos ou diretórios cujas informações de auditoria você deseja exibir. Você pode exibir a saída em forma de resumo ou como uma lista detalhada.

- Os volumes e qtrees de estilo de segurança UNIX usam apenas SACLs NFSv4 para políticas de auditoria.
- Arquivos e diretórios em um volume misto de estilo de segurança que são de estilo de segurança UNIX podem ter políticas de auditoria NFSv4 aplicadas a eles.

  Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e diretórios que usam permissões de arquivo UNIX, bits de modo ou ACLs NFSv4 e alguns arquivos e diretórios que usam permissões de arquivo NTFS.

- O nível superior de um volume de estilo de segurança misto pode ter segurança efetiva UNIX ou NTFS e pode ou não conter SACLs NFSv4.
- A saída ACL é exibida apenas para arquivos e pastas com segurança NTFS ou NFSv4.

  Este campo está vazio para arquivos e pastas que usam segurança UNIX que têm apenas permissões de bits de modo aplicadas (sem ACLs NFSv4).

- Os campos de saída do proprietário e do grupo na saída da ACL aplicam-se apenas no caso de descritores de segurança NTFS.
- Como a segurança do Storage-Level Access Guard pode ser configurada em um volume ou qtree misto de estilo de segurança, mesmo que o estilo de segurança efetivo da raiz de volume ou qtree seja UNIX, a saída para um caminho de volume ou qtree em que o Storage-Level Access Guard esteja configurado pode exibir tanto SACLs de arquivo NFSv4 regulares como de diretório e SACLs de acesso no nível de armazenamento NTFS SACLs.
- Como a segurança do Storage-Level Access Guard é suportada em um volume ou qtree UNIX se um servidor CIFS estiver configurado no SVM, a saída pode conter informações sobre a segurança do Storage-Level Access Guard aplicada ao volume ou qtree especificado no `-path` parâmetro.

Passos

1. Exiba as configurações de segurança de arquivo e diretório com o nível de detalhes desejado:

Se você quiser exibir informações…	Digite o seguinte comando…
Em forma de resumo	`vserver security file-directory show -vserver vserver_name -path path`
Com detalhes expandidos	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

Exemplos

O exemplo a seguir exibe as informações de segurança sobre o caminho `/lab` no SVM VS1. Este caminho de

estilo de segurança UNIX tem um SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

Maneiras de exibir informações sobre segurança de arquivos e diretivas de auditoria

Você pode usar o caractere curinga (*) para exibir informações sobre segurança de arquivos e políticas de auditoria de todos os arquivos e diretórios em um determinado caminho ou volume raiz.

O caractere curinga (**) pode ser usado como o último subcomponente de um determinado caminho de diretório abaixo do qual você deseja exibir informações de todos os arquivos e diretórios. Se você quiser exibir informações de um arquivo ou diretório específico chamado "*"**, então você precisa fornecer o caminho completo dentro de aspas duplas ("*").

Exemplo

O comando a seguir com o caractere curinga exibe as informações sobre todos os arquivos e diretórios abaixo do caminho `/1/` do SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

O comando a seguir exibe as informações de um arquivo chamado "*" no caminho `/vol1/a` do SVM VS1. O caminho está entre aspas duplas (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: “/vol1/a/*”
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 1002
          Unix Group Id: 65533
         Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                    ACLs: NFSV4 Security Descriptor
                          Control:0x8014
                          SACL - ACEs
                            AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                          DACL - ACEs
                            ALLOW-EVERYONE@-0x1f00a9-FI|DI
                            ALLOW-OWNER@-0x1f01ff-FI|DI
                            ALLOW-GROUP@-0x1200a9-IG
```

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a CLI

Gerencie a segurança de arquivos NTFS, as políticas de auditoria NTFS e o Storage-Level Access Guard em SVMs usando a visão geral da CLI

Você pode gerenciar a segurança de arquivos NTFS, políticas de auditoria NTFS e o Storage-Level Access Guard em máquinas virtuais de armazenamento (SVMs) usando a CLI.

Você pode gerenciar políticas de segurança e auditoria de arquivos NTFS de clientes SMB ou usando a CLI. No entanto, usar a CLI para configurar políticas de segurança e auditoria de arquivos remove a necessidade de usar um cliente remoto para gerenciar a segurança de arquivos. Usar a CLI pode reduzir significativamente o tempo necessário para aplicar a segurança em muitos arquivos e pastas usando um único comando.

Você pode configurar o Storage-Level Access Guard, que é outra camada de segurança aplicada pelo ONTAP aos volumes SVM. O Storage-Level Access Guard aplica-se a acessos de todos os protocolos nas ao objeto de armazenamento ao qual o Storage-Level Access Guard é aplicado.

O protetor de acesso no nível de storage pode ser configurado e gerenciado somente a partir da CLI do ONTAP. Não é possível gerenciar as configurações do protetor de acesso em nível de armazenamento de clientes SMB. Além disso, se você exibir as configurações de segurança em um arquivo ou diretório de um cliente NFS ou SMB, não verá a segurança Storage-Level Access Guard. A segurança do Access Guard no nível de armazenamento não pode ser revogada de um cliente, mesmo por um administrador do sistema (Windows ou UNIX). Portanto, o Storage-Level Access Guard fornece uma camada extra de segurança para o acesso aos dados que é definido e gerenciado de forma independente pelo administrador do armazenamento.

Embora apenas as permissões de acesso NTFS sejam suportadas pelo Guarda de Acesso em nível de armazenamento, o ONTAP pode executar verificações de segurança para acesso através de NFS a dados em volumes em que o Guarda de Acesso em nível de armazenamento é aplicado se o utilizador do UNIX mapear para um utilizador do Windows na SVM que possui o volume.

Volumes de estilo de segurança NTFS

Todos os arquivos e pastas contidos em volumes e qtrees de estilo de segurança NTFS têm segurança efetiva NTFS. Você pode usar a `vserver security file-directory` família de comandos para implementar os seguintes tipos de segurança em volumes de estilo de segurança NTFS:

- Permissões de arquivo e políticas de auditoria para arquivos e pastas contidos no volume
- Segurança no nível de armazenamento de acesso Guarda em volumes

Volumes mistos de estilo de segurança

Volumes mistos de estilo de segurança e qtrees podem conter alguns arquivos e pastas que têm segurança efetiva UNIX e usam permissões de arquivos UNIX, bits de modo ou ACLs NFSv4.x e diretivas de auditoria NFSv4.x, e alguns arquivos e pastas que têm segurança efetiva NTFS e usam permissões de arquivos NTFS e políticas de auditoria. Você pode usar a `vserver security file-directory` família de comandos para aplicar os seguintes tipos de segurança a dados mistos de estilo de segurança:

- Permissões de arquivos e diretivas de auditoria para arquivos e pastas com o estilo de segurança eficaz NTFS no volume ou qtree misto
- Proteção de acesso no nível de armazenamento para volumes com o estilo de segurança eficaz NTFS e UNIX

Volumes de estilo de segurança UNIX

Os volumes e qtrees de estilo de segurança UNIX contêm arquivos e pastas que têm segurança efetiva UNIX (bits de modo ou ACLs NFSv4.x). Você deve ter em mente o seguinte se quiser usar a `vserver security file-directory` família de comandos para implementar a segurança em volumes estilo de segurança UNIX:

- A `vserver security file-directory` família de comandos não pode ser usada para gerenciar políticas de segurança e auditoria de arquivos UNIX em volumes e qtrees de estilo de segurança UNIX.
- Você pode usar a `vserver security file-directory` família de comandos para configurar o Storage-Level Access Guard em volumes de estilo de segurança UNIX, desde que o SVM com o volume de destino contenha um servidor CIFS.

Informações relacionadas

Exibir informações sobre segurança de arquivos e diretivas de auditoria

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Proteja o acesso aos arquivos usando o Storage-Level Access Guard

Use casos para usar a CLI para definir a segurança de arquivos e pastas

Como você pode aplicar e gerenciar a segurança de arquivos e pastas localmente sem envolvimento de um cliente remoto, você pode reduzir significativamente o tempo necessário para definir a segurança em massa em um grande número de arquivos ou pastas.

Você pode se beneficiar do uso da CLI para definir a segurança de arquivos e pastas nos seguintes casos de uso:

- Armazenamento de arquivos em grandes ambientes empresariais, como armazenamento de arquivos em diretórios base
- Migração de dados
- Mudança de domínio do Windows
- Padronização de políticas de segurança e auditoria de arquivos em sistemas de arquivos NTFS

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Você precisa estar ciente de certos limites ao usar a CLI para definir a segurança de arquivos e pastas.

- A `vserver security file-directory` família de comandos não suporta a configuração de ACLs NFSv4.

  Você só pode aplicar descritores de segurança NTFS a arquivos e pastas NTFS.

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

Os descritores de segurança contêm as listas de controle de acesso que determinam quais ações um usuário pode executar em arquivos e pastas e o que é auditado quando um usuário acessa arquivos e pastas.

- **Permissões**

  As permissões são permitidas ou negadas pelo proprietário de um objeto e determinam quais ações um objeto (usuários, grupos ou objetos de computador) pode executar em arquivos ou pastas especificados.

- **Descritores de segurança**

  Descritores de segurança são estruturas de dados que contêm informações de segurança que definem permissões associadas a um arquivo ou pasta.

- **Listas de controle de acesso (ACLs)**

  Listas de controle de acesso são as listas contidas em um descritor de segurança que contêm informações sobre quais ações os usuários, grupos ou objetos de computador podem executar no arquivo ou pasta à qual o descritor de segurança é aplicado. O descritor de segurança pode conter os dois tipos de ACLs a seguir:

  - Listas de controle de acesso discricionárias (DACLs)
  - Listas de controle de acesso do sistema (SACLs)

- **Listas de controle de acesso discricionárias (DACLs)**

  As DACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador que têm acesso permitido ou negado para executar ações em arquivos ou pastas. As DACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Listas de controle de acesso do sistema (SACLs)**

  Os SACLs contêm a lista de SIDS para os usuários, grupos e objetos de computador para os quais eventos de auditoria bem-sucedidos ou com falha são registrados. SACLs contêm zero ou mais entradas de controle de acesso (ACEs).

- **Entradas de Controle de Acesso (ACEs)**

  Os ases são entradas individuais em DACLs ou SACLs:

  - Uma entrada de controle de acesso DACL especifica os direitos de acesso que são permitidos ou negados para usuários, grupos ou objetos de computador específicos.
  - Uma entrada de controle de acesso SACL especifica os eventos de sucesso ou falha a serem registrados ao auditar ações especificadas executadas por determinados usuários, grupos ou objetos de computador.

- * Herança de permissão*

  A herança de permissões descreve como as permissões definidas em descritores de segurança são propagadas para um objeto de um objeto pai. Somente permissões herdáveis são herdadas por objetos filho. Ao definir permissões no objeto pai, você pode decidir se pastas, subpastas e arquivos podem herdá-los com ""aplicar a `this-folder`, `sub-folders` e 'arquivos"".

Informações relacionadas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configurando e aplicando políticas de auditoria a arquivos e pastas NTFS usando a CLI

Diretrizes para a aplicação de políticas de diretório de arquivos que usam usuários locais ou grupos no destino da recuperação de desastres do SVM

Há certas diretrizes que você deve ter em mente antes de aplicar políticas de diretório de arquivos no destino de recuperação de desastres de máquina virtual de armazenamento (SVM) em uma configuração de descarte de ID se a configuração de diretiva de diretório de arquivos usar usuários locais ou grupos no descritor de segurança ou nas entradas DACL ou SACL.

Você pode configurar uma configuração de recuperação de desastre para um SVM em que o SVM de origem no cluster de origem replique os dados e a configuração da SVM de origem a um SVM de destino em um cluster de destino.

É possível configurar um dos dois tipos de recuperação de desastres da SVM:

- Identidade preservada

  Com essa configuração, a identidade do SVM e do servidor CIFS é preservada.

- Identidade descartada

  Com essa configuração, a identidade do SVM e do servidor CIFS não é preservada. Nesse cenário, o nome do SVM e do servidor CIFS no SVM de destino são diferentes do SVM e do nome do servidor CIFS na SVM de origem.

Diretrizes para configurações de identidade descartadas

Em uma configuração de identidade descartada, para uma origem SVM que contenha configurações de usuário, grupo e privilégio locais, o nome do domínio local (nome do servidor CIFS local) deve ser alterado para corresponder ao nome do servidor CIFS no destino SVM. Por exemplo, se o nome do SVM de origem for "'VS1'" e o nome do servidor CIFS for "'CIFS1 user1'", e o nome do SVM de destino for "'VS1 user1_dst'" e o nome do servidor CIFS for "'CIFS1_DST'", então o nome de domínio local para um usuário local chamado "'CIFS1'" é alterado automaticamente para "'CIFS1_DST'" no destino:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

Mesmo que os nomes de usuários e grupos locais sejam alterados automaticamente nos bancos de dados de usuários e grupos locais, usuários locais ou nomes de grupos não são alterados automaticamente nas configurações de diretiva de diretório de arquivos (políticas configuradas na CLI usando a `vserver security file-directory` família de comandos).

Por exemplo, para "'VS1'", se você configurou uma entrada DACL onde o `-account` parâmetro é definido como "'CIFS1 " user1'", a configuração não será alterada automaticamente no SVM de destino para refletir o nome do servidor CIFS de destino.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

Você deve usar os `vserver security file-directory modify` comandos para alterar manualmente o nome do servidor CIFS para o nome do servidor CIFS de destino.

Componentes de configuração de diretiva de diretório de arquivos que contêm parâmetros de conta

Há três componentes de configuração de diretiva de diretório de arquivos que podem usar configurações de parâmetros que podem conter usuários ou grupos locais:

- Descritor de segurança

  Opcionalmente, você pode especificar o proprietário do descritor de segurança e o grupo principal do proprietário do descritor de segurança. Se o descritor de segurança usar um usuário ou grupo local para as entradas do proprietário e do grupo primário, você deverá modificar o descritor de segurança para usar o SVM de destino no nome da conta. Você pode usar o `vserver security file-directory ntfs modify` comando para fazer quaisquer alterações necessárias nos nomes de conta.

- Entradas DACL

  Cada entrada DACL deve ser associada a uma conta. Você deve modificar quaisquer DACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o nome da conta para entradas DACL existentes, você deve remover quaisquer entradas DACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas DACL com os nomes de conta de destino corrigidos e associar essas novas entradas DACL aos descritores de segurança apropriados.

- Entradas SACL

  Cada entrada SACL deve ser associada a uma conta. Você deve modificar quaisquer SACLs que usem contas de usuário ou grupo locais para usar o nome do SVM de destino. Como você não pode modificar o

nome da conta para entradas SACL existentes, você deve remover quaisquer entradas SACL com usuários locais ou grupos dos descritores de segurança, criar novas entradas SACL com os nomes de conta de destino corrigidos e associar essas novas entradas SACL aos descritores de segurança apropriados.

Você deve fazer as alterações necessárias aos usuários locais ou grupos usados na configuração da diretiva de diretório de arquivos antes de aplicar a diretiva; caso contrário, a tarefa aplicar falha.

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar um descritor de segurança NTFS (política de segurança de arquivos) é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em máquinas virtuais de armazenamento (SVMs). Você pode associar o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Adicione entradas de controle de acesso NTFS DACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) DACL (lista de controle de acesso discricionária) ao descritor de segurança NTFS é a segunda etapa na configuração e aplicação de ACLs NTFS a um arquivo ou pasta. Cada entrada identifica qual objeto é permitido ou negado acesso e define o que o objeto pode ou não pode fazer aos arquivos ou pastas definidos no ACE.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs à DACL do descritor de segurança.

Se o descritor de segurança contiver uma DACL que tenha ACEs existentes, o comando adicionará o novo ACE à DACL. Se o descritor de segurança não contiver uma DACL, o comando criará a DACL e adicionará a nova ACE a ele.

Opcionalmente, você pode personalizar entradas DACL especificando quais direitos deseja permitir ou negar para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

> Se você não especificar direitos para a entrada DACL, o padrão será definir os direitos como `Full Control`.

Opcionalmente, você pode personalizar entradas DACL especificando como aplicar herança.

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma entrada DACL a um descritor de segurança: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. Verifique se a entrada DACL está correta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

```
                Vserver: vs1
      Security Descriptor Name: sd1
                Allow or Deny: deny
           Account Name or SID: DOMAIN\joe
                Access Rights: full-control
        Advanced Access Rights: -
                     Apply To: this-folder
                Access Rights: full-control
```

Crie políticas de segurança

Criar uma política de segurança de arquivos para SVMs é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada SVM (contendo volumes de estilo de segurança NTFS ou volumes de estilo de segurança misto).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para

um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Ao adicionar tarefas a políticas de segurança, você deve especificar os quatro parâmetros necessários a seguir:

- Nome do SVM
- Nome da política
- Caminho
- Descritor de segurança para associar ao caminho

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas

de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de segurança de arquivos a SVMs é a última etapa na criação e aplicação de ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a segurança do arquivo aplicado

Você pode verificar as configurações de segurança do arquivo para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações desejadas.

Sobre esta tarefa

Você deve fornecer o nome do SVM que contém os dados e o caminho para o arquivo e pastas em que deseja verificar as configurações de segurança. Você pode usar o parâmetro opcional `-expand-mask` para exibir informações detalhadas sobre as configurações de segurança.

Passo

1. Exibir configurações de segurança de arquivos e pastas: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   ```
   vserver security file-directory show -vserver vs1 -path /data/engineering
   -expand-mask true
   ```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
```

```
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
```

```
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
                              .... .... .... .... .... .... .... 0... =
Read EA
                              .... .... .... .... .... .... .... .0.. =
Append
                              .... .... .... .... .... .... .... ..0. =
Write
                              .... .... .... .... .... .... .... ...0 =
Read
```

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a CLI

Configure e aplique políticas de auditoria a arquivos e pastas NTFS usando a visão geral da CLI

Existem várias etapas que você deve executar para aplicar políticas de auditoria a arquivos e pastas NTFS ao usar a CLI do ONTAP. Primeiro, você cria um descritor de segurança NTFS e adiciona SACLs ao descritor de segurança. Em seguida, você cria uma política de segurança e adiciona tarefas de política. Em seguida, você aplica a política de segurança a uma máquina virtual de storage (SVM).

Sobre esta tarefa

Depois de aplicar a política de segurança, pode monitorizar o trabalho de política de segurança e, em seguida, verificar as definições da política de auditoria aplicada.

Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Informações relacionadas

Protegendo o acesso aos arquivos usando o Storage-Level Access Guard

Limites ao usar a CLI para definir a segurança de arquivos e pastas

Como os descritores de segurança são usados para aplicar a segurança de arquivos e pastas

"Auditoria de SMB e NFS e rastreamento de segurança"

Configure e aplique segurança de arquivos em arquivos e pastas NTFS usando a CLI

Crie um descritor de segurança NTFS

Criar uma política de auditoria do descritor de segurança NTFS é a primeira etapa na configuração e aplicação de listas de controle de acesso (ACLs) NTFS a arquivos e pastas residentes em SVMs. Você associará o descritor de segurança ao caminho do arquivo ou da pasta em uma tarefa de diretiva.

Sobre esta tarefa

Você pode criar descritores de segurança NTFS para arquivos e pastas que residem em volumes de estilo de segurança NTFS ou para arquivos e pastas que residem em volumes de estilo de segurança misto.

Por padrão, quando um descritor de segurança é criado, quatro entradas de controle de acesso (ACEs) da lista de controle de acesso discricionária (DACL) são adicionadas a esse descritor de segurança. Os quatro ACEs predefinidos são os seguintes:

Objeto	Tipo de acesso	Direitos de acesso	Onde aplicar as permissões
CRIAR/Administradores	Permitir	Controlo total	esta pasta, subpastas, ficheiros
CONSTRUIR/usuários	Permitir	Controlo total	esta pasta, subpastas, ficheiros
PROPRIETÁRIO DO CRIADOR	Permitir	Controlo total	esta pasta, subpastas, ficheiros
AUTORIDADE NT/SISTEMA	Permitir	Controlo total	esta pasta, subpastas, ficheiros

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Proprietário do descritor de segurança
- Grupo primário do proprietário
- Flags de controle bruto

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Se pretender utilizar os parâmetros avançados, defina o nível de privilégio para avançado: `set -privilege advanced`
2. Criar um descritor de segurança: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. Verifique se a configuração do descritor de segurança está correta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. Se estiver no nível de privilégio avançado, regresse ao nível de privilégio admin: `set -privilege admin`

Adicione entradas de controle de acesso NTFS SACL ao descritor de segurança NTFS

Adicionar entradas de controle de acesso (ACEs) SACL (lista de controle de acesso do sistema) ao descritor de segurança NTFS é a segunda etapa na criação de políticas de auditoria NTFS para arquivos ou pastas em SVMs. Cada entrada identifica o usuário ou grupo que você deseja auditar. A entrada SACL define se você deseja auditar tentativas de acesso bem-sucedidas ou com falha.

Sobre esta tarefa

Você pode adicionar um ou mais ACEs ao SACL do descritor de segurança.

Se o descritor de segurança contiver um SACL que tenha ACEs existentes, o comando adicionará o novo ACE ao SACL. Se o descritor de segurança não contiver um SACL, o comando criará o SACL e adicionará o novo ACE a ele.

Você pode configurar entradas SACL especificando quais direitos deseja auditar para eventos de sucesso ou falha para a conta especificada no `-account` parâmetro. Existem três métodos mutuamente exclusivos para especificar direitos:

- Direitos
- Direitos avançados
- Direitos brutos (privilégio avançado)

Se não especificar direitos para a entrada SACL, a predefinição é `Full Control`.

Opcionalmente, você pode personalizar entradas SACL especificando como aplicar herança com o `apply to` parâmetro. Se você não especificar esse parâmetro, o padrão é aplicar essa entrada SACL a essa pasta, subpastas e arquivos.

Passos

1. Adicione uma entrada SACL a um descritor de segurança: `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. Verifique se a entrada SACL está correta: `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                Vserver: vs1
                  Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                       Account Name or SID: DOMAIN\joe
                             Access Rights: full-control
                    Advanced Access Rights: -
                                  Apply To: this-folder
                             Access Rights: full-control
   ```

Crie políticas de segurança

Criar uma política de auditoria para máquinas virtuais de armazenamento (SVMs) é a terceira etapa na configuração e aplicação de ACLs a um arquivo ou pasta. Uma política atua como um contentor para várias tarefas, onde cada tarefa é uma única entrada que pode ser aplicada a arquivos ou pastas. Pode adicionar tarefas à política de segurança mais tarde.

Sobre esta tarefa

As tarefas que você adiciona a uma diretiva de segurança contêm associações entre o descritor de segurança NTFS e os caminhos de arquivo ou pasta. Portanto, você deve associar a política de segurança a cada máquina virtual de armazenamento (SVM) (contendo volumes de estilo de segurança NTFS ou volumes mistos de estilo de segurança).

Passos

1. Criar uma política de segurança: `vserver security file-directory policy create -vserver`

```
vserver_name -policy-name policy_name

vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. Verifique a política de segurança: `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

Adicione uma tarefa à política de segurança

Criar e adicionar uma tarefa de diretiva a uma diretiva de segurança é a quarta etapa na configuração e aplicação de ACLs a arquivos ou pastas em SVMs. Ao criar a tarefa de política, associe a tarefa a uma política de segurança. Você pode adicionar uma ou mais entradas de tarefa a uma diretiva de segurança.

Sobre esta tarefa

A política de segurança é um contentor para uma tarefa. Uma tarefa refere-se a uma única operação que pode ser feita por uma política de segurança para arquivos ou pastas com NTFS ou segurança mista (ou para um objeto de volume se configurar o Storage-Level Access Guard).

Existem dois tipos de tarefas:

- Tarefas de arquivo e diretório

  Usado para especificar tarefas que aplicam descritores de segurança a arquivos e pastas especificados. As ACLs aplicadas através de tarefas de arquivo e diretório podem ser gerenciadas com clientes SMB ou com a CLI do ONTAP.

- Tarefas do Access Guard no nível de storage

  Usado para especificar tarefas que aplicam descritores de segurança do Storage-Level Access Guard a um volume especificado. As ACLs aplicadas por meio de tarefas de proteção de acesso no nível do storage podem ser gerenciadas somente por meio da CLI do ONTAP.

Uma tarefa contém definições para a configuração de segurança de um ficheiro (ou pasta) ou conjunto de ficheiros (ou pastas). Cada tarefa em uma política é identificada exclusivamente pelo caminho. Só pode haver uma tarefa por caminho dentro de uma única política. Uma política não pode ter entradas de tarefa duplicadas.

Diretrizes para adicionar uma tarefa a uma política:

- Pode haver um máximo de 10.000 entradas de tarefas por política.
- Uma política pode conter uma ou mais tarefas.

  Mesmo que uma diretiva possa conter mais de uma tarefa, você não pode configurar uma diretiva para conter tarefas de diretório de arquivos e Guarda de Acesso em nível de armazenamento. Uma diretiva

deve conter todas as tarefas do Guarda de Acesso no nível de armazenamento ou todas as tarefas do diretório de arquivos.

- O Access Guard no nível de storage é usado para restringir permissões.

  Ele nunca dará permissões de acesso extra.

Você pode personalizar a configuração do descritor de segurança usando os seguintes parâmetros opcionais:

- Tipo de segurança
- Modo de propagação
- Posição do índice
- Tipo de controle de acesso

O valor de qualquer parâmetro opcional é ignorado para o Storage-Level Access Guard. Consulte as páginas de manual para obter mais informações.

Passos

1. Adicione uma tarefa com um descritor de segurança associado à diretiva de segurança: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` é o valor padrão para o `-access-control` parâmetro. Especificar o tipo de controle de acesso ao configurar tarefas de acesso a arquivos e diretórios é opcional.

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. Verifique a configuração da tarefa de política: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS       NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate  sd2
   ```

Aplicar políticas de segurança

Aplicar uma política de auditoria a SVMs é a última etapa na criação e aplicação de

ACLs NTFS a arquivos ou pastas.

Sobre esta tarefa

Você pode aplicar as configurações de segurança definidas na diretiva de segurança a arquivos e pastas NTFS residentes em volumes FlexVol (NTFS ou estilo de segurança misto).

> Quando uma política de auditoria e SACLs associados são aplicados, todas as DACLs existentes são substituídas. Quando uma diretiva de segurança e suas DACLs associadas são aplicadas, todas as DACLs existentes são substituídas. Você deve revisar as políticas de segurança existentes antes de criar e aplicar novas.

Passo

1. Aplicar uma política de segurança: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   ```
   vserver security file-directory apply -vserver vs1 -policy-name policy1
   ```

   O trabalho de aplicação de política está agendado e o Código trabalho é devolvido.

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

Monitorize o trabalho de política de segurança

Ao aplicar a diretiva de segurança a máquinas virtuais de armazenamento (SVMs), você pode monitorar o progresso da tarefa monitorando a tarefa de diretiva de segurança. Isso é útil se você quiser verificar se a aplicação da diretiva de segurança foi bem-sucedida. Isso também é útil se você tiver um trabalho de longa duração onde você estiver aplicando segurança em massa a um grande número de arquivos e pastas.

Sobre esta tarefa

Para exibir informações detalhadas sobre um trabalho de política de segurança, use o `-instance` parâmetro.

Passo

1. Monitorar o trabalho de política de segurança: `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

Verifique a política de auditoria aplicada

Você pode verificar a política de auditoria para confirmar se os arquivos ou pastas na máquina virtual de armazenamento (SVM) à qual você aplicou a diretiva de segurança têm as configurações de segurança de auditoria desejadas.

Sobre esta tarefa

Você usa o `vserver security file-directory show` comando para exibir informações da política de auditoria. Você deve fornecer o nome do SVM que contém os dados e o caminho para os dados cujas informações de política de auditoria de arquivo ou pasta você deseja exibir.

Passo

1. Exibir configurações da política de auditoria: `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

Exemplo

O comando a seguir exibe as informações da política de auditoria aplicadas ao caminho "'/corp" no SVM VS1. O caminho tem um SUCESSO e uma entrada SACL DE SUCESSO/FALHA aplicada a ele:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
      Security Style: ntfs
     Effective Style: ntfs
      DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
       Unix Group Id: 0
      Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                  ACLs: NTFS Security Descriptor
                        Control:0x8014
                        Owner:DOMAIN\Administrator
                        Group:BUILTIN\Administrators
                        SACL - ACEs
                          ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                          SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                        DACL - ACEs
                          ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                          ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                          ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Considerações ao gerenciar trabalhos de diretiva de segurança

Se existir um trabalho de política de segurança, em determinadas circunstâncias, não é possível modificar essa política de segurança ou as tarefas atribuídas a essa diretiva. Você deve entender em que condições você pode ou não pode modificar políticas de segurança para que quaisquer tentativas que você fizer para modificar a diretiva sejam bem-sucedidas. As modificações à política incluem adicionar, remover ou modificar tarefas atribuídas à política e excluir ou modificar a política.

Não é possível modificar uma política de segurança ou uma tarefa atribuída a essa política se existir um trabalho para essa política e essa tarefa estiver nos seguintes estados:

- O trabalho está em execução ou em curso.
- O trabalho está em pausa.
- O trabalho é retomado e está no estado em execução.
- Se a tarefa estiver aguardando o failover para outro nó.

Nas seguintes circunstâncias, se existir um trabalho para uma política de segurança, pode modificar com êxito essa política de segurança ou uma tarefa atribuída a essa política:

- O trabalho de política é interrompido.
- O trabalho de política foi concluído com êxito.

Comandos para gerenciar descritores de segurança NTFS

Existem comandos ONTAP específicos para gerenciar descritores de segurança. Você pode criar, modificar, excluir e exibir informações sobre descritores de segurança.

Se você quiser…	Use este comando…
Crie descritores de segurança NTFS	`vserver security file-directory ntfs create`
Modificar descritores de segurança NTFS existentes	`vserver security file-directory ntfs modify`
Exibir informações sobre descritores de segurança NTFS existentes	`vserver security file-directory ntfs show`
Excluir descritores de segurança NTFS	`vserver security file-directory ntfs delete`

Consulte as páginas de manual para `vserver security file-directory ntfs` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS DACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso

DACL (ACEs). Você pode adicionar ACEs a DACLs NTFS a qualquer momento. Você também pode gerenciar DACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em DACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a DACLs NTFS	`vserver security file-directory ntfs dacl add`
Modificar ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl modify`
Exibir informações sobre ACEs existentes em DACLs NTFS	`vserver security file-directory ntfs dacl show`
Remover ACEs existentes de DACLs NTFS	`vserver security file-directory ntfs dacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs dacl` obter mais informações.

Comandos para gerenciar entradas de controle de acesso NTFS SACL

Existem comandos ONTAP específicos para gerenciar entradas de controle de acesso SACL (ACEs). Você pode adicionar ACEs a SACLs NTFS a qualquer momento. Você também pode gerenciar SACLs NTFS existentes modificando, excluindo e exibindo informações sobre ACEs em SACLs.

Se você quiser…	Use este comando…
Crie ACEs e adicione-os a SACLs NTFS	`vserver security file-directory ntfs sacl add`
Modificar ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl modify`
Exibir informações sobre ACEs existentes em SACLs NTFS	`vserver security file-directory ntfs sacl show`
Remover ACEs existentes de SACLs NTFS	`vserver security file-directory ntfs sacl remove`

Consulte as páginas de manual para `vserver security file-directory ntfs sacl` obter mais informações.

Comandos para gerenciar políticas de segurança

Existem comandos ONTAP específicos para gerenciar políticas de segurança. Você pode exibir informações sobre políticas e excluir políticas. Não é possível modificar uma política de segurança.

Se você quiser…	Use este comando…
Crie políticas de segurança	`vserver security file-directory policy create`
Exibir informações sobre políticas de segurança	`vserver security file-directory policy show`
Eliminar políticas de segurança	`vserver security file-directory policy delete`

Consulte as páginas de manual para `vserver security file-directory policy` obter mais informações.

Comandos para gerenciar tarefas de diretiva de segurança

Existem comandos ONTAP para adicionar, modificar, remover e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Adicione tarefas de política de segurança	`vserver security file-directory policy task add`
Modificar tarefas de política de segurança	`vserver security file-directory policy task modify`
Exibir informações sobre as tarefas da diretiva de segurança	`vserver security file-directory policy task show`
Remover tarefas de política de segurança	`vserver security file-directory policy task remove`

Consulte as páginas de manual para `vserver security file-directory policy task` obter mais informações.

Comandos para gerenciar trabalhos de diretiva de segurança

Existem comandos ONTAP para pausar, retomar, parar e exibir informações sobre tarefas de diretiva de segurança.

Se você quiser…	Use este comando…
Pausar trabalhos de diretiva de segurança	`vserver security file-directory job pause -vserver vserver_name -id integer`
Retomar os trabalhos de política de segurança	`vserver security file-directory job resume -vserver vserver_name -id integer`
Exibir informações sobre os trabalhos de diretiva de segurança	`vserver security file-directory job show -vserver vserver_name` Pode determinar a ID da tarefa de uma tarefa utilizando este comando.
Interromper trabalhos de política de segurança	`vserver security file-directory job stop -vserver vserver_name -id integer`

Consulte as páginas de manual para `vserver security file-directory job` obter mais informações.

Configure o cache de metadados para compartilhamentos SMB

Como o armazenamento em cache de metadados SMB funciona

O armazenamento em cache de metadados permite o armazenamento em cache de atributos de arquivo em clientes SMB 1,0 para fornecer acesso mais rápido aos atributos de arquivo e pasta. Você pode ativar ou desativar o cache de atributos por compartilhamento. Você também pode configurar o tempo de permanência para entradas em cache se o armazenamento em cache de metadados estiver habilitado. A configuração do cache de metadados não é necessária se os clientes estiverem se conetando a compartilhamentos por SMB 2.x ou SMB 3,0.

Quando ativado, o cache de metadados SMB armazena dados de caminho e atributo de arquivo por um período limitado de tempo. Isso pode melhorar a performance do SMB para clientes SMB 1,0 com workloads comuns.

Para certas tarefas, o SMB cria uma quantidade significativa de tráfego que pode incluir várias consultas idênticas para metadados de caminho e arquivo. Você pode reduzir o número de consultas redundantes e melhorar o desempenho para clientes SMB 1,0 usando o cache de metadados SMB para buscar informações do cache.

> Embora improvável, é possível que o cache de metadados possa servir informações obsoletas para clientes SMB 1,0. Se o seu ambiente não puder suportar esse risco, você não deve habilitar esse recurso.

Ative o cache de metadados SMB

Você pode melhorar o desempenho do SMB para clientes SMB 1,0 ativando o cache de metadados SMB. Por padrão, o armazenamento em cache de metadados SMB está desativado.

Passo

1. Execute a ação desejada:

Se você quiser…	Digite o comando…
Ative o armazenamento em cache de metadados SMB ao criar um compartilhamento	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache`
Habilite o armazenamento em cache de metadados SMB em um compartilhamento existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache`

Informações relacionadas

Configurando o tempo de vida das entradas de cache de metadados SMB

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Configure o tempo de vida das entradas de cache de metadados SMB

Você pode configurar o tempo de vida das entradas de cache de metadados SMB para otimizar o desempenho do cache de metadados SMB em seu ambiente. O padrão é 10 segundos.

Antes de começar

Você deve ter habilitado o recurso de cache de metadados SMB. Se o armazenamento em cache de metadados SMB não estiver ativado, a configuração TTL de cache SMB não será usada.

Passo

1. Execute a ação desejada:

Se você quiser configurar o tempo de vida das entradas de cache de metadados SMB quando…	Digite o comando…
Crie um compartilhamento	`vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]`
Modificar um compartilhamento existente	`vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]`

Você pode especificar opções e propriedades de configuração de compartilhamento adicionais ao criar ou modificar compartilhamentos. Consulte as páginas de manual para obter mais informações.

Gerenciar bloqueios de arquivos

Acerca do bloqueio de ficheiros entre protocolos

Bloqueio de arquivos é um método usado por aplicativos cliente para impedir que um usuário acesse um arquivo aberto anteriormente por outro usuário. A forma como o ONTAP bloqueia ficheiros depende do protocolo do cliente.

Se o cliente for um cliente NFS, os bloqueios são consultivos; se o cliente for um cliente SMB, os bloqueios são obrigatórios.

Devido às diferenças entre os bloqueios de arquivos NFS e SMB, um cliente NFS pode não conseguir acessar um arquivo aberto anteriormente por um aplicativo SMB.

O seguinte ocorre quando um cliente NFS tenta aceder a um ficheiro bloqueado por uma aplicação SMB:

- Em volumes mistos ou NTFS, operações de manipulação de arquivos como `rm` , `rmdir` e `mv` podem causar falha no aplicativo NFS.
- As operações de leitura e gravação NFS são negadas pelos modos abertos SMB deny-read e deny-write, respetivamente.
- As operações de gravação NFS falham quando o intervalo escrito do arquivo é bloqueado com um bytelock SMB exclusivo.
- Desvincular
  - Para sistemas de arquivos NTFS, as operações de exclusão SMB e CIFS são suportadas.

    O arquivo será removido após o último fechamento.
  - As operações de desvinculação NFS não são suportadas.

    Ele não é suportado porque as semânticas NTFS e SMB são necessárias e a última operação Excluir-em-close não é suportada para NFS.
  - Para sistemas de arquivos UNIX, a operação de desvinculação é suportada.

    Ele é compatível porque a semântica NFS e UNIX são necessárias.
- Mudar o nome
  - Para sistemas de arquivos NTFS, se o arquivo de destino for aberto a partir de SMB ou CIFS, o arquivo de destino pode ser renomeado.
  - O nome de NFS não é suportado.

    Não é suportado porque as semânticas NTFS e SMB são necessárias.

Em volumes de estilo de segurança UNIX, as operações NFS desvincular e renomear ignoram o estado de bloqueio SMB e permitem o acesso ao arquivo. Todas as outras operações NFS em volumes estilo segurança UNIX honram o estado de bloqueio SMB.

Como o ONTAP trata bits somente de leitura

O bit somente leitura é definido em uma base arquivo por arquivo para refletir se um arquivo é gravável (desativado) ou somente leitura (habilitado).

Os clientes SMB que usam o Windows podem definir um bit somente leitura por arquivo. Os clientes NFS não definem um bit somente leitura por arquivo porque os clientes NFS não têm operações de protocolo que usam um bit somente leitura por arquivo.

O ONTAP pode definir um bit somente leitura em um arquivo quando um cliente SMB que usa o Windows cria esse arquivo. O ONTAP também pode definir um bit somente leitura quando um arquivo é compartilhado entre clientes NFS e clientes SMB. Alguns softwares, quando usados por clientes NFS e clientes SMB, exigem que o bit somente leitura seja ativado.

Para que o ONTAP mantenha as permissões de leitura e gravação apropriadas em um arquivo compartilhado entre clientes NFS e clientes SMB, ele trata o bit somente leitura de acordo com as seguintes regras:

- O NFS trata qualquer arquivo com o bit somente leitura ativado como se ele não tivesse bits de permissão de gravação ativados.
- Se um cliente NFS desativar todos os bits de permissão de gravação e pelo menos um desses bits tiver sido ativado anteriormente, o ONTAP ativa o bit somente leitura para esse arquivo.
- Se um cliente NFS ativar qualquer bit de permissão de gravação, o ONTAP desativa o bit somente leitura para esse arquivo.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente NFS tentar descobrir permissões para o arquivo, os bits de permissão para o arquivo não serão enviados para o cliente NFS; em vez disso, o ONTAP enviará os bits de permissão para o cliente NFS com os bits de permissão de gravação mascarados.
- Se o bit somente leitura de um arquivo estiver ativado e um cliente SMB desabilitar o bit somente leitura, o ONTAP ativa o bit de permissão de gravação do proprietário para o arquivo.
- Os arquivos com o bit somente leitura habilitado são graváveis somente pelo root.

> As alterações às permissões de arquivo entram em vigor imediatamente em clientes SMB, mas podem não ter efeito imediatamente em clientes NFS se o cliente NFS ativar o armazenamento em cache de atributos.

Como o ONTAP difere do Windows ao lidar com bloqueios em componentes de caminho de compartilhamento

Ao contrário do Windows, o ONTAP não bloqueia cada componente do caminho para um arquivo aberto enquanto o arquivo está aberto. Esse comportamento também afeta os caminhos de compartilhamento SMB.

Como o ONTAP não bloqueia cada componente do caminho, é possível renomear um componente do caminho acima do arquivo aberto ou do compartilhamento, o que pode causar problemas para determinados aplicativos ou fazer com que o caminho de compartilhamento na configuração do SMB seja inválido. Isso pode fazer com que o compartilhamento seja inacessível.

Para evitar problemas causados pela renomeação de componentes de caminho, você pode aplicar configurações de segurança que impedem que usuários ou aplicativos renomeem diretórios críticos.

Apresentar informações sobre bloqueios

Você pode exibir informações sobre os bloqueios de arquivo atuais, incluindo quais tipos de bloqueios são mantidos e qual é o estado de bloqueio, detalhes sobre bloqueios de intervalo de bytes, modos de sharelock, bloqueios de delegação e bloqueios oportunistas, e se os bloqueios são abertos com alças duráveis ou persistentes.

Sobre esta tarefa

O endereço IP do cliente não pode ser exibido para bloqueios estabelecidos através de NFSv4 ou NFSv4,1.

Por padrão, o comando exibe informações sobre todos os bloqueios. Você pode usar parâmetros de comando para exibir informações sobre bloqueios de uma máquina virtual de armazenamento específica (SVM) ou para filtrar a saída do comando por outros critérios.

O `vserver locks show` comando exibe informações sobre quatro tipos de bloqueios:

- Bloqueios de intervalo de bytes, que bloqueiam apenas uma parte de um arquivo.
- Bloqueios de compartilhamento, que bloqueiam arquivos abertos.
- Bloqueios oportunistas, que controlam o cache do lado do cliente sobre SMB.
- Delegações, que controlam o cache do lado do cliente sobre NFSv4.x.

Ao especificar parâmetros opcionais, você pode determinar informações importantes sobre cada tipo de bloqueio. Consulte a página de manual para obter mais informações.

Passo

1. Exiba informações sobre bloqueios usando o `vserver locks show` comando.

Exemplos

O exemplo a seguir exibe informações de resumo de um bloqueio NFSv4 em um arquivo com o `/vol1/file1` caminho . O modo de acesso sharelock é write-deny_none, e o bloqueio foi concedido com delegação de gravação:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

O exemplo a seguir exibe informações detalhadas de oplock e sharelock sobre o bloqueio SMB em um arquivo com o `/data2/data2_2/intro.pptx` caminho . Um manipulador durável é concedido no arquivo com um modo de acesso de bloqueio de compartilhamento de write-deny_none para um cliente com um endereço IP de 10,3.1,3. Uma locação de oplock é concedida com um nível de lote de oplock:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
```

```
                Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
            Lock Protocol: cifs
                Lock Type: share-level
   Node Holding Lock State: node3
              Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                  Vserver: vs1
                   Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
               Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
```

```
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

Bloqueios de rutura

Quando os bloqueios de arquivos estão impedindo o acesso do cliente aos arquivos, você pode exibir informações sobre os bloqueios atualmente mantidos e, em seguida, quebrar bloqueios específicos. Exemplos de cenários em que você pode precisar quebrar bloqueios incluem depuração de aplicativos.

Sobre esta tarefa

O `vserver locks break` comando está disponível apenas no nível de privilégio avançado e superior. A página de manual do comando contém informações detalhadas.

Passos

1. Para encontrar as informações que você precisa para quebrar um bloqueio, use o `vserver locks show` comando.

   A página de manual do comando contém informações detalhadas.

2. Defina o nível de privilégio como avançado: `set -privilege advanced`
3. Execute uma das seguintes ações:

Se você quiser quebrar um bloqueio especificando…	Digite o comando…
O nome do SVM, o nome do volume, o nome LIF e o caminho do arquivo	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
A ID de bloqueio	`vserver locks break -lockid UUID`

4. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Monitorar a atividade de SMB

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	**Digite o seguinte comando…**
Para todas as sessões no SVM de forma resumida	`vserver cifs session show -vserver vserver_name`
Em um ID de conexão especificado	`vserver cifs session show -vserver vserver_name -connection-id integer`
A partir de um endereço IP de estação de trabalho especificado	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
Em um endereço IP de LIF especificado	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
Em um nó especificado	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	De um usuário do Windows especificado
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	Com um mecanismo de autenticação especificado
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
Com uma versão de protocolo especificada	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
SMB3	SMB3_1}`  [NOTE] ==== A proteção continuamente disponível e o SMB multicanal estão disponíveis apenas nas sessões SMB 3,0 e posteriores. Para ver o seu estado em todas as sessões de qualificação, deve especificar este parâmetro com o valor definido para `SMB3` ou posterior. ====
Com um nível especificado de proteção continuamente disponível	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode usar o `vserver cifs sessions file show` comando para determinar quais arquivos na sessão estabelecida não estão abertos com proteção continuamente disponível. ====
Com um status de sessão de assinatura SMB especificado	`vserver cifs session show -vserver vserver_name -is-session-signed {true

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1.1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2         23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Informações relacionadas

Exibindo informações sobre arquivos SMB abertos

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show`

comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	`vserver cifs session file show -vserver vserver_name`
Em um nó especificado	`vserver cifs session file show -vserver vserver_name -node {node_name`
local}`	Em um ID de arquivo especificado
`vserver cifs session file show -vserver vserver_name -file-id integer`	Em uma ID de conexão SMB especificada
`vserver cifs session file show -vserver vserver_name -connection-id integer`	Em um SMB Session ID especificado
`vserver cifs session file show -vserver vserver_name -session-id integer`	No agregado de hospedagem especificado
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	No volume especificado
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	No compartilhamento SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
`vserver cifs session file show -vserver vserver_name -share share_name`	No caminho SMB especificado
`vserver cifs session file show -vserver vserver_name -path path`	Com o nível especificado de proteção continuamente disponível
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade. ====
Com o estado de reconexão especificado	`vserver cifs session file show -vserver vserver_name -reconnected {No

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informações relacionadas

Exibindo informações de sessão SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object object_name`
Quais contadores estão disponíveis	`statistics catalog counter show object object_name`

   Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível de privilégio avançado:

Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- ----------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Informações relacionadas

Exibindo estatísticas

Apresentar estatísticas

É possível exibir várias estatísticas, incluindo estatísticas sobre CIFS e SMB, auditoria e hashes BranchCache, para monitorar a performance e diagnosticar problemas.

Antes de começar

Você deve ter coletado amostras de dados usando os `statistics start` comandos e `statistics stop` antes de exibir informações sobre objetos.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite…
Todas as versões do SMB	`statistics show -object cifs`
SMB 1,0	`statistics show -object smb1`
SMB 2.x e SMB 3,0	`statistics show -object smb2`
Subsistema CIFS do nó	`statistics show -object nblade_cifs`
Auditoria multiprotocolo	`statistics show -object audit_ng`
Serviço de hash BranchCache	`statistics show -object hashd`
DNS dinâmico	`statistics show -object ddns_update`

   Consulte a página de manual de cada comando para obter mais informações.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Determinando quais objetos e contadores de estatísticas estão disponíveis

Monitoramento de estatísticas de sessão assinadas pelo SMB

Exibindo estatísticas do BranchCache

Uso de estatísticas para monitorar a atividade automática de referência de nós

"Configuração SMB para Microsoft Hyper-V e SQL Server"

"Configuração do monitoramento de desempenho"

Implantar serviços baseados em cliente SMB

Use arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Use arquivos off-line para permitir o armazenamento em cache de arquivos para visão geral de uso off-line

O ONTAP suporta o recurso arquivos off-line da Microsoft, ou *cache do lado do cliente*, que permite que os arquivos sejam armazenados em cache no host local para uso off-line. Os usuários podem usar a funcionalidade de arquivos off-line para continuar trabalhando em arquivos, mesmo quando eles são desconetados da rede.

Você pode especificar se os documentos e programas do usuário do Windows são automaticamente armazenados em cache em um compartilhamento ou se os arquivos devem ser selecionados manualmente para armazenamento em cache. O armazenamento em cache manual é ativado por padrão para novos compartilhamentos. Os arquivos disponibilizados offline são sincronizados com o disco local do cliente Windows. A sincronização ocorre quando a conetividade de rede a um compartilhamento de sistema de armazenamento específico é restaurada.

Como os arquivos e pastas offline mantêm as mesmas permissões de acesso que a versão dos arquivos e pastas salvos no servidor CIFS, o usuário deve ter permissões suficientes nos arquivos e pastas salvos no servidor CIFS para executar ações nos arquivos e pastas offline.

Quando o usuário e outra pessoa na rede fazem alterações no mesmo arquivo, o usuário pode salvar a versão local do arquivo na rede, manter a outra versão ou salvar ambas. Se o usuário mantiver ambas as versões, um novo arquivo com as alterações do usuário local será salvo localmente e o arquivo em cache será substituído por alterações da versão do arquivo salvo no servidor CIFS.

Você pode configurar arquivos off-line em uma base de compartilhamento por compartilhamento usando as configurações de compartilhamento. Você pode escolher uma das quatro configurações de pastas offline ao criar ou modificar compartilhamentos:

- Sem armazenamento em cache

  Desativa o cache do lado do cliente para o compartilhamento. Arquivos e pastas não são automaticamente armazenados em cache localmente em clientes e os usuários não podem optar por armazenar em cache arquivos ou pastas localmente.

- Armazenamento manual em cache

  Permite a seleção manual de arquivos a serem armazenados em cache no compartilhamento. Esta é a configuração padrão. Por padrão, nenhum arquivo ou pasta é armazenado em cache no cliente local. Os usuários podem escolher quais arquivos e pastas desejam armazenar em cache localmente para uso off-line.

- Armazenamento automático de documentos

  Permite que os documentos do usuário sejam automaticamente armazenados em cache no compartilhamento. Somente arquivos e pastas acessados são armazenados em cache localmente.

- Armazenamento em cache automático do programa

  Permite que programas e documentos do usuário sejam automaticamente armazenados em cache no compartilhamento. Somente arquivos, pastas e programas acessados são armazenados em cache localmente. Além disso, essa configuração permite que o cliente execute executáveis armazenados

localmente em cache, mesmo quando conetado à rede.

Para obter mais informações sobre a configuração de arquivos off-line em servidores e clientes do Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM

Usando redirecionamento de pasta para armazenar dados em um servidor CIFS

Usando o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos para usar arquivos off-line

Antes de poder utilizar a funcionalidade ficheiros offline da Microsoft com o servidor CIFS, tem de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que suportam a funcionalidade.

Requisitos de versão do ONTAP

As versões do ONTAP suportam arquivos off-line.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte a arquivos off-line em todas as versões do SMB.

Requisitos do cliente Windows

O cliente Windows deve suportar os arquivos off-line.

Para obter as informações mais recentes sobre quais clientes do Windows oferecem suporte ao recurso arquivos off-line, consulte Matriz de interoperabilidade.

"mysupport.NetApp.com/matrix"

Diretrizes para a implantação de arquivos offline

Existem algumas diretrizes importantes que você precisa entender quando você implantar arquivos off-line em compartilhamentos de diretório home que têm a `showsnapshot` propriedade de compartilhamento definida em diretórios home.

Se a `showsnapshot` propriedade compartilhar estiver definida em um compartilhamento de diretório inicial que tenha arquivos off-line configurados, os clientes do Windows armazenam em cache todas as cópias Snapshot `~snapshot` na pasta no diretório inicial do usuário.

Os clientes Windows armazenam em cache todas as cópias Snapshot no diretório inicial se uma das seguintes opções for verdadeira:

- O usuário torna o diretório home disponível offline a partir do cliente.

O conteúdo da `~snapshot` pasta no diretório inicial é incluído e disponibilizado offline.

- O usuário configura o redirecionamento de pasta para redirecionar uma pasta, como `My Documents` a raiz de um diretório home que reside no compartilhamento do servidor CIFS.

  Alguns clientes do Windows podem tornar a pasta redirecionada automaticamente disponível offline. Se a pasta for redirecionada para a raiz do diretório inicial, a `~snapshot` pasta será incluída no conteúdo offline em cache.

> Implantações de arquivos offline onde a `~snapshot` pasta está incluída em arquivos offline devem ser evitadas. As cópias Snapshot na `~snapshot` pasta contêm todos os dados no volume no ponto em que o ONTAP criou a cópia Snapshot. Portanto, criar uma cópia off-line da `~snapshot` pasta consome armazenamento local significativo no cliente, consome largura de banda da rede durante a sincronização de arquivos off-line e aumenta o tempo necessário para sincronizar arquivos off-line.

Configure o suporte a arquivos off-line em compartilhamentos SMB usando a CLI

Você pode configurar o suporte a arquivos off-line usando a CLI do ONTAP especificando uma das quatro configurações de arquivos off-line ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte manual de arquivos offline é a configuração padrão.

Sobre esta tarefa

Ao configurar o suporte a arquivos off-line, você pode escolher uma das quatro configurações de arquivos off-line a seguir:

Definição	Descrição
`none`	Não permite que os clientes Windows armazenem quaisquer arquivos neste compartilhamento.
`manual`	Permite que os usuários em clientes Windows selecionem manualmente os arquivos a serem armazenados em cache.
`documents`	Permite que os clientes Windows armazenem documentos de usuário que são usados pelo usuário para acesso off-line.
`programs`	Permite que os clientes do Windows armazenem programas que são usados pelo usuário para acesso off-line. Os clientes podem usar os arquivos de programa armazenados em cache no modo offline, mesmo que o compartilhamento esteja disponível.

Você pode escolher apenas uma configuração de arquivo off-line. Se você modificar uma configuração de arquivos off-line em um compartilhamento SMB existente, a nova configuração arquivos off-line substituirá a configuração original. Outras configurações de compartilhamento SMB existentes e propriedades de compartilhamento não são removidas ou substituídas. Eles permanecem em vigor até que sejam

explicitamente removidos ou alterados.

Passos

1. Execute a ação apropriada:

Se você quiser configurar arquivos off-line em…	Digite o comando…
Um novo compartilhamento SMB	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	Um compartilhamento SMB existente
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. Verifique se a configuração do compartilhamento SMB está correta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemplo

O comando a seguir cria um compartilhamento SMB chamado "d.ATA1" com arquivos off-line definidos como `documents`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                 Share Properties: oplocks
                                   browsable
                                   changenotify
                Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

O comando a seguir modifica um compartilhamento SMB existente chamado "d.ATA1" alterando a configuração de arquivos off-line `manual` e adicionando valores para a máscara de criação de modo de arquivo e diretório:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                      Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Configure o suporte a arquivos off-line em compartilhamentos SMB usando o MMC Gerenciamento do computador

Se você quiser permitir que os usuários armazenem arquivos localmente para uso off-line, você pode configurar o suporte a arquivos off-line usando o MMC de Gerenciamento do computador (Microsoft Management Console).

Passos

1. Para abrir o MMC no servidor Windows, no Windows Explorer, clique com o botão direito do Mouse no ícone do computador local e selecione **Gerenciar**.
2. No painel esquerdo, selecione **Gerenciamento de computador**.
3. Selecione **Ação** > **ligar a outro computador**.

   A caixa de diálogo Selecionar computador é exibida.

4. Digite o nome do servidor CIFS ou clique em **Procurar** para localizar o servidor CIFS.

   Se o nome do servidor CIFS for o mesmo nome do host da máquina virtual de storage (SVM), digite o nome do SVM. Se o nome do servidor CIFS for diferente do nome do host SVM, digite o nome do servidor CIFS.

5. Clique em **OK**.
6. Na árvore da consola, clique em **Ferramentas do sistema** > **pastas partilhadas**.
7. Clique em **compartilhamentos**.
8. No painel de resultados, clique com o botão direito do rato no partilhar.
9. Clique em **Propriedades**.

   As propriedades para a partilha selecionada são apresentadas.

10. Na guia **Geral**, clique em **Configurações off-line**.

    A caixa de diálogo Configurações off-line é exibida.

11. Configure as opções de disponibilidade off-line conforme apropriado.
12. Clique em **OK**.

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado ao SVM

Use perfis de roaming para armazenar perfis de usuário centralmente em um servidor SMB associado à visão geral da SVM

O ONTAP suporta o armazenamento de perfis de roaming do Windows em um servidor CIFS associado à máquina virtual de armazenamento (SVM). A configuração de perfis de roaming de usuários oferece vantagens para o usuário, como disponibilidade automática de recursos, independentemente de onde o usuário faz login. Os perfis de roaming também simplificam a administração e o gerenciamento de perfis de usuário.

Os perfis de usuário de roaming têm as seguintes vantagens:

- Disponibilidade automática de recursos

  O perfil exclusivo de um usuário fica automaticamente disponível quando esse usuário faz login em qualquer computador na rede que esteja executando o Windows 8, Windows 7, Windows 2000 ou Windows XP. Os usuários não precisam criar um perfil em cada computador que usam em uma rede.

- Substituição simplificada do calculador

  Como todas as informações de perfil do usuário são mantidas separadamente na rede, o perfil de um usuário pode ser facilmente baixado em um novo computador de substituição. Quando o usuário faz login no novo computador pela primeira vez, a cópia do perfil do usuário é copiada para o novo computador.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Usando redirecionamento de pasta para armazenar dados em um servidor CIFS

Requisitos para usar perfis de roaming

Antes de poder utilizar os perfis de roaming da Microsoft com o seu servidor CIFS, tem de saber quais versões do ONTAP e SMB e quais clientes do Windows suportam a funcionalidade.

Requisitos de versão do ONTAP

ONTAP suporta perfis de roaming.

Requisitos de versão do protocolo SMB

Para máquina virtual de armazenamento (SVM), o ONTAP oferece suporte a perfis de roaming em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar os perfis de roaming, o cliente Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam perfis de roaming, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurar perfis de roaming

Se você quiser disponibilizar automaticamente o perfil de um usuário quando ele fizer logon em qualquer computador da rede, poderá configurar perfis de roaming através do snap-in MMC usuários e computadores do ative Directory. Se estiver configurando perfis de roaming no Windows Server, você poderá usar o Centro de Administração do ative Directory.

Passos

1. No servidor Windows, abra o MMC usuários e computadores do ative Directory (ou o Centro de Administração do ative Directory em servidores Windows).
2. Localize o usuário para o qual você deseja configurar um perfil de roaming.
3. Clique com o botão direito do rato no utilizador e clique em **Propriedades**.
4. Na guia **Perfil**, insira o caminho do perfil para o compartilhamento onde deseja armazenar o perfil de roaming do usuário, seguido de `%username%`.

   Por exemplo, um caminho de perfil pode ser o seguinte `\\vs1.example.com\profiles\%username%`: . A primeira vez que um utilizador inicia sessão `%username%` é substituído pelo nome do utilizador.

   > No caminho `\\vs1.example.com\profiles\%username%` `profiles` , é o nome de compartilhamento de um compartilhamento na máquina virtual de armazenamento (SVM) VS1 que tem direitos de controle total para todos.

5. Clique em **OK**.

Use o redirecionamento de pastas para armazenar dados em um servidor SMB

Use o redirecionamento de pastas para armazenar dados em uma visão geral do servidor SMB

O ONTAP oferece suporte ao redirecionamento de pastas da Microsoft, o que permite que usuários ou administradores redirecionem o caminho de uma pasta local para um local no servidor CIFS. Aparece como se as pastas redirecionadas fossem armazenadas

no cliente Windows local, mesmo que os dados estejam armazenados em um compartilhamento SMB.

O redirecionamento de pastas destina-se principalmente a organizações que já implantaram diretórios base e que desejam manter a compatibilidade com seu ambiente de diretório base existente.

- `Documents`, `Desktop` e `Start Menu` são exemplos de pastas que podem ser redirecionadas.
- Os usuários podem redirecionar pastas de seu cliente Windows.
- Os administradores podem configurar e gerenciar centralmente o redirecionamento de pastas configurando GPOs no ative Directory.
- Se os administradores tiverem configurado perfis de roaming, o redirecionamento de pastas permite que os administradores dividam os dados do usuário dos dados do perfil.
- Os administradores podem usar o redirecionamento de pastas e arquivos offline juntos para redirecionar o armazenamento de dados para pastas locais para o servidor CIFS, permitindo que os usuários armazenem o conteúdo localmente.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Usando perfis de roaming para armazenar perfis de usuário centralmente em um servidor CIFS associado ao SVM

Requisitos para usar o redirecionamento de pastas

Antes de poder usar o redirecionamento de pastas da Microsoft com o servidor CIFS, você precisa saber quais versões do ONTAP e SMB e quais clientes do Windows suportam o recurso.

Requisitos de versão do ONTAP

O ONTAP suporta redirecionamento de pastas da Microsoft.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP oferece suporte ao redirecionamento de pastas da Microsoft em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar o redirecionamento de pastas da Microsoft, o cliente do Windows deve suportar o recurso.

Para obter as informações mais recentes sobre quais clientes do Windows suportam redirecionamento de pastas, consulte Matriz de interoperabilidade.

"mysupport.NetApp.com/matrix"

Configurar redirecionamento de pastas

Você pode configurar o redirecionamento de pastas usando a janela Propriedades do Windows. A vantagem de usar esse método é que o usuário do Windows pode

configurar o redirecionamento de pastas sem a ajuda do administrador SVM.

Passos

1. No Explorador do Windows, clique com o botão direito do rato na pasta que pretende redirecionar para uma partilha de rede.
2. Clique em **Propriedades**.

   As propriedades para a partilha selecionada são apresentadas.

3. Na guia **atalho**, clique em **destino** e especifique o caminho para o local da rede onde deseja redirecionar a pasta selecionada.

   Por exemplo, se você quiser redirecionar uma pasta para a `data` pasta em um diretório inicial mapeado para `Q:\`, especifique `Q:\data` como destino.

4. Clique em **OK**.

   Para obter mais informações sobre como configurar pastas offline, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Acesse o diretório de snapshot de clientes Windows usando SMB 2.x

O método usado para acessar o `~snapshot` diretório de clientes do Windows usando SMB 2.x difere do método usado para SMB 1,0. Você precisa entender como acessar o `~snapshot` diretório ao usar conexões SMB 2.x para acessar com êxito os dados armazenados em cópias Snapshot.

O administrador do SVM controla se os usuários em clientes Windows podem exibir e acessar o `~snapshot` diretório em um compartilhamento ativando ou desativando a `showsnapshot` propriedade de compartilhamento usando comandos das famílias de propriedades de compartilhamento cifs do vserver.

Quando a `showsnapshot` propriedade compartilhar está desativada, um usuário em um cliente Windows que usa SMB 2.x não pode exibir o `~snapshot` diretório e não pode acessar cópias Snapshot dentro `~snapshot` do diretório, mesmo quando manualmente inserir o caminho para `~snapshot` o diretório ou para cópias Snapshot específicas dentro do diretório.

Quando a `showsnapshot` propriedade compartilhar está ativada, um usuário em um cliente Windows que usa SMB 2.x ainda não pode exibir o `~snapshot` diretório na raiz do compartilhamento ou em qualquer junção ou diretório abaixo da raiz do compartilhamento. No entanto, depois de se conetar a um compartilhamento, o usuário pode acessar o diretório oculto `~snapshot` anexando manualmente `\~snapshot` ao final do caminho de compartilhamento. O diretório oculto `~snapshot` é acessível a partir de dois pontos de entrada:

- Na raiz da partilha
- Em cada ponto de junção no espaço de partilha

O diretório oculto `~snapshot` não é acessível a partir de subdiretórios que não sejam de junção dentro do compartilhamento.

Exemplo

Com a configuração mostrada no exemplo a seguir, um usuário em um cliente Windows com uma conexão SMB 2.x ao compartilhamento "'eng'" pode acessar o `~snapshot` diretório anexando manualmente `\~snapshot` o caminho de compartilhamento na raiz do compartilhamento e em cada ponto de junção no caminho. O diretório oculto `~snapshot` é acessível a partir dos seguintes três caminhos:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

Recupere arquivos e pastas usando versões anteriores

Recupere arquivos e pastas usando a visão geral das versões anteriores

A capacidade de usar as versões anteriores da Microsoft é aplicável a sistemas de arquivos que suportam cópias Snapshot de alguma forma e as habilitam. A tecnologia Snapshot faz parte integrante do ONTAP. Os usuários podem recuperar arquivos e pastas de cópias Snapshot de seu cliente Windows usando o recurso versões anteriores da Microsoft.

A funcionalidade de versões anteriores fornece um método para os usuários navegarem pelas cópias Snapshot ou restaurarem dados de uma cópia Snapshot sem a intervenção do administrador de storage. As versões anteriores não são configuráveis. Está sempre ativado. Se o administrador de storage disponibilizar cópias Snapshot em um compartilhamento, o usuário poderá usar versões anteriores para executar as seguintes tarefas:

- Recuperar arquivos que foram excluídos acidentalmente.
- Recuperar de acidentalmente sobrescrever um arquivo.
- Compare versões do arquivo enquanto trabalha.

Os dados armazenados nas cópias Snapshot são somente leitura. Os usuários devem salvar uma cópia de

um arquivo em outro local para fazer quaisquer alterações no arquivo. As cópias snapshot são excluídas periodicamente; portanto, os usuários precisam criar cópias de arquivos contidos em versões anteriores se quiserem manter indefinidamente uma versão anterior de um arquivo.

Requisitos para usar versões anteriores da Microsoft

Antes de poder utilizar versões anteriores com o seu servidor CIFS, precisa de saber quais as versões do ONTAP e SMB e quais os clientes do Windows que o suportam. Você também precisa saber sobre o requisito de configuração de cópia Snapshot.

Requisitos de versão do ONTAP

Suporta versões anteriores.

Requisitos de versão do protocolo SMB

Para máquina virtual de storage (SVM), o ONTAP é compatível com versões anteriores em todas as versões do SMB.

Requisitos do cliente Windows

Antes que um usuário possa usar versões anteriores para acessar dados em cópias Snapshot, o cliente do Windows deve oferecer suporte ao recurso.

Para obter as informações mais recentes sobre quais clientes Windows suportam versões anteriores, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos para configurações de cópia Snapshot

Para usar versões anteriores para acessar dados em cópias Snapshot, uma política de Snapshot habilitada deve estar associada ao volume que contém os dados, os clientes precisam ter acesso aos dados do Snapshot e as cópias Snapshot devem existir.

Use a guia versões anteriores para exibir e gerenciar dados de cópia Snapshot

Os usuários em máquinas clientes Windows podem usar a guia versões anteriores na janela Propriedades do Windows para restaurar dados armazenados em cópias Snapshot sem precisar envolver o administrador da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

Você só poderá usar a guia versões anteriores para exibir e gerenciar dados em cópias Snapshot de dados armazenados no SVM se o administrador tiver habilitado cópias Snapshot no volume que contém o compartilhamento e se o administrador configurar o compartilhamento para mostrar cópias Snapshot.

Passos

1. No Windows Explorer, exiba o conteúdo da unidade mapeada dos dados armazenados no servidor CIFS.
2. Clique com o botão direito do rato no ficheiro ou pasta na unidade de rede mapeada cujas cópias Snapshot pretende visualizar ou gerir.
3. Clique em **Propriedades**.

As propriedades para o arquivo ou pasta selecionado são exibidas.

4. Clique no separador **versões anteriores**.

   Uma lista de cópias Snapshot disponíveis do arquivo ou pasta selecionado é exibida na caixa versões da pasta:. As cópias Snapshot listadas são identificadas pelo prefixo do nome da cópia Snapshot e pelo carimbo de data/hora da criação.

5. Na caixa **versões da pasta:**, clique com o botão direito do Mouse na cópia do arquivo ou pasta que você deseja gerenciar.
6. Execute a ação apropriada:

Se você quiser…	Faça o seguinte…
Exibir dados dessa cópia Snapshot	Clique em **abrir**.
Crie uma cópia dos dados dessa cópia Snapshot	Clique em **Copiar**.

   Os dados nas cópias Snapshot são somente leitura. Se você quiser fazer modificações nos arquivos e pastas listados na guia versões anteriores, salve uma cópia dos arquivos e pastas que deseja modificar para um local gravável e faça modificações nas cópias.

7. Depois de concluir o gerenciamento dos dados do Snapshot, feche a caixa de diálogo **Propriedades** clicando em **OK**.

   Para obter mais informações sobre como usar a guia versões anteriores para exibir e gerenciar dados do Snapshot, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Determine se as cópias Snapshot estão disponíveis para uso em versões anteriores

Você pode exibir cópias Snapshot da guia versões anteriores somente se uma política de snapshot habilitada for aplicada ao volume que contém o compartilhamento e se a configuração de volume permitir acesso a cópias snapshot. Determinar a disponibilidade da cópia Snapshot é útil ao ajudar um usuário com acesso a versões anteriores.

Passos

1. Determine se o volume no qual residem os dados de compartilhamento tem cópias automáticas do Snapshot ativadas e se os clientes têm acesso aos diretórios do Snapshot: `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   A saída exibe a política Snapshot associada ao volume, se o acesso ao diretório Snapshot do cliente está habilitado e o número de cópias Snapshot disponíveis.

2. Determine se a política de snapshot associada está ativada: `volume snapshot policy show -policy policy-name`
3. Listar as cópias Snapshot disponíveis: `volume snapshot show -volume volume_name`

Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "Proteção de dados"consulte .

Exemplo

O exemplo a seguir exibe informações sobre políticas de Snapshot associadas ao volume chamado "ATA1" que contém os dados compartilhados e as cópias Snapshot disponíveis no "ATA1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                SnapMirror Label
    ---------------- -----     --------------------- -------------------
    hourly               6     hourly                -
    daily                2     daily                 daily
    weekly               2     weekly                weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

Informações relacionadas

Criando uma configuração Snapshot para habilitar o acesso a versões anteriores

"Proteção de dados"

Crie uma configuração Snapshot para habilitar o acesso a versões anteriores

A funcionalidade de versões anteriores está sempre disponível, desde que o acesso do cliente às cópias Snapshot esteja habilitado e desde que existam cópias Snapshot. Se a configuração da cópia Snapshot não atender a esses requisitos, você poderá criar uma configuração de cópia Snapshot correspondente.

Passos

1. Se o volume que contém o compartilhamento ao qual você deseja permitir o acesso a versões anteriores não tiver uma política Snapshot associada, associe uma política Snapshot ao volume e ative-a usando o `volume modify` comando.

   Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

2. Habilite o acesso às cópias Snapshot usando o `volume modify` comando para definir a `-snap-dir` opção como `true`.

   Para obter mais informações sobre como usar o `volume modify` comando, consulte as páginas de manual.

3. Verifique se as políticas Snapshot estão ativadas e se o acesso aos diretórios Snapshot está ativado usando os `volume show` comandos e. `volume snapshot policy show`

   Para obter mais informações sobre como usar os `volume show` comandos e `volume snapshot policy show`, consulte as páginas de manual.

   Para obter mais informações sobre como configurar e gerenciar políticas de Snapshot e programações de snapshot, "Proteção de dados"consulte .

Informações relacionadas

"Proteção de dados"

Diretrizes para restaurar diretórios que contêm junções

Existem certas diretrizes que você deve ter em mente ao usar versões anteriores para restaurar pastas que contêm pontos de junção.

Ao usar versões anteriores para restaurar pastas com pastas filhas que são pontos de junção, a restauração pode falhar com um `Access Denied` erro.

Você pode determinar se a pasta que você está tentando restaurar contém uma junção usando o `vol show` comando com a `-parent` opção. Você também pode usar os `vserver security trace` comandos para criar logs detalhados sobre problemas de acesso a arquivos e pastas.

Informações relacionadas

Criação e gerenciamento de volumes de dados em namespaces nas

Implante serviços baseados em servidor SMB

Gerenciar diretórios base

Como o ONTAP ativa diretórios base dinâmicos

Os diretórios iniciais do ONTAP permitem configurar um compartilhamento SMB que mapeia para diferentes diretórios com base no usuário que se coneta a ele e um conjunto de variáveis. Em vez de criar compartilhamentos separados para cada usuário, você pode configurar um compartilhamento com alguns parâmetros do diretório inicial para definir a relação de um usuário entre um ponto de entrada (o compartilhamento) e o diretório inicial (um diretório no SVM).

Um usuário que está conetado como um usuário convidado não tem um diretório home e não pode acessar os diretórios home de outros usuários. Existem quatro variáveis que determinam como um usuário é mapeado para um diretório:

- **Nome da partilha**

  Este é o nome do compartilhamento que você cria ao qual o usuário se coneta. Você deve definir a propriedade do diretório base para esse compartilhamento.

  O nome do compartilhamento pode usar os seguintes nomes dinâmicos:

  - `%w` (O nome de utilizador do Windows do utilizador)
  - `%d` (O nome de domínio do Windows do utilizador)
  - `%u` (O nome de usuário UNIX mapeado do usuário) para tornar o nome de compartilhamento exclusivo em todos os diretórios base, o nome de compartilhamento deve conter a/`%w` variável ou `%u`. O nome do compartilhamento pode conter tanto a `%d` e a/`%w` variável (por exemplo, `%d`/`%w`), ou o nome do compartilhamento pode conter uma porção estática e uma porção variável (por exemplo, Home_/`%w`).
- **Caminho de compartilhamento**

  Este é o caminho relativo, que é definido pelo compartilhamento e, portanto, está associado a um dos nomes de compartilhamento, que é anexado a cada caminho de pesquisa para gerar o caminho do diretório home inteiro do usuário a partir da raiz do SVM. Pode ser estático (por exemplo, `home`), dinâmico (por exemplo, `%w`) ou uma combinação dos dois (por exemplo, `eng/%w`).
- **Pesquisar caminhos**

  Esse é o conjunto de caminhos absolutos da raiz do SVM que você especifica que direciona a busca do ONTAP por diretórios base. Você pode especificar um ou mais caminhos de pesquisa usando o `vserver cifs home-directory search-path add` comando. Se você especificar vários caminhos de pesquisa, o ONTAP os tentará na ordem especificada até encontrar um caminho válido.
- **Diretório**

  Este é o diretório home do usuário que você cria para o usuário. O nome do diretório é geralmente o nome do usuário. Você deve criar o diretório home em um dos diretórios que são definidos pelos caminhos de pesquisa.

Como exemplo, considere a seguinte configuração:

- Usuário: John Smith

- Domínio de usuário: acme
- Nome de usuário: jsmith
- Nome do SVM: VS1
- Nome de compartilhamento de diretório base nº 1: Home_ `%w` - caminho de compartilhamento: `%w`
- Nome de compartilhamento do diretório base nº 2: `%w` - Caminho de compartilhamento: `%d/%w`
- Caminho de pesquisa nº 1: `/vol0home/home`
- Caminho de pesquisa nº 2: `/vol1home/home`
- Caminho de pesquisa nº 3: `/vol2home/home`
- Diretório base: `/vol1home/home/jsmith`

Cenário 1: O usuário se coneta `\\vs1\home_jsmith` ao . Isso corresponde ao primeiro nome de compartilhamento do diretório inicial e gera o caminho `jsmith`relativo . O ONTAP procura agora um diretório nomeado `jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/jsmith` existe; portanto, o caminho de pesquisa nº 3 não está marcado; o usuário agora está conetado ao seu diretório inicial.

Cenário 2: O usuário se coneta `\\vs1\jsmith` ao . Isso corresponde ao segundo nome de compartilhamento do diretório inicial e gera o caminho `acme/jsmith`relativo . O ONTAP procura agora um diretório nomeado `acme/jsmith` verificando cada caminho de pesquisa em ordem:

- `/vol0home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 2.
- `/vol1home/home/acme/jsmith` não existe; passando para o caminho de pesquisa nº 3.
- `/vol2home/home/acme/jsmith` não existe; o diretório home não existe; portanto, a conexão falha.

Compartilhamentos de diretório base

Adicione um compartilhamento de diretório base

Se você quiser usar o recurso diretório base SMB, você deve adicionar pelo menos um compartilhamento com a propriedade diretório base incluída nas propriedades de compartilhamento.

Sobre esta tarefa

Você pode criar um compartilhamento de diretório inicial no momento em que você cria o compartilhamento usando o `vserver cifs share create` comando, ou você pode alterar um compartilhamento existente em um compartilhamento de diretório inicial a qualquer momento usando o `vserver cifs share modify` comando.

Para criar um compartilhamento de diretório inicial, você deve incluir o `homedirectory` valor na `-share -properties` opção quando criar ou modificar um compartilhamento. Você pode especificar o nome do compartilhamento e o caminho do compartilhamento usando variáveis que são expandidas dinamicamente quando os usuários se conetam a seus diretórios base. As variáveis disponíveis que você pode usar no caminho são `%w`, `%d` e `%u`, correspondentes ao nome de usuário, domínio e nome de usuário UNIX mapeado do Windows, respetivamente.

Passos

1. Adicionar um diretório de casa compartilhar
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name` *`share-name`* especifica o nome de compartilhamento do diretório base.

   Além de conter uma das variáveis necessárias, se o nome do compartilhamento contiver uma das strings literais `%w` , `%u`, ou `%d`, você deve preceder a string literal com um caractere % (percentual) para impedir que o ONTAP trate a string literal como uma variável (por exemplo, `%%w`).

   - O nome do compartilhamento deve conter a `%w` variável ou `%u`.
   - O nome do compartilhamento também pode conter a `%d` variável (por exemplo, `%d/%w`) ou uma parte estática no nome do compartilhamento (por exemplo, home1_/`%w`).
   - Se o compartilhamento for usado pelos administradores para se conetar aos diretórios home de outros usuários ou para permitir que os usuários se conetem aos diretórios home de outros usuários, o padrão de nome de compartilhamento dinâmico deve ser precedido por um til (.).

     ```
     `vserver cifs home-directory modify`O é utilizado para ativar este acesso definindo `-is-home-dirs-access-for-admin-enabled` a opção como `true`) ou definindo a opção avançada `-is-home-dirs-access-for-public-enabled` como `true`.
     ```

   `-path path` especifica o caminho relativo para o diretório home.

`-share-properties homedirectory[,…]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

1. Verifique se você adicionou com êxito o compartilhamento do diretório home usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento de diretório base `%w` chamado . As `oplocks` propriedades , `browsable`, e `changenotify` compartilhar são definidas além de definir a `homedirectory` propriedade compartilhar.

> Este exemplo não exibe a saída de todos os compartilhamentos no SVM. A saída é truncada.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver    Share    Path         Properties     Comment  ACL
---------- -------- ------------ -------------- -------- -----------
vs1        %w       %w           oplocks        -        Everyone / Full
Control
                                 browsable
                                 changenotify
                                 homedirectory
```

Informações relacionadas

Adicionando um caminho de pesquisa de diretório base

Requisitos e diretrizes para o uso de referências automáticas de nós

Gerenciando a acessibilidade aos diretórios home dos usuários

Compartilhamentos de diretório inicial exigem nomes de usuário exclusivos

Tenha cuidado para atribuir nomes de usuário exclusivos ao criar compartilhamentos de diretório inicial usando as `%w` variáveis (nome de usuário do Windows) ou `%u` (nome de usuário UNIX) para gerar compartilhamentos dinamicamente. O nome da partilha é mapeado para o seu nome de utilizador.

Podem ocorrer dois problemas quando o nome de uma partilha estática e o nome de um utilizador são os mesmos:

- Quando o usuário lista os compartilhamentos em um cluster usando o `net view` comando, dois compartilhamentos com o mesmo nome de usuário são exibidos.
- Quando o usuário se coneta a esse nome de compartilhamento, o usuário está sempre conetado ao compartilhamento estático e não pode acessar o compartilhamento do diretório inicial com o mesmo nome.

Por exemplo, há um compartilhamento chamado "administrador" e você tem um nome de usuário do Windows. Se você criar um compartilhamento de diretório base e se conetar a esse compartilhamento, você será conetado ao compartilhamento estático "'administrador'", não ao compartilhamento de diretório principal "'administrador'".

Você pode resolver o problema com nomes de compartilhamento duplicados seguindo qualquer uma destas etapas:

- Renomear o compartilhamento estático para que ele não fique em conflito com o compartilhamento do diretório home do usuário.
- Dando ao usuário um novo nome de usuário para que ele não fique em conflito com o nome de compartilhamento estático.
- Criando um compartilhamento de diretório home CIFS com um nome estático, como "'home'", em vez de

usar o `%w` parâmetro para evitar conflitos com os nomes de compartilhamento.

O que acontece com nomes estáticos de compartilhamento de diretório base após a atualização

Os nomes de compartilhamento de diretório base devem conter a `%w` variável dinâmica ou `%u` . Você deve estar ciente do que acontece com nomes de compartilhamento de diretório home estático existentes após atualizar para uma versão do ONTAP com o novo requisito.

Se a configuração do diretório base contiver nomes de compartilhamento estáticos e você atualizar para o ONTAP, os nomes de compartilhamento do diretório base estático não serão alterados e ainda serão válidos. No entanto, você não pode criar novos compartilhamentos de diretório base que não contenham a `%w` variável ou `%u`.

Exigir que uma dessas variáveis seja incluída no nome de compartilhamento do diretório home do usuário garante que cada nome de compartilhamento seja exclusivo em toda a configuração do diretório home. Se desejar, você pode alterar os nomes estáticos de compartilhamento do diretório base para nomes que contêm a `%w` variável ou `%u`.

Adicione um caminho de pesquisa de diretório base

Se você quiser usar diretórios home do ONTAP SMB, você deve adicionar pelo menos um caminho de pesquisa de diretório base.

Sobre esta tarefa

Você pode adicionar um caminho de pesquisa de diretório base usando o `vserver cifs home-directory search-path add` comando.

O `vserver cifs home-directory search-path add` comando verifica o caminho especificado na `-path` opção durante a execução do comando. Se o caminho especificado não existir, o comando gera uma mensagem solicitando se deseja continuar. Você escolhe `y` ou `n`. Se você optar `y` por continuar, o ONTAP criará o caminho de pesquisa. No entanto, você deve criar a estrutura do diretório antes de usar o caminho de pesquisa na configuração do diretório base. Se você optar por não continuar, o comando falhará; o caminho de pesquisa não será criado. Em seguida, você pode criar a estrutura de diretório de caminho e executar novamente o `vserver cifs home-directory search-path add` comando.

Passos

1. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.

Exemplo

O exemplo a seguir adiciona o caminho `/home1` à configuração do diretório base no SVM VS1.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

O exemplo a seguir tenta adicionar o caminho `/home2` à configuração do diretório base no SVM VS1. O caminho não existe. A escolha é feita para não continuar.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

Informações relacionadas

Adicionando um compartilhamento de diretório inicial

Crie uma configuração de diretório base usando as variáveis %W e %d

Você pode criar uma configuração de diretório base usando as `%w` variáveis e. `%d` Os usuários podem então se conetar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente.

Passos

1. Crie uma qtree para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a qtree está usando o estilo de segurança correto: `volume qtree show`
3. Se a qtree não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name %w` especifica o nome de compartilhamento do diretório base. O ONTAP cria dinamicamente o nome do compartilhamento à medida que cada usuário se coneta ao seu diretório inicial. O nome da partilha será do formulário *Windows_user_name*.

   `-path %d/%w` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e será do formulário *domain/Windows_user_name*.

`-share-properties homedirectory[,…]+` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

   `-path` *`path`* especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Para usuários com um diretório home, crie um diretório correspondente na qtree ou volume designado para conter diretórios home.

   Por exemplo, se você criou uma qtree com o caminho `/vol/vol1/users` e o nome de usuário cujo diretório você deseja criar é mydomain.user1, você criará um diretório com o seguinte caminho: `/vol/vol1/users/mydomain/user1`.

   Se você criou um volume chamado "'home1" montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/mydomain/user1`.

9. Verifique se um usuário pode se conetar com êxito ao compartilhamento doméstico mapeando uma unidade ou conetando-se usando o caminho UNC.

   Por exemplo, se o usuário mydomain/user1 quiser se conetar ao diretório criado na Etapa 8 que está localizado na SVM VS1, o user1 se conetaria usando o caminho UNC `\\vs1\user1` .

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é %w.
- O caminho do diretório home relativo é %d/%w.
- O caminho de pesquisa usado para conter os diretórios base `/home1` , é um volume configurado com estilo de segurança NTFS.
- A configuração é criada no SVM VS1.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base a partir de hosts do Windows. Você também pode usar esse tipo de configuração quando os usuários acessam seus diretórios base a partir de hosts Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados no Windows para controlar o acesso ao sistema de arquivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

Informações relacionadas

Configurando diretórios base usando a variável %u

Configurações adicionais do diretório base

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configure diretórios base usando a variável %u

Você pode criar uma configuração de diretório inicial onde você designar o nome de compartilhamento usando a `%w` variável, mas você usa a `%u` variável para designar o caminho relativo para o compartilhamento de diretório inicial. Em seguida, os usuários podem se conetar ao compartilhamento doméstico usando compartilhamentos criados dinamicamente usando o nome de usuário do Windows sem estar ciente do nome ou caminho real do diretório inicial.

Passos

1. Crie uma qtree para conter os diretórios iniciais do usuário: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verifique se a qtree está usando o estilo de segurança correto: `volume qtree show`
3. Se a qtree não estiver usando o estilo de segurança desejado, altere o estilo de segurança usando o `volume qtree security` comando.
4. Adicionar uma partilha de diretório base: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` Especifica a máquina virtual de storage (SVM) habilitada para CIFS na qual adicionar o caminho de pesquisa.

   `-share-name %w` especifica o nome de compartilhamento do diretório base. O nome do compartilhamento é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e é do formulário *Windows_user_name*.

   > Você também pode usar a `%u` variável para a `-share-name` opção. Isso cria um caminho de compartilhamento relativo que usa o nome de usuário UNIX mapeado.

   `-path %u` especifica o caminho relativo para o diretório home. O caminho relativo é criado dinamicamente à medida que cada usuário se coneta ao seu diretório inicial e é do formulário *mapeado_UNIX_user_name*.

   > O valor para esta opção também pode conter elementos estáticos. Por exemplo, `eng/%u`.

   `-share-properties homedirectory\[,...\]` especifica as propriedades de compartilhamento para esse compartilhamento. Você deve especificar o `homedirectory` valor. Você pode especificar propriedades de compartilhamento adicionais usando uma lista delimitada por vírgulas.

5. Verifique se o compartilhamento tem a configuração desejada usando o `vserver cifs share show` comando.
6. Adicionar um caminho de pesquisa de diretório base: `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` Especifica o SVM habilitado para CIFS no qual adicionar o caminho de pesquisa.

   `-path path` especifica o caminho absoluto do diretório para o caminho de pesquisa.

7. Verifique se você adicionou com êxito o caminho de pesquisa usando o `vserver cifs home-directory search-path show` comando.
8. Se o usuário UNIX não existir, crie o usuário UNIX usando o `vserver services unix-user create` comando.

   > O nome de usuário UNIX para o qual você mapeia o nome de usuário do Windows deve existir antes de mapear o usuário.

9. Crie um mapeamento de nomes para o usuário do Windows para o usuário UNIX usando o seguinte comando: `vserver name-mapping create -vserver vserver_name -direction win-unix`

`-priority integer -pattern windows_user_name -replacement unix_user_name`

> Se já existirem mapeamentos de nomes que mapeiem os usuários do Windows para usuários UNIX, você não precisará executar a etapa de mapeamento.

O nome de usuário do Windows é mapeado para o nome de usuário UNIX correspondente. Quando o usuário do Windows se coneta ao compartilhamento do diretório inicial, ele se coneta a um diretório inicial criado dinamicamente com um nome de compartilhamento que corresponde ao nome de usuário do Windows sem saber que o nome do diretório corresponde ao nome de usuário do UNIX.

10. Para usuários com um diretório home, crie um diretório correspondente na qtree ou volume designado para conter diretórios home.

    Por exemplo, se você criou uma qtree com o caminho `/vol/vol1/users` e o nome de usuário UNIX mapeado do usuário cujo diretório você deseja criar é ""unixuser1"", você criará um diretório com o seguinte caminho: `/vol/vol1/users/unixuser1`.

    Se você criou um volume chamado "'home1" montado no `/home1`, você criará um diretório com o seguinte caminho: `/home1/unixuser1`.

11. Verifique se um usuário pode se conetar com êxito ao compartilhamento doméstico mapeando uma unidade ou conetando-se usando o caminho UNC.

    Por exemplo, se o usuário mydomain/user1 mapeia para o usuário UNIX unixuser1 e quiser se conetar ao diretório criado na Etapa 10 que está localizado na SVM VS1, o user1 se conetaria usando o caminho UNC `\\vs1\user1` .

Exemplo

Os comandos no exemplo a seguir criam uma configuração de diretório base com as seguintes configurações:

- O nome da partilha é %w.
- O caminho relativo do diretório base é %u.
- O caminho de pesquisa usado para conter os diretórios base `/home1` , é um volume configurado com estilo de segurança UNIX.
- A configuração é criada no SVM VS1.

Você pode usar esse tipo de configuração de diretório base quando os usuários acessam seus diretórios base de hosts do Windows ou hosts do Windows e UNIX e o administrador do sistema de arquivos usa usuários e grupos baseados em UNIX para controlar o acesso ao sistema de arquivos.

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

Informações relacionadas

Criando uma configuração de diretório base usando as variáveis %W e %d

Configurações adicionais do diretório base

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configurações adicionais do diretório base

Você pode criar configurações adicionais do diretório base usando as `%w` variáveis , `%d`, e `%u` , que permitem personalizar a configuração do diretório base para atender às suas necessidades.

Você pode criar uma série de configurações de diretório inicial usando uma combinação de variáveis e strings estáticas nos nomes de compartilhamento e caminhos de pesquisa. A tabela a seguir fornece alguns exemplos ilustrando como criar diferentes configurações de diretório base:

Caminhos criados quando `/vol1/user` **contém diretórios base…**	**Compartilhar comando…**
Para criar um caminho de compartilhamento `\\vs1\~win_username` que direcione o usuário `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\win_username` que direcione o usuário `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\win_username` que direcione o usuário `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
Para criar um caminho de compartilhamento `\\vs1\unix_username` que direcione o usuário `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

Comandos para gerenciar caminhos de pesquisa

Existem comandos ONTAP específicos para gerenciar caminhos de pesquisa para configurações de diretório base SMB. Por exemplo, existem comandos para adicionar, remover e exibir informações sobre caminhos de pesquisa. Há também um comando para alterar a ordem do caminho de pesquisa.

Se você quiser…	**Use este comando…**
Adicionar um caminho de pesquisa	`vserver cifs home-directory search-path add`
Exibir caminhos de pesquisa	`vserver cifs home-directory search-path show`

Se você quiser…	Use este comando…
Altere a ordem do caminho de pesquisa	`vserver cifs home-directory search-path reorder`
Remova um caminho de pesquisa	`vserver cifs home-directory search-path remove`

Consulte a página de manual de cada comando para obter mais informações.

Exiba informações sobre o caminho do diretório inicial de um usuário SMB

Você pode exibir o caminho do diretório inicial de um usuário SMB na máquina virtual de armazenamento (SVM), que pode ser usado se você tiver vários caminhos de diretório inicial CIFS configurados e quiser ver qual caminho contém o diretório inicial do usuário.

Passo

1. Exiba o caminho do diretório base usando o `vserver cifs home-directory show-user` comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

Informações relacionadas

Gerenciando a acessibilidade aos diretórios home dos usuários

Gerencie a acessibilidade aos diretórios home dos usuários

Por padrão, o diretório home de um usuário só pode ser acessado por esse usuário. Para compartilhamentos em que o nome dinâmico do compartilhamento é precedido por um til ("til"), você pode habilitar ou desabilitar o acesso aos diretórios iniciais dos usuários por administradores do Windows ou por qualquer outro usuário (acesso público).

Antes de começar

Os compartilhamentos de diretório inicial na máquina virtual de armazenamento (SVM) devem ser configurados com nomes de compartilhamento dinâmicos que são precedidos por um til ("tilde"). Os seguintes casos ilustram os requisitos de nomeação de compartilhamento:

Nome de compartilhamento do diretório base	Exemplo de comando para se conetar ao compartilhamento
clique no botão "ok"	`net use * \\IPaddress\~domain~user/u:credentials`

Nome de compartilhamento do diretório base	Exemplo de comando para se conetar ao compartilhamento
clique no botão "ok"	`net use * \\IPaddress\~user/u:credentials`
clique no botão "ok"	`net use * \\IPaddress\abc~user/u:credentials`

Passo

1. Execute a ação apropriada:

Se você quiser ativar ou desativar o acesso aos diretórios home dos usuários para…	Digite o seguinte…
Administradores do Windows	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` A predefinição é `true`.
Qualquer utilizador (acesso público)	a. Defina o nível de privilégio como avançado `set -privilege advanced` b. Ativar ou desativar o acesso: `vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs-access-for-public-enabled {true

O exemplo a seguir permite o acesso público aos diretórios home dos usuários

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

Informações relacionadas

Exibindo informações sobre o caminho do diretório inicial de um usuário SMB

Configurar o acesso de cliente SMB a links simbólicos UNIX

Como o ONTAP permite que você forneça acesso de cliente SMB a links simbólicos UNIX

Um link simbólico é um arquivo criado em um ambiente UNIX que contém uma referência a outro arquivo ou diretório. Se um cliente acessar um link simbólico, o cliente será redirecionado para o arquivo de destino ou diretório ao qual o link simbólico se refere. O ONTAP suporta links simbólicos relativos e absolutos, incluindo widelinks (links absolutos com alvos fora do sistema de arquivos local).

O ONTAP fornece aos clientes SMB a capacidade de seguir links simbólicos UNIX configurados no SVM. Este recurso é opcional, e você pode configurá-lo por compartilhamento, usando a `-symlink-properties` opção `vserver cifs share create` do comando, com uma das seguintes configurações:

- Habilitado com acesso de leitura/gravação
- Habilitado com acesso somente leitura
- Desabilitado ocultando links simbólicos de clientes SMB
- Desativado sem acesso a links simbólicos de clientes SMB

Se você habilitar links simbólicos em um compartilhamento, links simbólicos relativos funcionam sem configuração adicional.

Se você habilitar links simbólicos em um compartilhamento, links simbólicos absolutos não funcionam imediatamente. Você deve primeiro criar um mapeamento entre o caminho UNIX do link simbólico para o caminho SMB de destino. Ao criar mapeamentos de links simbólicos absolutos, você pode especificar se é um link local ou um *widelink*; widelinks podem ser links para sistemas de arquivos em outros dispositivos de armazenamento ou links para sistemas de arquivos hospedados em SVMs separadas no mesmo sistema ONTAP. Quando você cria um widelink, ele deve incluir as informações para o cliente seguir; ou seja, você cria um ponto de reparação para o cliente descobrir o ponto de junção do diretório. Se você criar um link simbólico absoluto para um arquivo ou diretório fora do compartilhamento local, mas definir a localidade como local, o ONTAP não permite o acesso ao destino.

> Se um cliente tentar excluir um link simbólico local (absoluto ou relativo), apenas o link simbólico é excluído, não o arquivo ou diretório de destino. No entanto, se um cliente tentar excluir um widelink, ele pode excluir o arquivo ou diretório de destino real ao qual o widelink se refere. O ONTAP não tem controle sobre isso porque o cliente pode abrir explicitamente o arquivo ou diretório de destino fora do SVM e excluí-lo.

- **Reparse Points e serviços de sistema de arquivos ONTAP**

  Um *ponto de reparação* é um objeto de sistema de arquivos NTFS que pode ser opcionalmente armazenado em volumes junto com um arquivo. Os pontos Reparse fornecem aos clientes SMB a capacidade de receber serviços de sistema de arquivos aprimorados ou estendidos ao trabalhar com volumes de estilo NTFS. Os pontos Reparse consistem em tags padrão que identificam o tipo de ponto de reparação e o conteúdo do ponto de reparação que pode ser recuperado por clientes SMB para processamento posterior pelo cliente. Dos tipos de objeto disponíveis para a funcionalidade estendida do sistema de arquivos, o ONTAP implementa suporte para links simbólicos NTFS e pontos de junção de diretório usando tags de ponto de reparação. Os clientes SMB que não conseguem entender o conteúdo de um ponto de reparação simplesmente ignoram e não fornecem o serviço de sistema de arquivos estendido que o ponto de reparação pode habilitar.

- * Diretório de pontos de junção e suporte ONTAP para links simbólicos*

  Os pontos de junção de diretório são locais dentro de uma estrutura de diretórios do sistema de arquivos que podem se referir a locais alternativos onde os arquivos são armazenados, seja em um caminho diferente (links simbólicos) ou em um dispositivo de armazenamento separado (widelinks). Os servidores SMB do ONTAP expõem pontos de junção de diretório para clientes Windows como pontos de reparação, permitindo que clientes capazes obtenham conteúdos de pontos de reparação do ONTAP quando um ponto de junção de diretório é atravessado. Eles podem, assim, navegar e se conetar a diferentes caminhos ou dispositivos de armazenamento como se fossem parte do mesmo sistema de arquivos.

- * Habilitando o suporte de widelink usando opções de ponto de reparação*

  A `-is-use-junctions-as-reparse-points-enabled` opção está ativada por predefinição no ONTAP 9. Nem todos os clientes SMB suportam widelinks, portanto, a opção de ativar as informações é configurável com base na versão por protocolo, permitindo que os administradores acomodem clientes SMB com suporte e não suporte. No ONTAP 9.2 e versões posteriores, você deve habilitar a opção

`-widelink-as-reparse-point-versions` para cada protocolo cliente que acessa o compartilhamento usando widelinks; o padrão é SMB1. Em versões anteriores, apenas os widelinks acessados usando o SMB1 padrão foram relatados e os sistemas que usam SMB2 ou SMB3 não conseguiram acessar os widelinks.

Informações relacionadas

- "Aplicativos de backup do Windows e links simbólicos em estilo Unix"
- "Documentação da Microsoft: Pontos de reanálise"

Limites ao configurar links simbólicos UNIX para acesso SMB

Você precisa estar ciente de certos limites ao configurar links simbólicos UNIX para acesso SMB.

Limite	Descrição
45	Comprimento máximo do nome do servidor CIFS que você pode especificar ao usar um FQDN para o nome do servidor CIFS. Você pode, alternativamente, especificar o nome do servidor CIFS como um nome NetBIOS, que é limitado a 15 carateres.
80	Comprimento máximo do nome da partilha.
256	Comprimento máximo do caminho UNIX que você pode especificar ao criar um link simbólico ou ao modificar o caminho UNIX de um link simbólico existente. O caminho UNIX deve começar com um "`"/" (slash) and end with a "/"`". As barras de início e fim contam como parte do limite de 256 carateres.
256	Comprimento máximo do caminho CIFS que você pode especificar ao criar um link simbólico ou ao modificar o caminho CIFS de um link simbólico existente. O caminho CIFS deve começar com um "`"/" (slash) and end with a "/"`". As barras de início e fim contam como parte do limite de 256 carateres.

Informações relacionadas

Criando mapeamentos de links simbólicos para compartilhamentos SMB

Controle anúncios DFS automáticos no ONTAP com uma opção de servidor CIFS

Uma opção de servidor CIFS controla como os recursos do DFS são anunciados para clientes SMB ao se conetar a compartilhamentos. Como o ONTAP usa referências DFS

quando os clientes acessam links simbólicos sobre o SMB, você deve estar ciente do impactos ao desativar ou ativar essa opção.

Uma opção de servidor CIFS determina se os servidores CIFS anunciam automaticamente que são capazes de DFS para clientes SMB. Por padrão, essa opção está ativada e o servidor CIFS sempre anuncia que é capaz de DFS para clientes SMB (mesmo quando se coneta a compartilhamentos onde o acesso a links simbólicos está desativado). Se você quiser que o servidor CIFS anuncie que ele é capaz de clientes somente quando eles estão se conetando a compartilhamentos onde o acesso a links simbólicos está ativado, você pode desativar essa opção.

Você deve estar ciente do que acontece quando essa opção está desativada:

- As configurações de compartilhamento para links simbólicos não são alteradas.
- Se o parâmetro share estiver definido para permitir acesso a links simbólicos (acesso de leitura e gravação ou acesso somente leitura), o servidor CIFS anuncia recursos DFS aos clientes que se conetam a esse compartilhamento.

  As conexões do cliente e o acesso a links simbólicos continuam sem interrupção.

- Se o parâmetro share estiver definido para não permitir acesso a links simbólicos (desabilitando o acesso ou se o valor do parâmetro share for nulo), o servidor CIFS não anunciará recursos DFS aos clientes que se conetam a esse compartilhamento.

  Como os clientes têm informações em cache que o servidor CIFS é capaz de DFS e não está mais anunciando que são, os clientes que estão conetados a compartilhamentos onde o acesso a links simbólicos está desativado podem não ser capazes de acessar esses compartilhamentos depois que a opção do servidor CIFS é desativada. Depois que a opção estiver desativada, talvez seja necessário reinicializar os clientes que estão conetados a esses compartilhamentos, limpando assim as informações em cache.

Essas alterações não se aplicam às conexões SMB 1,0.

Configurar o suporte a links simbólicos UNIX em compartilhamentos SMB

Você pode configurar o suporte a links simbólicos UNIX em compartilhamentos SMB especificando uma configuração de propriedade de compartilhamento de link simbólico ao criar compartilhamentos SMB ou a qualquer momento modificando compartilhamentos SMB existentes. O suporte a links simbólicos UNIX está habilitado por padrão. Você também pode desativar o suporte a links simbólicos UNIX em um compartilhamento.

Sobre esta tarefa

Ao configurar o suporte a links simbólicos UNIX para compartilhamentos SMB, você pode escolher uma das seguintes configurações:

Definição	Descrição
`enable` (OBSOLETO*)	Especifica que links simbólicos estão habilitados para acesso de leitura e gravação.

Definição	Descrição
`read_only` (OBSOLETO*)	Especifica que os links simbólicos estão ativados para acesso somente leitura. Esta definição não se aplica a widelinks. O acesso à Widelink é sempre leitura-escrita.
`hide` (OBSOLETO*)	Especifica que os clientes SMB são impedidos de ver links simbólicos.
`no-strict-security`	Especifica que os clientes seguem links simbólicos fora dos limites de compartilhamento.
`symlinks`	Especifica que os links simbólicos são ativados localmente para acesso de leitura e gravação. Os anúncios DFS não são gerados mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `true`. Esta é a configuração padrão.
`symlinks-and-widelinks`	Especifica que os links simbólicos locais e os widelinks para acesso de leitura e gravação. Os anúncios DFS são gerados para links simbólicos locais e widelinks, mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `false`.
`disable`	Especifica que links simbólicos e widelinks estão desativados. Os anúncios DFS não são gerados mesmo que a opção CIFS `is-advertise-dfs-enabled` esteja definida como `true`.
`""` (nulo, não definido)	Desativa links simbólicos no compartilhamento.
– (não definido)	Desativa links simbólicos no compartilhamento.

*Os parâmetros *enable*, *hide* e *read-only* são obsoletos e podem ser removidos em uma versão futura do ONTAP.

Passos

1. Configure ou desative o suporte a links simbólicos:

Se for…	Digite…
Um novo compartilhamento SMB	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only

Se for…	Digite…
""	-
symlinks	symlinks-and-widelinks
disable},…]+`	Um compartilhamento SMB existente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},…]+`

2. Verifique se a configuração do compartilhamento SMB está correta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

Exemplo

O comando a seguir cria um compartilhamento SMB chamado "d.ATA1" com a configuração de link simbólico UNIX definida como `enable`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
               Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

Informações relacionadas

Criando mapeamentos de links simbólicos para compartilhamentos SMB

Crie mapeamentos de links simbólicos para compartilhamentos SMB

Você pode criar mapeamentos de links simbólicos UNIX para compartilhamentos SMB. Você pode criar um link simbólico relativo, que se refere ao arquivo ou pasta relativa à sua pasta pai, ou você pode criar um link simbólico absoluto, que se refere ao arquivo ou pasta usando um caminho absoluto.

Sobre esta tarefa

Os Winelinks não são acessíveis a partir de clientes Mac os X se você usar SMB 2.x. Quando um usuário tenta se conetar a um compartilhamento usando widelinks de um cliente Mac os X, a tentativa falha. No entanto, você pode usar widelinks com clientes Mac os X se você usar SMB 1.

Passos

1. Para criar mapeamentos de links simbólicos para compartilhamentos SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` Especifica o nome da máquina virtual de storage (SVM).

   `-unix-path path` Especifica o caminho UNIX. O caminho UNIX deve começar com uma barra (`/`) e deve terminar com uma barra (`/`).

   `-share-name share_name` Especifica o nome do compartilhamento SMB para mapear.

   `-cifs-path path` Especifica o caminho CIFS. O caminho CIFS deve começar com uma barra (`/`) e deve terminar com uma barra (`/`).

   `-cifs-server server_name` Especifica o nome do servidor CIFS. O nome do servidor CIFS pode ser especificado como um nome DNS (por exemplo, mynetwork.cifs.server.com), endereço IP ou nome NetBIOS. O nome NetBIOS pode ser determinado usando o `vserver cifs show` comando. Se este parâmetro opcional não for especificado, o valor padrão será o nome NetBIOS do servidor CIFS local.

   `-locality local|free|widelink`especifica se deseja criar um link local, um link gratuito ou um link simbólico amplo. Um link simbólico local mapeia para o compartilhamento SMB local. Um link simbólico gratuito pode mapear qualquer lugar no servidor SMB local. Um link simbólico amplo mapeia para qualquer compartilhamento SMB na rede. Se não especificar este parâmetro opcional, o valor predefinido é `local.

   `-home-directory true false`especifica se o compartilhamento de destino é um diretório home. Mesmo que esse parâmetro seja opcional, você deve definir esse parâmetro para `true` quando o compartilhamento de destino for configurado como um diretório inicial. A predefinição é `false`.

Exemplo

O comando a seguir cria um mapeamento de link simbólico no SVM chamado VS1. Ele tem o caminho UNIX `/src/` , o nome de compartilhamento SMB "'SOURCE'", o caminho CIFS `/mycompany/source/` e o

endereço IP do servidor CIFS 123.123.123.123, e é um widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

Informações relacionadas

Configurando o suporte a links simbólicos UNIX em compartilhamentos SMB

Comandos para gerenciar mapeamentos de links simbólicos

Existem comandos ONTAP específicos para gerenciar mapeamentos de links simbólicos.

Se você quiser…	Use este comando…
Crie um mapeamento de link simbólico	`vserver cifs symlink create`
Exibir informações sobre mapeamentos de links simbólicos	`vserver cifs symlink show`
Modifique um mapeamento de link simbólico	`vserver cifs symlink modify`
Excluir um mapeamento de link simbólico	`vserver cifs symlink delete`

Consulte a página de manual de cada comando para obter mais informações.

Aplicativos de backup do Windows e links simbólicos em estilo Unix

Quando um aplicativo de backup executado no Windows encontra um link simbólico (link simbólico) estilo Unix, o link é seguido e os dados são copiados. Começando com ONTAP 9.15,1, você tem a opção de fazer backup dos links simbólicos em vez dos dados. Esse recurso é totalmente compatível com FlexGroups e FlexVols da ONTAP.

Visão geral

Antes de alterar a forma como o ONTAP lida com links simbólicos durante uma operação de backup do Windows, você deve estar familiarizado com os benefícios, os principais conceitos e as opções de configuração.

Benefícios

Quando esse recurso está desativado ou indisponível, cada link simbólico é percorrido e os dados aos quais ele se vincula são copiados. Por causa disso, dados desnecessários podem às vezes ser copiados e, em certas situações, o aplicativo pode acabar em um loop. Ao invés disso, fazer backup dos links simbólicos evita esses problemas. E como os arquivos de link simbólico são muito pequenos em comparação com os dados na maioria dos casos, os backups levam menos tempo para serem concluídos. O desempenho geral do cluster também pode melhorar devido à redução das operações de e/S.

Ambiente de servidor Windows

Este recurso é compatível com aplicativos de backup executados no Windows. Você deve entender os aspetos técnicos relevantes do ambiente antes de usá-lo.

Atributos estendidos

O Windows suporta atributos estendidos (EA) que formam coletivamente metadados adicionais associados opcionalmente aos arquivos. Esses atributos são usados por vários aplicativos, como o subsistema do Windows para Linux, conforme descrito em "Permissões de arquivo para WSL". Os aplicativos podem solicitar atributos estendidos para cada arquivo ao ler dados do ONTAP.

Os links simbólicos são retornados nos atributos estendidos quando o recurso é ativado. Portanto, um aplicativo de backup deve fornecer suporte padrão EA, que é usado para armazenar os metadados. Alguns utilitários do Windows suportam e preservam os atributos estendidos. No entanto, se o software de backup não suportar backup e restauração dos atributos estendidos, ele não preservará os metadados associados a cada arquivo e não processará os links simbólicos corretamente.

Configuração do Windows

Os aplicativos de backup executados em um servidor Microsoft Windows podem receber um privilégio especial, permitindo que eles ignorem a segurança normal de arquivos. Isso geralmente é feito adicionando os aplicativos ao grupo operadores de backup. Os aplicativos podem então fazer backup e restaurar arquivos conforme necessário, bem como executar outras operações relacionadas ao sistema. Há alterações sutis no protocolo SMB usado pelos aplicativos de backup que podem ser detetadas pelo ONTAP à medida que os dados são lidos e gravados.

Requisitos

O recurso de backup de link simbólico tem vários requisitos, incluindo:

- O cluster está executando o ONTAP 9.15,1 ou posterior.
- Um aplicativo de backup do Windows que recebeu Privileges de backup especial.
- O aplicativo de backup também deve dar suporte a atributos estendidos e solicitá-los durante as operações de backup.
- O recurso de backup de link simbólico do ONTAP está habilitado para o SVM de dados aplicável.

Opções de configuração

Além da CLI do ONTAP, você também pode gerenciar esse recurso usando a API REST. Consulte "Novidades com a API REST e a automação do ONTAP" para obter mais informações. A configuração que determina como o ONTAP processa os links simbólicos em estilo Unix deve ser executada separadamente para cada SVM.

Ative o recurso de backup de link simbólico no ONTAP

Uma opção de configuração foi introduzida a um comando CLI existente com ONTAP 9.15,1. Você pode usar essa opção para ativar ou desativar o processamento de link simbólico estilo Unix.

Antes de começar

Reveja o básico Requisitos. Além disso:

- Ser capaz de elevar seu privilégio CLI para o nível avançado.
- Determine os dados SVM que você deseja modificar. O SVM `vs1` é usado no comando exemplo.

Passos

1. Defina o nível de privilégio avançado.

```
set privilege advanced
```

2. Habilite o backup de arquivos de link simbólico.

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

Use BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma filial

Use o BranchCache para armazenar em cache conteúdo de compartilhamento SMB em uma visão geral de filiais

BranchCache foi desenvolvido pela Microsoft para permitir o armazenamento em cache de conteúdo em computadores locais para clientes solicitantes. A implementação do ONTAP do BranchCache pode reduzir a utilização da rede de área ampla (WAN) e fornecer um melhor tempo de resposta de acesso quando os usuários de uma filial acessam conteúdo armazenado em máquinas virtuais de armazenamento (SVMs) usando SMB.

Se você configurar o BranchCache, os clientes do Windows BranchCache primeiro recuperam o conteúdo do SVM e, em seguida, armazenam o conteúdo em um computador dentro da filial. Se outro cliente habilitado para BranchCache na filial solicitar o mesmo conteúdo, o SVM autentica e autoriza o usuário solicitante. Em seguida, o SVM determina se o conteúdo em cache ainda está atualizado e, se estiver, envia os metadados do cliente sobre o conteúdo em cache. O cliente então usa os metadados para recuperar conteúdo diretamente do cache baseado localmente.

Informações relacionadas

Usando arquivos off-line para permitir o armazenamento em cache de arquivos para uso off-line

Requisitos e diretrizes

Suporte à versão BranchCache

Você deve estar ciente de quais versões do BranchCache o ONTAP suporta.

O ONTAP oferece suporte ao BranchCache 1 e ao BranchCache 2 aprimorado:

- Ao configurar o BranchCache no servidor SMB para a máquina virtual de armazenamento (SVM), você pode habilitar o BranchCache 1, o BranchCache 2 ou todas as versões.

  Por padrão, todas as versões estão ativadas.

- Se você ativar apenas o BranchCache 2, as máquinas cliente Windows do escritório remoto devem suportar o BranchCache 2.

  Somente clientes SMB 3,0 ou posteriores suportam BranchCache 2.

Para obter mais informações sobre as versões do BranchCache, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos de suporte ao protocolo de rede

Você deve estar ciente dos requisitos de protocolo de rede para implementar o ONTAP BranchCache.

Você pode implementar o recurso ONTAP BranchCache em redes IPv4 e IPv6 usando SMB 2,1 ou posterior.

Todos os servidores CIFS e máquinas de filiais que participam da implementação do BranchCache devem ter o protocolo SMB 2,1 ou posterior ativado. O SMB 2,1 tem extensões de protocolo que permitem que um cliente participe de um ambiente BranchCache. Esta é a versão mínima do protocolo SMB que oferece suporte ao BranchCache. O SMB 2,1 suporta a versão BranchCache 1.

Se você quiser usar o BranchCache versão 2, o SMB 3,0 é a versão mínima suportada. Todos os servidores CIFS e máquinas de filiais que participam de uma implementação BranchCache 2 devem ter o SMB 3,0 ou posterior habilitado.

Se você tiver escritórios remotos onde alguns dos clientes suportam apenas o SMB 2,1 e alguns dos clientes suportam o SMB 3,0, você pode implementar uma configuração BranchCache no servidor CIFS que fornece suporte de cache tanto no BranchCache 1 quanto no BranchCache 2.

Embora o recurso Microsoft BranchCache suporte ao uso dos protocolos HTTP/HTTPS e SMB como protocolos de acesso a arquivos, o ONTAP BranchCache só suporta o uso de SMB.

O ONTAP e o Windows hosts requisitos de versão

Os hosts do ONTAP e da filial do Windows devem atender a certos requisitos de versão antes de poder configurar o BranchCache.

Antes de configurar o BranchCache, você deve garantir que a versão do ONTAP no cluster e clientes de filiais participantes ofereçam suporte ao SMB 2,1 ou posterior e ofereça suporte ao recurso BranchCache. Se você configurar o modo Cache hospedado, você também deve garantir que você use um host suportado para o servidor de cache.

O BranchCache 1 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: Máquina virtual de storage (SVM) com ONTAP
- Servidor de cache: Windows Server 2008 R2 ou Windows Server 2012 ou posterior
- Peer ou cliente: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 ou posterior

O BranchCache 2 é compatível com as seguintes versões do ONTAP e hosts do Windows:

- Servidor de conteúdo: SVM com ONTAP
- Servidor de cache: Windows Server 2012 ou posterior
- Peer ou cliente: Windows 8 ou Windows Server 2012 ou posterior

Razões pelas quais o ONTAP invalida hashes do BranchCache

Entender as razões pelas quais o ONTAP invalida hashes pode ser útil ao Planejar sua configuração do BranchCache. Ele pode ajudá-lo a decidir qual modo de operação você deve configurar e pode ajudá-lo a escolher em quais compartilhamentos ativar o BranchCache.

O ONTAP deve gerenciar hashes do BranchCache para garantir que os hashes sejam válidos. Se um hash não for válido, o ONTAP invalida o hash e computa um novo hash na próxima vez que o conteúdo for solicitado, supondo que o BranchCache ainda esteja habilitado.

O ONTAP invalida hashes pelos seguintes motivos:

- A chave do servidor é modificada.

  Se a chave do servidor for modificada, o ONTAP invalida todos os hashes no armazenamento de hash.

- Um hash é removido do cache porque o tamanho máximo do armazenamento de hash BranchCache foi atingido.

  Este é um parâmetro sintonizável e pode ser modificado para atender aos requisitos da sua empresa.

- Um arquivo é modificado por meio do acesso SMB ou NFS.
- Um arquivo para o qual há hashes computados é restaurado usando o `snap restore` comando.
- Um volume que contém compartilhamentos SMB habilitados para BranchCache é restaurado usando o `snap restore` comando.

Diretrizes para escolher o local de armazenamento de hash

Ao configurar o BranchCache, você escolhe onde armazenar hashes e qual tamanho o armazenamento de hash deve ser. Entender as diretrizes ao escolher o local e o tamanho do armazenamento de hash pode ajudá-lo a Planejar sua configuração do BranchCache em um SVM habilitado para CIFS.

- Você deve localizar o armazenamento de hash em um volume onde atualizações de tempo são permitidas.

  O tempo de acesso em um arquivo hash é usado para manter os arquivos acessados com frequência no armazenamento de hash. Se as atualizações do atime estiverem desativadas, a hora de criação será usada para esse fim. É preferível usar o tempo para rastrear arquivos usados com frequência.

- Não é possível armazenar hashes em sistemas de arquivos somente leitura, como destinos SnapMirror e volumes SnapLock.
- Se o tamanho máximo do armazenamento de hash for atingido, os hashes mais antigos serão lavados para abrir espaço para novos hashes.

  Você pode aumentar o tamanho máximo do armazenamento de hash para reduzir a quantidade de hashes que são lavados do cache.

- Se o volume no qual você armazena hashes estiver indisponível ou cheio, ou se houver um problema com a comunicação intra-cluster em que o serviço BranchCache não pode recuperar informações de hash, os serviços BranchCache não estarão disponíveis.

O volume pode estar indisponível porque está offline ou porque o administrador de armazenamento especificou um novo local para o armazenamento de hash.

Isso não causa problemas com acesso a arquivos. Se o acesso ao armazenamento de hash for impedido, o ONTAP retornará um erro definido pela Microsoft ao cliente, o que faz com que o cliente solicite o arquivo usando a solicitação de leitura normal de SMB.

Informações relacionadas

Configure o BranchCache no servidor SMB

Modifique a configuração do BranchCache

Recomendações do BranchCache

Antes de configurar o BranchCache, há certas recomendações que você deve ter em mente ao decidir quais compartilhamentos SMB você deseja ativar o armazenamento em cache do BranchCache.

Você deve ter em mente as seguintes recomendações ao decidir em qual modo de operação usar e em quais compartilhamentos SMB para ativar o BranchCache:

- Os benefícios do BranchCache são reduzidos quando os dados a serem armazenados remotamente em cache são alterados com frequência.
- Os serviços BranchCache são benéficos para compartilhamentos que contêm conteúdo de arquivo que é reutilizado por vários clientes de escritório remoto ou por conteúdo de arquivo que é repetidamente acessado por um único usuário remoto.
- Considere ativar o armazenamento em cache para conteúdo somente leitura, como dados em cópias Snapshot e destinos SnapMirror.

Configurar BranchCache

Configurar visão geral do BranchCache

Você configura o BranchCache no servidor SMB usando comandos ONTAP. Para implementar o BranchCache, você também deve configurar seus clientes e, opcionalmente, seus servidores de cache hospedados nas filiais onde você deseja armazenar conteúdo em cache.

Se você configurar o BranchCache para habilitar o armazenamento em cache de forma compartilhada, você deverá habilitar o BranchCache nos compartilhamentos SMB para os quais deseja fornecer serviços de armazenamento em cache do BranchCache.

Requisitos para configurar o BranchCache

Depois de atender a alguns pré-requisitos, você pode configurar o BranchCache.

Antes de configurar o BranchCache no servidor CIFS para sua SVM, você precisa atender aos requisitos a seguir:

- O ONTAP deve ser instalado em todos os nós do cluster.
- O CIFS deve ser licenciado e um servidor SMB deve ser configurado. A licença SMB está incluída no

"ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

- A conetividade de rede IPv4G ou IPv6G deve ser configurada.
- Para BranchCache 1, o SMB 2,1 ou posterior deve estar ativado.
- Para BranchCache 2, o SMB 3,0 deve estar ativado e os clientes remotos do Windows devem suportar o BranchCache 2.

Configure o BranchCache no servidor SMB

Você pode configurar o BranchCache para fornecer serviços do BranchCache por compartilhamento. Como alternativa, você pode configurar o BranchCache para ativar automaticamente o cache em todos os compartilhamentos SMB.

Sobre esta tarefa

Você pode configurar o BranchCache em SVMs.

- Você pode criar uma configuração BranchCache de todos os compartilhamentos se quiser oferecer serviços de cache para todo o conteúdo contido em todos os compartilhamentos SMB no servidor CIFS.
- Você pode criar uma configuração de BranchCache por compartilhamento se quiser oferecer serviços de cache para conteúdo contido em compartilhamentos SMB selecionados no servidor CIFS.

Você deve especificar os seguintes parâmetros ao configurar o BranchCache:

Parâmetros necessários	Descrição
Nome da SVM	O BranchCache é configurado por SVM. Você deve especificar em qual SVM habilitado para CIFS deseja configurar o serviço BranchCache.
Path to hash store	Os hashes do BranchCache são armazenados em arquivos regulares no volume SVM. Você deve especificar o caminho para um diretório existente onde você deseja que o ONTAP armazene os dados de hash.o caminho de hash do BranchCache deve ser lido-gravável. Caminhos somente leitura, como diretórios Snapshot, não são permitidos. Você pode armazenar dados de hash em um volume que contém outros dados ou pode criar um volume separado para armazenar dados de hash. Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres. O caminho hash pode conter espaços em branco e quaisquer carateres de nome de arquivo válidos.

Opcionalmente, você pode especificar os seguintes parâmetros:

Parâmetros opcionais	Descrição
Versões suportadas	ONTAP suporta BranchCache 1 e 2. Pode ativar a versão 1, a versão 2 ou ambas as versões. O padrão é ativar ambas as versões.
Tamanho máximo do armazenamento de hash	Você pode especificar o tamanho a ser usado para o armazenamento de dados de hash. Se os dados de hash excederem esse valor, o ONTAP excluirá hashes mais antigos para abrir espaço para hashes mais recentes. O tamanho padrão para o armazenamento de hash é de 1 GB. O BranchCache funciona de forma mais eficiente se os hashes não forem descartados de forma excessivamente agressiva. Se você determinar que hashes são descartados frequentemente porque o armazenamento de hash está cheio, você pode aumentar o tamanho do armazenamento de hash modificando a configuração BranchCache.
Chave do servidor	Você pode especificar uma chave de servidor que o serviço BranchCache usa para impedir que os clientes personificem o servidor BranchCache. Se você não especificar uma chave de servidor, uma será gerada aleatoriamente quando você criar a configuração BranchCache. Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor. Se a chave do servidor contiver espaços, você deverá inserir a chave do servidor entre aspas.
Modo de funcionamento	O padrão é habilitar o BranchCache por compartilhamento. • Para criar uma configuração do BranchCache na qual você habilite o BranchCache por compartilhamento, não é possível especificar esse parâmetro opcional ou especificar `per-share`. • Para ativar automaticamente o BranchCache em todos os compartilhamentos, você deve definir o modo operacional como `all-shares`.

Passos

1. Habilite o SMB 2,1 e 3,0 conforme necessário:
   a. Defina o nível de privilégio como avançado: `set -privilege advanced`
   b. Verifique as configurações configuradas do SVM SMB para determinar se todas as versões

necessárias do SMB estão ativadas: `vserver cifs options show -vserver vserver_name`

c. Se necessário, ative o SMB 2,1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

   O comando habilita o SMB 2,0 e o SMB 2,1.

d. Se necessário, ative o SMB 3,0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`

e. Voltar ao nível de privilégio de administrador: `set -privilege admin`

2. Configurar BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

   O caminho de storage de hash especificado deve existir e residir em um volume gerenciado pela SVM. O caminho também deve estar localizado em um volume gravável de leitura. O comando falha se o caminho for somente leitura ou não existir.

   Se você quiser usar a mesma chave de servidor para configurações adicionais do SVM BranchCache, Registre o valor inserido para a chave de servidor. A chave do servidor não aparece quando você exibe informações sobre a configuração do BranchCache.

3. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplos

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados e configuram o BranchCache para habilitar automaticamente o armazenamento em cache em todos os compartilhamentos SMB no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

Os comandos a seguir verificam se o SMB 2,1 e o 3,0 estão ativados, configuram o BranchCache para habilitar o armazenamento em cache por compartilhamento no SVM VS1 e verificam a configuração do BranchCache:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informações relacionadas

Requisitos e diretrizes: Suporte à versão BranchCache

Onde encontrar informações sobre como configurar o BranchCache no escritório remoto

Crie um compartilhamento SMB habilitado para BranchCache

Ative o BranchCache em um compartilhamento SMB existente

Modifique a configuração do BranchCache

Desative a visão geral de BranchCache na SMB shares

Exclua a configuração BranchCache em SVMs

Onde encontrar informações sobre como configurar o BranchCache no escritório remoto

Depois de configurar o BranchCache no servidor SMB, você deve instalar e configurar o BranchCache em computadores clientes e, opcionalmente, em servidores de cache em seu escritório remoto. A Microsoft fornece instruções para configurar o BranchCache no escritório remoto.

Instruções para configurar clientes de filiais e, opcionalmente, colocar em cache servidores para usar o BranchCache estão no site do Microsoft BranchCache.

"Microsoft BranchCache Docs: O que há de novo"

Configurar compartilhamentos SMB habilitados para BranchCache

Configure a visão geral de compartilhamentos SMB habilitados para BranchCache

Depois de configurar o BranchCache no servidor SMB e na filial, você pode habilitar o BranchCache em compartilhamentos SMB que contenham conteúdo que você deseja permitir que os clientes nas filiais armazenem cache.

O cache BranchCache pode ser ativado em todos os compartilhamentos SMB no servidor SMB ou em uma base de compartilhamento por compartilhamento.

- Se você ativar o BranchCache de forma compartilhada, poderá ativar o BranchCache à medida que você cria o compartilhamento ou modificando compartilhamentos existentes.

  Se você habilitar o armazenamento em cache em um compartilhamento SMB existente, o ONTAP começará a computar hashes e enviar metadados para clientes solicitando conteúdo assim que você ativar o BranchCache nesse compartilhamento.

- Quaisquer clientes que tenham uma conexão SMB existente a um compartilhamento não recebem suporte do BranchCache se o BranchCache for posteriormente habilitado nesse compartilhamento.

  O ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconetar e se reconetar para usar o conteúdo em cache para esse compartilhamento.

> Se o BranchCache em um compartilhamento SMB for posteriormente desativado, o ONTAP interrompe o envio de metadados para o cliente solicitante. Um cliente que precisa de dados recupera-os diretamente do servidor de conteúdo (servidor SMB).

Crie um compartilhamento SMB habilitado para BranchCache

Você pode ativar o BranchCache em um compartilhamento SMB ao criar o compartilhamento definindo a `branchcache` propriedade compartilhar.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

  Esta é a configuração padrão quando você cria um compartilhamento.

- Você também pode especificar parâmetros opcionais adicionais de compartilhamento quando você cria o compartilhamento habilitado para BranchCache.
- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

  No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o

BranchCache no SVM.

- Como não há propriedades de compartilhamento padrão aplicadas ao compartilhamento quando você usa o `-share-properties` parâmetro, você deve especificar todas as outras propriedades de compartilhamento que deseja aplicar ao compartilhamento além da `branchcache` propriedade de compartilhamento usando uma lista delimitada por vírgulas.
- Para obter mais informações, consulte a página man para o `vserver cifs share create` comando.

Passo

1. Crie um compartilhamento SMB habilitado para BranchCache
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties branchcache[,…]`
2. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB usando o `vserver cifs share show` comando.

Exemplo

O comando a seguir cria um compartilhamento SMB habilitado para BranchCache chamado "data" com um caminho de `/data` no SVM VS1. Por padrão, a configuração arquivos off-line é definida como `manual`:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
              Share Properties: branchcache
                                oplocks
                                browsable
                                changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informações relacionadas

Desativar BranchCache em um único compartilhamento SMB

Ative o BranchCache em um compartilhamento SMB existente

Você pode ativar o BranchCache em um compartilhamento SMB existente adicionando a

`branchcache` propriedade share à lista existente de propriedades de compartilhamento.

Sobre esta tarefa

- Se o BranchCache estiver ativado no compartilhamento SMB, o compartilhamento deve ter a configuração de arquivos off-line definida como cache manual.

  Se a configuração arquivos offline do compartilhamento existente não estiver definida como armazenamento manual em cache, você deverá configurá-lo modificando o compartilhamento.

- Você pode definir a `branchcache` propriedade em um compartilhamento, mesmo que o BranchCache não esteja configurado e habilitado na máquina virtual de storage (SVM).

  No entanto, se você quiser que o compartilhamento ofereça conteúdo em cache, configure e ative o BranchCache no SVM.

- Quando você adiciona a `branchcache` propriedade de compartilhamento ao compartilhamento, as configurações de compartilhamento existentes e as propriedades de compartilhamento são preservadas.

  A propriedade de compartilhamento BranchCache é adicionada à lista existente de propriedades de compartilhamento. Para obter mais informações sobre como usar o `vserver cifs share properties add` comando, consulte as páginas de manual.

Passos

1. Se necessário, configure a configuração de compartilhamento de arquivos offline para cache manual:
   a. Determine qual é a configuração de compartilhamento de arquivos off-line usando o `vserver cifs share show` comando.
   b. Se a definição de partilha de ficheiros offline não estiver definida para manual, altere-a para o valor pretendido: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Ativar BranchCache em um compartilhamento SMB existente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verifique se a propriedade BranchCache Share está definida no compartilhamento SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

Exemplo

O comando a seguir habilita o BranchCache em um compartilhamento SMB existente chamado "ata2" com um caminho `/data2` de no SVM VS1:

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Desativar BranchCache em um único compartilhamento SMB

Gerencie e monitore a configuração do BranchCache

Modifique as configurações do BranchCache

Você pode modificar a configuração do serviço BranchCache em SVMs, incluindo alterar o caminho do diretório de armazenamento de hash, o tamanho máximo do diretório de armazenamento de hash, o modo operacional e quais versões do BranchCache são suportadas. Você também pode aumentar o tamanho do volume que contém o armazenamento de hash.

Passos

1. Execute a ação apropriada:

Se você quiser…	Digite o seguinte…
Modifique o tamanho do diretório de armazenamento de hash	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
Aumente o tamanho do volume que contém o armazenamento de hash	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` Se o volume que contém o armazenamento de hash for preenchido, você poderá aumentar o tamanho do volume. Você pode especificar o novo tamanho de volume como um número seguido de uma designação de unidade. Saiba mais sobre "Gerenciamento de volumes do FlexVol"	Modifique o caminho do diretório de armazenamento de hash

Se você quiser…	Digite o seguinte…
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` Se o SVM for uma fonte de recuperação de desastres SVM, o caminho hash não poderá estar no volume raiz. Isso ocorre porque o volume raiz não é replicado para o destino de recuperação de desastres. O caminho hash BranchCache pode conter espaços em branco e quaisquer carateres de nome de arquivo válidos. Se você modificar o caminho de hash, `-flush -hashes` é um parâmetro obrigatório que especifica se você deseja que o ONTAP lave os hashes do local de armazenamento de hash original. Pode definir os seguintes valores para o `-flush -hashes` parâmetro: **Se você especificar `true`, o ONTAP excluirá os hashes no local original e criará novos hashes no novo local à medida que novas solicitações forem feitas por clientes habilitados para BranchCache.** Se você especificar `false`, os hashes não serão lavados. + Nesse caso, você pode optar por reutilizar os hashes existentes mais tarde alterando o caminho de armazenamento de hash de volta para o local original.
Altere o modo de funcionamento	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` Ao modificar o modo de funcionamento, deve estar ciente do seguinte: **O ONTAP anuncia o suporte do BranchCache para um compartilhamento quando a sessão SMB está configurada.** Os clientes que já tiverem sessões estabelecidas quando o BranchCache estiver habilitado precisam se desconetar e se reconetar para usar o conteúdo em cache para esse compartilhamento.
Altere o suporte à versão do BranchCache	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. Verifique as alterações de configuração usando o `vserver cifs branchcache show` comando.

Exibir informações sobre configurações do BranchCache

Você pode exibir informações sobre as configurações do BranchCache em máquinas virtuais de armazenamento (SVMs), que podem ser usadas ao verificar uma configuração ou ao determinar as configurações atuais antes de modificar uma configuração.

Passo

1. Execute uma das seguintes ações:

Se você quiser exibir…	Digite este comando…
Informações resumidas sobre as configurações do BranchCache em todos os SVMs	`vserver cifs branchcache show`
Informações detalhadas sobre a configuração em uma SVM específica	`vserver cifs branchcache show -vserver` *`vserver_name`*

Exemplo

O exemplo a seguir exibe informações sobre a configuração BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
           Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
           Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
         CIFS BranchCache Operating Modes: per_share
```

Altere a chave do servidor BranchCache

Você pode alterar a chave do servidor BranchCache modificando a configuração BranchCache na máquina virtual de armazenamento (SVM) e especificando uma chave de servidor diferente.

Sobre esta tarefa

Você pode definir a chave do servidor para um valor específico para que, se vários servidores estiverem fornecendo dados do BranchCache para os mesmos arquivos, os clientes possam usar hashes de qualquer servidor usando essa mesma chave do servidor.

Quando você altera a chave do servidor, você também deve lavar o cache hash. Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passos

1. Altere a chave do servidor usando o seguinte comando: `vserver cifs branchcache modify`

`-vserver vserver_name -server-key text -flush-hashes true`

Ao configurar uma nova chave de servidor, você também deve especificar `-flush-hashes` e definir o valor como `true`.

2. Verifique se a configuração BranchCache está correta usando o `vserver cifs branchcache show` comando.

Exemplo

O exemplo a seguir define uma nova chave de servidor que contém espaços e limpa o cache de hash no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Informações relacionadas

Razões pelas quais o ONTAP invalida hashes do BranchCache

O BranchCache pré-computar hashes em caminhos especificados

Você pode configurar o serviço BranchCache para pré-calcular hashes para um único arquivo, para um diretório ou para todos os arquivos em uma estrutura de diretório. Isso pode ser útil se você quiser calcular hashes de dados em um compartilhamento habilitado pelo BranchCache durante horas fora do horário de pico.

Sobre esta tarefa

Se você quiser coletar uma amostra de dados antes de exibir estatísticas de hash, você deve usar os `statistics start` comandos e opcionais `statistics stop`.

- É necessário especificar a máquina virtual de storage (SVM) e o caminho no qual você deseja pré-calcular hashes.
- Você também deve especificar se deseja que os hashes sejam computados recursivamente.
- Se você quiser que os hashes sejam computados recursivamente, o serviço BranchCache percorre toda a árvore de diretórios sob o caminho especificado e calcula hashes para cada objeto elegível.

Passos

1. Pré-calcular hashes como desejado:

Se você quiser pré-calcular hashes em…	Digite o comando…
Um único arquivo ou diretório	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
Recursivamente em todos os arquivos em uma estrutura de diretório	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. Verifique se os hashes estão sendo computados usando o `statistics` comando:
   a. Exiba estatísticas para o `hashd` objeto na instância SVM desejada: `statistics show -object hashd -instance vserver_name`
   b. Verifique se o número de hashes criados está aumentando repetindo o comando.

Exemplos

O exemplo a seguir cria hashes no caminho `/data` e em todos os arquivos e subdiretórios contidos no SVM VS1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

Informações relacionadas

"Configuração do monitoramento de desempenho"

Lave os hashes do armazenamento de hash do SVM BranchCache

Você pode lavar todos os hashes armazenados em cache do armazenamento de hash BranchCache na máquina virtual de armazenamento (SVM). Isso pode ser útil se você tiver alterado a configuração BranchCache da filial. Por exemplo, se você reconfigurou recentemente o modo de armazenamento em cache de armazenamento distribuído para o modo de armazenamento em cache hospedado, você deseja limpar o armazenamento de hash.

Sobre esta tarefa

Depois de limpar os hashes, o ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Passo

1. Lave os hashes do armazenamento de hash BranchCache: `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

Exibir estatísticas do BranchCache

Você pode exibir estatísticas do BranchCache para, entre outras coisas, identificar o desempenho do cache, determinar se sua configuração está fornecendo conteúdo em cache para clientes e determinar se os arquivos hash foram excluídos para dar espaço aos dados de hash mais recentes.

Sobre esta tarefa

O `hashd` objeto estatístico contém contadores que fornecem informações estatísticas sobre hashes BranchCache. O `cifs` objeto estatístico contém contadores que fornecem informações estatísticas sobre a atividade relacionada ao BranchCache. Você pode coletar e exibir informações sobre esses objetos no nível avançado de privilégios.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. Exiba os contadores relacionados ao BranchCache usando o `statistics catalog counter show` comando.

   Para obter mais informações sobre contadores de estatísticas, consulte a página de manual deste comando.

   ```

   ```

```
cluster1::*> statistics catalog counter show -object hashd

Object: hashd
    Counter                     Description
    --------------------------
-------------------------------------------
    branchcache_hash_created    Number of times a request to generate
                                BranchCache hash for a file succeeded.
    branchcache_hash_files_replaced
                                Number of times a BranchCache hash file
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
```

```
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
                                data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                requesting hashes.
    branchcache_missing_hash_bytes
                                Total number of bytes of data that had
to be
                                read by the client because the hash for
that
                                content was not available on the server.
    ....Output truncated....
```

3. Colete estatísticas relacionadas ao BranchCache usando os `statistics start` comandos e. `statistics stop`

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

4. Exiba as estatísticas coletadas do BranchCache usando o `statistics show` comando.

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

5. Voltar ao nível de privilégio de administrador: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

Informações relacionadas

Exibindo estatísticas

"Configuração do monitoramento de desempenho"

Suporte para objetos de Diretiva de Grupo BranchCache

O ONTAP BranchCache fornece suporte para objetos de Diretiva de Grupo (GPOs) do

BranchCache, que permitem o gerenciamento centralizado para determinados parâmetros de configuração do BranchCache. Existem dois GPOs usados para BranchCache, a publicação Hash para BranchCache GPO e o suporte de versão Hash para BranchCache GPO.

- **Publicação Hash para o GPO BranchCache**

  A publicação Hash para BranchCache GPO corresponde ao `-operating-mode` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos de máquina virtual de armazenamento (SVM) contidos na unidade organizacional (ou) à qual a diretiva de grupo se aplica.

- **Suporte a versão Hash para o GPO BranchCache**

  O suporte de versão Hash para GPO BranchCache corresponde ao `-versions` parâmetro. Quando ocorrem atualizações de GPO, esse valor é aplicado a objetos SVM contidos na unidade organizacional à qual a diretiva de grupo se aplica.

Informações relacionadas

Aplicando objetos de Diretiva de Grupo a servidores CIFS

Exibir informações sobre os objetos de Diretiva de Grupo BranchCache

Você pode exibir informações sobre a configuração GPO (Group Policy Object) do servidor CIFS para determinar se os GPOs de BranchCache estão definidos para o domínio ao qual o servidor CIFS pertence e, em caso afirmativo, quais são as configurações permitidas. Você também pode determinar se as configurações de GPO do BranchCache são aplicadas ao servidor CIFS.

Sobre esta tarefa

Embora uma configuração de GPO seja definida dentro do domínio ao qual o servidor CIFS pertence, ela não é necessariamente aplicada à unidade organizacional (ou) que contém a máquina virtual de armazenamento (SVM) habilitada para CIFS. A configuração de GPO aplicada é o subconjunto de todos os GPOs definidos que são aplicados ao SVM habilitado para CIFS. As configurações do BranchCache aplicadas por meio de GPOs substituem as configurações aplicadas por meio da CLI.

Passos

1. Exiba a configuração de GPO BranchCache definida para o domínio do ative Directory usando o `vserver cifs group-policy show-defined` comando.

   Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. Exiba a configuração de GPO BranchCache aplicada ao servidor CIFS usando o `vserver cifs group-policy show-applied` comando. ""

> Este exemplo não exibe todos os campos de saída disponíveis para o comando. A saída é truncada.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

Informações relacionadas

Ativar ou desativar o suporte de GPO num servidor CIFS

Desativar BranchCache em compartilhamentos SMB

Desative a visão geral de BranchCache na SMB shares

Se você não quiser fornecer serviços de armazenamento em cache BranchCache em determinados compartilhamentos SMB, mas talvez queira fornecer serviços de armazenamento em cache nesses compartilhamentos posteriormente, você pode desativar o BranchCache de forma compartilhada. Se você tiver o BranchCache configurado para oferecer armazenamento em cache em todos os compartilhamentos, mas quiser desativar temporariamente todos os serviços de armazenamento em cache, você pode modificar a configuração do BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos.

Se o BranchCache em um compartilhamento SMB for posteriormente desativado após a primeira ativação, o ONTAP pára de enviar metadados para o cliente solicitante. Um cliente que precisa de dados os recupera diretamente do servidor de conteúdo (servidor CIFS na máquina virtual de armazenamento (SVM)).

Informações relacionadas

Configurando compartilhamentos SMB habilitados para BranchCache

Desative o BranchCache em um único compartilhamento SMB

Se você não quiser oferecer serviços de armazenamento em cache em determinados compartilhamentos que ofereciam conteúdo em cache anteriormente, você pode desativar o BranchCache em um compartilhamento SMB existente.

Passo

1. Introduza o seguinte comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

   A propriedade BranchCache Share foi removida. Outras propriedades de compartilhamento aplicadas permanecem em vigor.

Exemplo

O comando a seguir desativa o BranchCache em um compartilhamento SMB existente chamado "ata2":

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Parar o armazenamento em cache automático em todos os compartilhamentos SMB

Se a configuração do BranchCache ativar automaticamente o armazenamento em cache em todos os compartilhamentos SMB em cada máquina virtual de storage (SVM), você poderá modificar a configuração do BranchCache para interromper o armazenamento em cache automático de conteúdo para todos os compartilhamentos SMB.

Sobre esta tarefa

Para interromper o armazenamento em cache automático em todos os compartilhamentos SMB, você altera o modo operacional BranchCache para cache por compartilhamento.

Passos

1. Configure o BranchCache para interromper o armazenamento em cache automático em todos os compartilhamentos SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verifique se a configuração do BranchCache está correta: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O comando a seguir altera a configuração BranchCache na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1 para parar o armazenamento em cache automático em todos os compartilhamentos SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

Desative ou ative o BranchCache no SVM

O que acontece quando você desativa ou rehabilita o BranchCache no servidor CIFS

Se você configurou anteriormente o BranchCache, mas não quer que os clientes da filial usem conteúdo em cache, você pode desativar o cache no servidor CIFS. Você deve estar ciente do que acontece quando você desativa o BranchCache.

Quando você desativa o BranchCache, o ONTAP não computa hashes ou envia os metadados para o cliente solicitante. No entanto, não há interrupção no acesso aos arquivos. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados para conteúdo que desejam acessar, o ONTAP responde com um erro definido pela Microsoft, que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real

armazenado na máquina virtual de storage (SVM).

Depois que o BranchCache é desativado no servidor CIFS, os compartilhamentos SMB não anunciam os recursos do BranchCache. Para acessar dados em novas conexões SMB, os clientes fazem solicitações normais de leitura SMB.

Você pode reativar o BranchCache no servidor CIFS a qualquer momento.

- Como o armazenamento de hash não é excluído quando você desabilita o BranchCache, o ONTAP pode usar os hashes armazenados ao responder a solicitações de hash depois de reativar o BranchCache, desde que o hash solicitado ainda seja válido.
- Quaisquer clientes que tenham feito conexões SMB com compartilhamentos habilitados para BranchCache durante o tempo em que o BranchCache foi desativado não recebem suporte para BranchCache se o BranchCache for posteriormente reativado.

  Isso ocorre porque o ONTAP anuncia o suporte do BranchCache para um compartilhamento no momento em que a sessão SMB é configurada. Os clientes que estabeleceram sessões para compartilhamentos habilitados para BranchCache enquanto o BranchCache foi desativado precisam se desconetar e se reconetar para usar conteúdo em cache para esse compartilhamento.

> Se você não quiser salvar o armazenamento de hash depois de desativar o BranchCache em um servidor CIFS, você pode excluí-lo manualmente. Se você rehabilitar o BranchCache, você deve garantir que o diretório de armazenamento de hash existe. Depois que o BranchCache é reativado, os compartilhamentos habilitados para BranchCache anunciam os recursos do BranchCache. O ONTAP cria novos hashes à medida que novas solicitações são feitas por clientes habilitados para BranchCache.

Desative ou ative o BranchCache

Você pode desativar o BranchCache na máquina virtual de armazenamento (SVM) alterando o modo operacional BranchCache para `disabled`. Você pode ativar o BranchCache a qualquer momento alterando o modo operacional para oferecer serviços BranchCache por compartilhamento ou automaticamente para todos os compartilhamentos.

Passos

1. Execute o comando apropriado:

Se você quiser…	Em seguida, digite o seguinte…
Desativar BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
Ativar BranchCache por partilha	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`

Se você quiser…	Em seguida, digite o seguinte…
Ative o BranchCache para todos os compartilhamentos	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. Verifique se o modo de operação BranchCache está configurado com a configuração desejada: `vserver cifs branchcache show -vserver vserver_name`

Exemplo

O exemplo a seguir desativa o BranchCache no SVM VS1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

Exclua a configuração BranchCache em SVMs

O que acontece quando você exclui a configuração BranchCache

Se você configurou o BranchCache anteriormente, mas não deseja que a máquina virtual de armazenamento (SVM) continue fornecendo conteúdo em cache, você pode excluir a configuração BranchCache no servidor CIFS. Você deve estar ciente do que acontece quando você exclui a configuração.

Quando você exclui a configuração, o ONTAP remove as informações de configuração desse SVM do cluster e interrompe o serviço BranchCache. Você pode escolher se o ONTAP deve excluir o armazenamento de hash no SVM.

A exclusão da configuração BranchCache não interrompe o acesso por clientes habilitados para BranchCache. Depois disso, quando clientes habilitados para BranchCache solicitam informações de metadados sobre conexões SMB existentes para conteúdo que já está em cache, o ONTAP responde com um erro definido pela Microsoft, o que faz com que o cliente envie uma segunda solicitação, solicitando o conteúdo real. Em resposta à solicitação de conteúdo, o servidor CIFS envia o conteúdo real armazenado no SVM

Depois que a configuração do BranchCache é excluída, compartilhamentos SMB não anunciam recursos do BranchCache. Para acessar conteúdo que não foi armazenado em cache anteriormente usando novas conexões SMB, os clientes fazem solicitações de SMB de leitura normais.

Exclua a configuração do BranchCache

O comando que você usa para excluir o serviço BranchCache na máquina virtual de armazenamento (SVM) difere dependendo se você deseja excluir ou manter hashes existentes.

Passo

1. Execute o comando apropriado:

Se você quiser…	Em seguida, digite o seguinte…
Exclua a configuração do BranchCache e exclua hashes existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
Exclua a configuração do BranchCache, mas mantenha hashes existentes	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

Exemplo

O exemplo a seguir exclui a configuração BranchCache no SVM VS1 e exclui todos os hashes existentes:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

O que acontece com BranchCache ao reverter

É importante entender o que acontece quando você reverte o ONTAP para uma versão que não suporte o BranchCache.

- Quando você reverte para uma versão do ONTAP que não suporta BranchCache, os compartilhamentos SMB não anunciam os recursos do BranchCache para clientes habilitados para BranchCache; portanto, os clientes não solicitam informações de hash.

  Em vez disso, eles solicitam o conteúdo real usando solicitações normais de leitura SMB. Em resposta à solicitação de conteúdo, o servidor SMB envia o conteúdo real armazenado na máquina virtual de storage (SVM).

- Quando um nó que hospeda um armazenamento de hash é revertido para uma versão que não suporta BranchCache, o administrador de armazenamento precisa reverter manualmente a configuração do BranchCache usando um comando que é impresso durante a reversão.

  Esse comando exclui a configuração e os hashes do BranchCache.

  Após a conclusão da reversão, o administrador de armazenamento pode excluir manualmente o diretório que continha o armazenamento de hash, se desejado.

Informações relacionadas

Excluindo a configuração BranchCache em SVMs

Melhorar o desempenho de cópia remota da Microsoft

Melhore a visão geral do desempenho de cópia remota da Microsoft

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN. A origem pode ser um servidor CIFS ou LUN, e o destino pode ser um servidor CIFS ou LUN.

Em transferências de arquivos não ODX, os dados são lidos da fonte e são transferidos pela rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

Para ambientes SMB, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam SMB 3,0 e o recurso ODX. Para ambientes SAN, essa funcionalidade só está disponível quando o cliente e o servidor de armazenamento suportam o recurso ODX. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando, ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Informações relacionadas

Melhorar o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática

"Configuração SMB para Microsoft Hyper-V e SQL Server"

Como o ODX funciona

A descarga de cópia ODX usa um mecanismo baseado em token para ler e gravar dados dentro ou entre servidores CIFS habilitados para ODX. Em vez de rotear os dados através do host, o servidor CIFS envia um pequeno token, que representa os dados, para o cliente. O cliente ODX apresenta esse token para o servidor de destino, que então pode transferir os dados representados por esse token da origem para o destino.

Quando um cliente ODX descobre que o servidor CIFS é compatível com ODX, ele abre o arquivo de origem e solicita um token do servidor CIFS. Depois de abrir o arquivo de destino, o cliente usa o token para instruir o servidor a copiar os dados diretamente da origem para o destino.

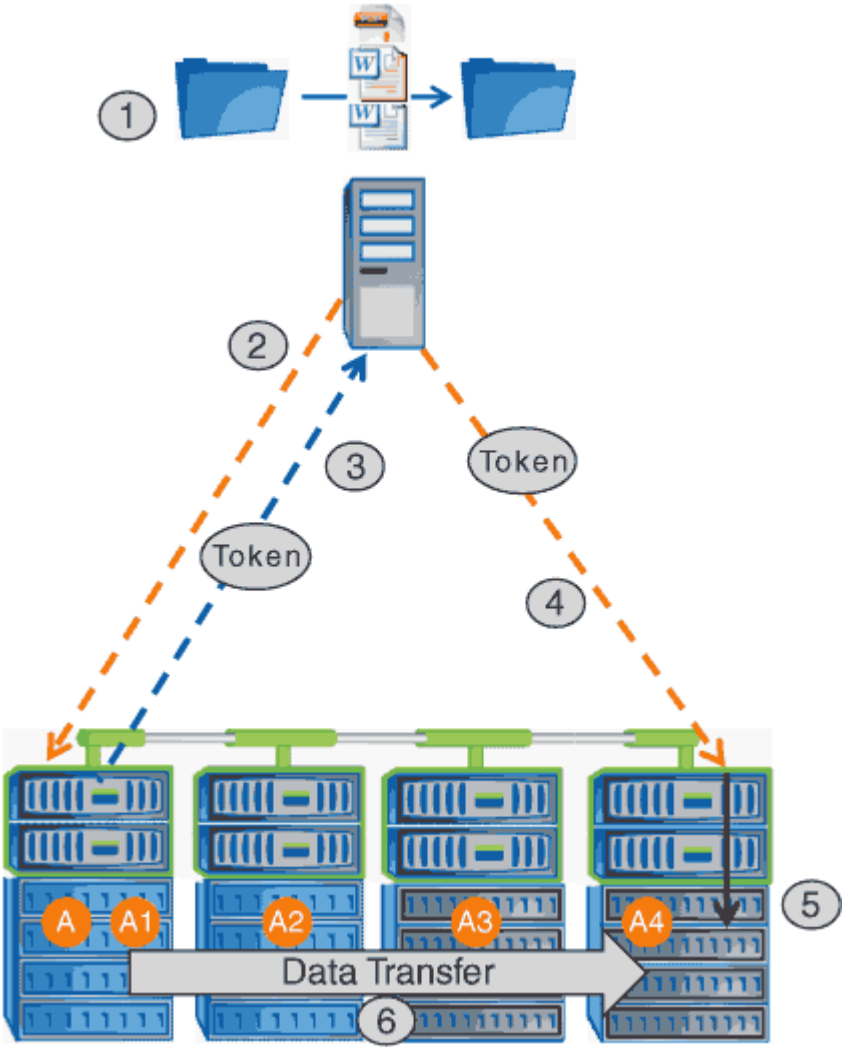
> A origem e o destino podem estar na mesma máquina virtual de storage (SVM) ou em SVMs diferentes, dependendo do escopo da operação de cópia.

O token serve como uma representação pontual dos dados. Como exemplo, quando você copia dados entre locais de armazenamento, um token representando um segmento de dados é retornado ao cliente solicitante, que o cliente copia para o destino, removendo assim a necessidade de copiar os dados subjacentes através

do cliente.

O ONTAP suporta tokens que representam 8 MB de dados. Cópias ODX de mais de 8 MB são executadas usando vários tokens, com cada token representando 8 MB de dados.

A figura a seguir explica as etapas envolvidas com uma operação de cópia ODX:



1. Um usuário copia ou move um arquivo usando o Windows Explorer, uma interface de linha de comando ou como parte de uma migração de máquina virtual, ou um aplicativo inicia cópias ou movimentos de arquivo.
2. O cliente compatível com ODX converte automaticamente essa solicitação de transferência em uma solicitação ODX.

   A solicitação ODX que é enviada para o servidor CIFS contém uma solicitação de um token.

3. Se o ODX estiver habilitado no servidor CIFS e a conexão for sobre SMB 3,0, o servidor CIFS gera um token, que é uma representação lógica dos dados na origem.
4. O cliente recebe um token que representa os dados e os envia com a solicitação de gravação para o servidor CIFS de destino.

   Estes são os únicos dados que são copiados pela rede da origem para o cliente e, em seguida, do cliente para o destino.

5. O token é entregue ao subsistema de armazenamento.
6. O SVM executa a cópia ou a movimentação internamente.

   Se o arquivo copiado ou movido for maior que 8 MB, vários tokens serão necessários para executar a cópia. Passos 2 a 6 conforme executado conforme necessário para concluir a cópia.

> Se houver uma falha com a cópia descarregada do ODX, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação. Da mesma forma, se o servidor CIFS de destino não suportar ODX ou ODX estiver desativado, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Requisitos para usar ODX

Antes de usar o ODX para descarregar cópias com sua máquina virtual de armazenamento (SVM), você precisa estar ciente de certos requisitos.

Requisitos de versão do ONTAP

As versões do ONTAP suportam ODX para descarregamentos de cópias.

Requisitos de versão SMB

- O ONTAP suporta ODX com SMB 3,0 e posterior.
- O SMB 3,0 deve estar habilitado no servidor CIFS antes que o ODX possa ser habilitado:
  - Ativar o ODX também ativa o SMB 3,0, se ele ainda não estiver ativado.
  - Desativar o SMB 3,0 também desativa o ODX.

Requisitos de servidor e cliente do Windows

Antes de poder utilizar o ODX para descarregar cópias, o cliente Windows tem de suportar a funcionalidade.

O "Matriz de interoperabilidade do NetApp"contém as informações mais recentes sobre clientes Windows suportados.

Requisitos de volume

- Os volumes de origem devem ter no mínimo 1,25 GB.
- Se você usar volumes compatados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

  O tipo de compressão secundária não é suportado.

Diretrizes para o uso do ODX

Antes de poder usar o ODX para descarga de cópia, você precisa estar ciente das diretrizes. Por exemplo, você precisa saber em quais tipos de volumes você pode usar ODX e você precisa entender as considerações do ODX intra-cluster e inter-cluster.

Diretrizes de volume

- Você não pode usar o ODX para descarga de cópia com as seguintes configurações de volume:
  - O tamanho do volume de origem é inferior a 1,25 GB

    O tamanho do volume deve ser de 1,25 GB ou maior para usar o ODX.

  - Volumes só de leitura

    O ODX não é usado para arquivos e pastas residentes em espelhos de compartilhamento de carga ou em volumes de destino SnapMirror ou SnapVault.

  - Se o volume de origem não for desduplicado
- Cópias ODX são suportadas apenas para cópias intra-cluster.

  Não é possível usar o ODX para copiar arquivos ou pastas para um volume em outro cluster.

Outras diretrizes

- Em ambientes SMB, para usar o ODX para descarga de cópia, os arquivos devem ter 256 kb ou mais.

  Arquivos menores são transferidos usando uma operação de cópia tradicional.

- O descarregamento de cópia ODX usa a deduplicação como parte do processo de cópia.

  Se você não quiser que a deduplicação ocorra em volumes SVM ao copiar ou mover dados, desative a descarga de cópia ODX nesse SVM.

- O aplicativo que executa a transferência de dados deve ser escrito para suportar ODX.

  As operações de aplicação que suportam ODX incluem o seguinte:

  - Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
  - Operações do Windows Explorer
  - Comandos de cópia do Windows PowerShell
  - Comandos de cópia do prompt de comando do Windows

    Robocopy no prompt de comando do Windows suporta ODX.

    > Os aplicativos devem estar em execução em servidores Windows ou clientes que suportem ODX.

  +
  Para obter mais informações sobre aplicativos ODX compatíveis em servidores e clientes Windows, consulte a Biblioteca Microsoft TechNet.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

  As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para CIFS.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conetadas a FC ou iSCSI.

  Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conetados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

  - Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB

mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

> Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Ativar ou desativar o ODX

Você pode ativar ou desativar o ODX em máquinas virtuais de armazenamento (SVMs). O padrão é habilitar o suporte para descarga de cópia ODX se o SMB 3,0 também estiver habilitado.

Antes de começar

O SMB 3,0 deve estar ativado.

Sobre esta tarefa

Se você desabilitar o SMB 3,0, o ONTAP também desabilitará o SMB ODX. Se você rehabilitar o SMB 3,0, será necessário reativar manualmente o SMB ODX.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Execute uma das seguintes ações:

Se você quiser que o descarregamento de cópia ODX seja…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Exemplo

O exemplo a seguir habilita a descarga de cópia ODX no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

Informações relacionadas

Opções de servidor SMB disponíveis

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com localização automática

Melhore o tempo de resposta do cliente fornecendo referências de nó automáticas SMB com visão geral de localização automática

A localização automática usa referências de nó automáticas SMB para aumentar a performance do cliente SMB em máquinas virtuais de armazenamento (SVMs). As referências automáticas de nós redirecionam automaticamente o cliente solicitante para um LIF no SVM do nó que hospeda o volume no qual os dados residem, o que pode levar a tempos de resposta aprimorados do cliente.

Quando um cliente SMB se coneta a um compartilhamento SMB hospedado no SVM, ele pode se conetar usando um LIF que está em um nó que não possui os dados solicitados. O nó ao qual o cliente está conetado acessa dados de propriedade de outro nó usando a rede do cluster. O cliente pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados:

- O ONTAP fornece essa funcionalidade usando referências do Microsoft DFS para informar clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar.

  Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados.

- As referências automáticas de nós são suportadas para endereços IP IPv4 e IPv6 LIF.
- As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.
- A referência ocorre durante a negociação SMB.

  A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.

Se um compartilhamento abranger vários pontos de junção e algumas das junções forem para volumes contidos em outros nós, os dados dentro do compartilhamento serão espalhados por vários nós. Como o ONTAP fornece referências locais à raiz do compartilhamento, o ONTAP deve usar a rede de cluster para recuperar os dados contidos nesses volumes não locais. Com esse tipo de arquitetura de namespace, as referências de nó automáticas podem não fornecer benefícios significativos de desempenho.

Se o nó que hospeda os dados não tiver um LIF disponível, o ONTAP estabelece a conexão usando o LIF escolhido pelo cliente. Depois que um arquivo é aberto por um cliente SMB, ele continua a acessar o arquivo através da mesma conexão referida.

Se, por qualquer motivo, o servidor CIFS não puder fazer uma referência, não haverá interrupção no serviço SMB. A conexão SMB é estabelecida como se as referências de nó automáticas não estivessem ativadas.

Informações relacionadas

Melhorando o desempenho de cópia remota da Microsoft

Requisitos e diretrizes para o uso de referências automáticas de nós

Antes de poder usar referências de nó automáticas SMB, também conhecidas como *autolocation*, você precisa estar ciente de certos requisitos, incluindo quais versões do ONTAP suportam o recurso. Você também precisa saber sobre versões de protocolo SMB compatíveis e algumas outras diretrizes especiais.

Requisitos de versão e licença do ONTAP

- Todos os nós no cluster devem estar executando uma versão do ONTAP que suporte referências automáticas de nós.
- Os Widelinks devem estar ativados em um compartilhamento SMB para usar a autenticação automática.
- O CIFS deve ser licenciado e um servidor SMB deve existir nos SVMs. A licença SMB está incluída no "ONTAP One". Se não tiver o ONTAP One e a licença não estiver instalada, contacte o seu representante de vendas.

Requisitos de versão do protocolo SMB

- Para SVMs, o ONTAP oferece suporte a referências automáticas de nós em todas as versões do SMB.

Requisitos do cliente SMB

Todos os clientes Microsoft suportados pelo ONTAP suportam referências de nó automáticas SMB.

A Matriz de interoperabilidade contém as informações mais recentes sobre quais clientes Windows ONTAP suportam.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de LIF de dados

Se você quiser usar um data LIF como potencial referência para clientes SMB, crie LIFs de dados com NFS e CIFS habilitados.

As referências automáticas de nós podem falhar ao funcionar se o nó de destino contiver LIFs de dados que

são ativados apenas para o protocolo NFS ou ativados apenas para o protocolo SMB.

Se este requisito não for cumprido, o acesso aos dados não será afetado. O cliente SMB mapeia o compartilhamento usando o LIF original usado pelo cliente para se conetar ao SVM.

Requisitos de autenticação NTLM ao fazer uma conexão SMB referida

A autenticação NTLM deve ser permitida no domínio que contém o servidor CIFS e nos domínios que contêm clientes que desejam usar referências automáticas de nós.

Ao fazer uma referência, o servidor SMB refere um endereço IP ao cliente Windows. Como a autenticação NTLM é usada ao fazer uma conexão usando um endereço IP, a autenticação Kerberos não é executada para conexões referidas.

Isso acontece porque o cliente Windows não pode criar o nome principal do serviço usado pelo Kerberos (que é do formulário `service/NetBIOS name` e `service/FQDN`), o que significa que o cliente não pode solicitar um ticket Kerberos ao serviço.

Diretrizes para o uso de referências automáticas de nós com o recurso de diretório base

Quando os compartilhamentos são configurados com a propriedade de compartilhamento do diretório base ativada, pode haver um ou mais caminhos de pesquisa do diretório base configurados para uma configuração do diretório base. Os caminhos de pesquisa podem apontar para volumes contidos em cada nó que contém volumes SVM. Os clientes recebem uma referência e, se um LIF de dados local ativo estiver disponível, se conetam através de um LIF referido que é local para o diretório home do usuário doméstico.

Há diretrizes quando clientes SMB 1,0 acessam diretórios base dinâmicos com referências automáticas de nós ativadas. Isso ocorre porque os clientes SMB 1,0 exigem a referência automática do nó antes de autenticarem, o que é antes que o servidor SMB tenha o nome do usuário. No entanto, o acesso ao diretório home SMB funciona corretamente para clientes SMB 1,0 se as seguintes instruções forem verdadeiras:

- Os diretórios home SMB são configurados para usar nomes simples, como "%W" (nome de usuário do Windows) ou ""%u" (nome de usuário UNIX mapeado), e não nomes de estilo de nome de domínio, como "%d%W "" (nome de domínio/nome de usuário).
- Ao criar compartilhamentos de diretório base, os nomes de compartilhamentos de diretório base CIFS são configurados com variáveis ("'%W'" ou "'%u'") e não com nomes estáticos, como "'HOME'".

Para clientes SMB 2.x e SMB 3,0, não há diretrizes especiais ao acessar diretórios base usando referências automáticas de nós.

Diretrizes para desabilitar referências automáticas de nós em servidores CIFS com conexões referidas existentes

Se você desativar as referências automáticas de nós depois que a opção tiver sido ativada, os clientes atualmente conetados a um LIF referido mantêm a conexão referida. Como o ONTAP usa referências DFS como o mecanismo para referências de nó automáticas SMB, os clientes podem até se reconetar ao LIF referido depois de desativar a opção até que a referência DFS armazenada em cache do cliente para a conexão referida expire. Isso é verdade mesmo no caso de uma reversão para uma versão do ONTAP que não suporta referências automáticas de nós. Os clientes continuam a usar referências até que o encaminhamento do DFS termine do cache do cliente.

A Autolocation usa referências de nó automáticas SMB para aumentar o desempenho do cliente SMB, referindo os clientes ao LIF no nó que possui o volume de dados de um SVM. Quando um cliente SMB se coneta a um compartilhamento SMB hospedado em um SVM, ele pode se conetar usando um LIF em um nó que não possui os dados solicitados e usa a rede de interconexão de cluster para recuperar dados. O cliente

pode ter tempos de resposta mais rápidos se a conexão SMB usar um LIF localizado no nó que contém os dados solicitados.

O ONTAP fornece essa funcionalidade usando referências do sistema de arquivos distribuídos da Microsoft (DFS) para informar os clientes SMB que um arquivo ou pasta solicitado no namespace está hospedado em outro lugar. Um nó faz uma referência quando determina que há um LIF SVM no nó que contém os dados. As referências são feitas com base na localização da raiz da partilha através da qual o cliente está ligado.

A referência ocorre durante a negociação SMB. A referência é feita antes da conexão ser estabelecida. Depois que o ONTAP refere o cliente SMB ao nó de destino, a conexão é feita e o cliente acessa os dados através do caminho LIF referido a partir desse ponto. Isso permite que os clientes tenham acesso mais rápido aos dados e evite a comunicação de cluster adicional.

Diretrizes para o uso de referências automáticas de nó com clientes Mac os

Os clientes Mac os X não suportam referências de nó automáticas SMB, mesmo que o Mac os suporte o sistema de arquivos distribuídos (DFS) da Microsoft. Os clientes Windows fazem uma solicitação de referência DFS antes de se conetar a um compartilhamento SMB. O ONTAP fornece uma referência a um LIF de dados encontrado no mesmo nó que hospeda os dados solicitados, o que leva a melhores tempos de resposta do cliente. Embora o Mac os suporte DFS, os clientes do Mac os não se comportam exatamente como os clientes do Windows nesta área.

Informações relacionadas

Como o ONTAP ativa diretórios base dinâmicos

"Gerenciamento de rede"

"Ferramenta de Matriz de interoperabilidade do NetApp"

Suporte para referências de nó automáticas SMB

Antes de ativar as referências de nó automático SMB, você deve estar ciente de que certas funcionalidades do ONTAP não suportam referências.

- Os seguintes tipos de volumes não suportam referências de nó automáticas SMB:
  - Membros somente leitura de um espelho de compartilhamento de carga
  - Volume de destino de um espelho de proteção de dados
- As referências de nó não se movem ao lado de uma movimentação de LIF.

  Se um cliente estiver usando uma conexão referida por meio de uma conexão SMB 2.x ou SMB 3,0 e um LIF de dados se mover sem interrupções, o cliente continuará a usar a mesma conexão referida, mesmo que o LIF não seja mais local para os dados.

- As referências de nó não se movem ao lado de uma movimentação de volume.

  Se um cliente estiver usando uma conexão referida em qualquer conexão SMB e ocorrer uma movimentação de volume, o cliente continuará a usar a mesma conexão referida, mesmo que o volume não esteja mais localizado no mesmo nó que o LIF de dados.

Ative ou desative referências de nó automáticas SMB

Você pode habilitar referências de nó automáticas SMB para aumentar o desempenho

de acesso de cliente SMB. Você pode desativar referências automáticas de nós se não quiser que o ONTAP faça referências a clientes SMB.

Antes de começar

Um servidor CIFS deve ser configurado e executado na máquina virtual de storage (SVM).

Sobre esta tarefa

A funcionalidade de referências de nó automático SMB está desativada por predefinição. Você pode ativar ou desativar essa funcionalidade em cada SVM conforme necessário.

Esta opção está disponível no nível de privilégio avançado.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Ative ou desative referências de nó automáticas SMB conforme necessário:

Se você quiser que as referências de nó automático SMB sejam…	Digite o seguinte comando…
Ativado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

   A configuração de opção entra em vigor para novas sessões SMB. Os clientes com conexão existente podem utilizar referência de nó somente quando o tempo limite de cache existente expirar.

3. Mudar para o nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Opções de servidor SMB disponíveis

Use as estatísticas para monitorar a atividade automática de referência de nós

Para determinar quantas conexões SMB são referidas, você pode monitorar a atividade automática de referência de nó usando o `statistics` comando. Ao monitorar referências, você pode determinar em que medida as referências automáticas estão localizando conexões em nós que hospedam os compartilhamentos e se você deve redistribuir seus LIFs de dados para fornecer melhor acesso local aos compartilhamentos no servidor CIFS.

Sobre esta tarefa

O `cifs` objeto fornece vários contadores no nível de privilégio avançado que são úteis ao monitorar referências automáticas de nó SMB:

- `node_referral_issued`

Número de clientes que receberam uma referência para o nó da raiz de compartilhamento depois que o cliente se conetou usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento.

- `node_referral_local`

  Número de clientes que se conetaram usando um LIF hospedado pelo mesmo nó que hospeda a raiz de compartilhamento. O acesso local geralmente proporciona um desempenho ideal.

- `node_referral_not_possible`

  Número de clientes que não receberam uma referência para o nó que hospeda a raiz de compartilhamento depois de se conetar usando um LIF hospedado por um nó diferente do nó da raiz de compartilhamento. Isso ocorre porque um LIF de dados ativo para o nó da raiz de compartilhamento não foi encontrado.

- `node_referral_remote`

  Número de clientes que se conetaram usando um LIF hospedado por um nó diferente do nó que hospeda a raiz de compartilhamento. O acesso remoto pode resultar em desempenho degradado.

Você pode monitorar as estatísticas automáticas de referência de nós na sua máquina virtual de storage (SVM) coletando e visualizando dados para um período de tempo específico (uma amostra). Você pode exibir dados da amostra se não parar a coleta de dados. Parar a coleta de dados dá-lhe uma amostra fixa. Não interromper a coleta de dados dá a você a capacidade de obter dados atualizados que você pode usar para comparar com consultas anteriores. A comparação pode ajudá-lo a identificar tendências de desempenho.

Para avaliar e usar as informações que você coleta a partir do `statistics` comando, você deve entender a distribuição de clientes em seus ambientes.

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`
2. Visualize estatísticas automáticas de referência de nó usando o `statistics` comando.

   Este exemplo exibe estatísticas automáticas de referência de nó coletando e visualizando dados para um período de tempo de amostragem:

   a. Inicie a coleção: `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. Aguarde até que o tempo de recolha pretendido decorra.

   c. Parar a coleção: `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   d. Veja as estatísticas automáticas de referência de nó: `statistics show -sample-id sample1 -counter` **`node`**

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    node_name                                   node1
    node_referral_issued                            0
    node_referral_local                             1
    node_referral_not_possible                      2
    node_referral_remote                            2
    ...

    node_name                                   node2
    node_referral_issued                            2
    node_referral_local                             1
    node_referral_not_possible                      0
    node_referral_remote                            2
    ...
```

A saída exibe contadores para todos os nós participantes do SVM VS1. Para maior clareza, apenas os campos de saída relacionados às estatísticas automáticas de referência de nó são fornecidos no exemplo.

3. Voltar ao nível de privilégio de administrador: `set -privilege admin`

Informações relacionadas

Exibindo estatísticas

"Configuração do monitoramento de desempenho"

Monitore informações de referência automática de nós SMB no lado do cliente usando um cliente Windows

Para determinar quais referências são feitas da perspetiva do cliente, você pode usar o utilitário Windows `dfsutil.exe`.

O kit RSAT (Remote Server Administration Tools) disponível com o Windows 7 e clientes posteriores contém o `dfsutil.exe` utilitário. Usando este utilitário, você pode exibir informações sobre o conteúdo do cache de referência, bem como visualizar informações sobre cada referência que o cliente está usando atualmente. Você também pode usar o utilitário para limpar o cache de referência do cliente. Para obter mais informações, consulte a Microsoft TechNet Library.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Forneça segurança de pastas em compartilhamentos com enumeração baseada em acesso

Forneça segurança de pastas em compartilhamentos com visão geral de enumeração baseada em acesso

Quando a enumeração baseada em acesso (ABE) está ativada em um compartilhamento SMB, os usuários que não têm permissão para acessar uma pasta ou arquivo contido no compartilhamento (seja por restrições de permissão individuais ou de grupo) não veem esse recurso compartilhado exibido em seu ambiente, embora o próprio compartilhamento permaneça visível.

As propriedades de compartilhamento convencionais permitem especificar quais usuários (individualmente ou em grupos) têm permissão para exibir ou modificar arquivos ou pastas contidos no compartilhamento. No entanto, eles não permitem que você controle se pastas ou arquivos dentro do compartilhamento são visíveis para usuários que não têm permissão para acessá-los. Isso pode causar problemas se os nomes dessas pastas ou arquivos dentro do compartilhamento descreverem informações confidenciais, como os nomes de clientes ou produtos em desenvolvimento.

A enumeração baseada em acesso (ABE) estende as propriedades de compartilhamento para incluir a enumeração de arquivos e pastas dentro do compartilhamento. Portanto, O ABE permite filtrar a exibição de arquivos e pastas dentro do compartilhamento com base nos direitos de acesso do usuário. Ou seja, o compartilhamento em si seria visível para todos os usuários, mas os arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultados de usuários designados. Além de proteger informações confidenciais em seu local de trabalho, o ABE permite simplificar a exibição de grandes estruturas de diretórios para benefício dos usuários que não precisam acessar toda a sua gama de conteúdo. Por exemplo, o compartilhamento em si seria visível para todos os usuários, mas arquivos e pastas dentro do compartilhamento poderiam ser exibidos ou ocultos.

Saiba mais "Impacto no desempenho ao usar enumeração baseada em acesso SMB/CIFS"sobre .

Ative ou desative a enumeração baseada em acesso em compartilhamentos SMB

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB para permitir ou impedir que os usuários vejam recursos compartilhados que eles não têm permissão para acessar.

Sobre esta tarefa

Por padrão, o ABE está desativado.

Passos

1. Execute uma das seguintes ações:

Se você quiser…	Digite o comando…
Ative o ABE em um novo compartilhamento	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration` Você pode especificar configurações de compartilhamento opcionais adicionais e propriedades de compartilhamento adicionais ao criar um compartilhamento SMB. Para obter mais informações, consulte a página man para o `vserver cifs share create` comando.
Ative o ABE em um compartilhamento existente	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` As propriedades de compartilhamento existentes são preservadas. A propriedade ABE Share é adicionada à lista existente de propriedades de ações.
Desative o ABE em um compartilhamento existente	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` Outras propriedades de compartilhamento são preservadas. Somente a propriedade ABE Share é removida da lista de propriedades de compartilhamento.

2. Verifique se a configuração de compartilhamento está correta usando o `vserver cifs share show` comando.

Exemplos

O exemplo a seguir cria um compartilhamento ABE SMB chamado "vendas" com um caminho de `/sales` no SVM VS1. A ação é criada com `access-based-enumeration` como uma propriedade de ação:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
            Share Properties: access-based-enumeration
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

O exemplo a seguir adiciona a `access-based-enumeration` propriedade share a um compartilhamento SMB chamado "ata2":

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

Informações relacionadas

Adicionar ou remover propriedades de compartilhamento em um compartilhamento SMB existente

Ativar ou desativar a enumeração baseada em acesso a partir de um cliente Windows

Você pode ativar ou desativar a enumeração baseada em acesso (ABE) em compartilhamentos SMB de um cliente Windows, o que permite configurar essa configuração de compartilhamento sem precisar se conetar ao servidor CIFS.

O `abecmd` utilitário não está disponível em novas versões dos clientes Windows Server e Windows. Foi lançado como parte do Windows Server 2008. O suporte terminou para o Windows Server 2008 em 14 de janeiro de 2020.

Passos

1. Em um cliente Windows que suporte ABE, digite o seguinte comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   Para obter mais informações sobre o `abecmd` comando, consulte a documentação do cliente Windows.

Dependências de nomes de arquivos e diretórios NFS e SMB

Visão geral das dependências de nomes de arquivos e diretórios NFS e SMB

As convenções de nomenclatura de arquivos e diretórios dependem tanto dos sistemas operacionais dos clientes de rede quanto dos protocolos de compartilhamento de arquivos, além das configurações de idioma do cluster e dos clientes do ONTAP.

O sistema operacional e os protocolos de compartilhamento de arquivos determinam o seguinte:

- Carateres que um nome de arquivo pode usar
- Sensibilidade em caso de um nome de ficheiro

O ONTAP suporta carateres multibyte em nomes de arquivo, diretório e qtree, dependendo da versão do ONTAP.

Carateres que um nome de arquivo ou diretório pode usar

Se você estiver acessando um arquivo ou diretório de clientes com sistemas operacionais diferentes, use carateres válidos em ambos os sistemas operacionais.

Por exemplo, se você usar UNIX para criar um arquivo ou diretório, não use dois pontos (:) no nome porque os dois pontos não são permitidos em nomes de arquivo ou diretório MS-dos. Como as restrições em carateres válidos variam de um sistema operacional para outro, consulte a documentação do sistema operacional cliente para obter mais informações sobre carateres proibidos.

Sensibilidade de casos de nomes de arquivos e diretórios em um ambiente multiprotocolo

Os nomes de arquivos e diretórios são sensíveis a maiúsculas e minúsculas para clientes NFS, mas que preservam casos para clientes SMB. Você deve entender quais são as implicações em um ambiente multiprotocolo e as ações que pode precisar tomar ao especificar o caminho ao criar compartilhamentos SMB e ao acessar dados nos compartilhamentos.

Se um cliente SMB criar um diretório `testdir` chamado , os clientes SMB e NFS exibirão o nome do arquivo como `testdir`. No entanto, se um usuário SMB tentar criar um nome de diretório mais tarde `TESTDIR` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar posteriormente um diretório `TESTDIR` chamado , clientes NFS e SMB exibirão o nome do diretório de maneira diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de diretório à medida que foram criados, por `testdir` exemplo e `TESTDIR`, porque os nomes de diretório são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois diretórios. Um diretório tem o nome do arquivo base. Os diretórios adicionais recebem um nome de arquivo 8,3.
  - Em clientes SMB, você verá `testdir` e `TESTDI~1`.
  - O ONTAP cria o `TESTDI~1` nome do diretório para diferenciar os dois diretórios.

    Nesse caso, você deve usar o nome 8,3 ao especificar um caminho de compartilhamento ao criar ou modificar um compartilhamento em uma máquina virtual de storage (SVM).

Da mesma forma para arquivos, se um cliente SMB criar `test.txt`, os clientes SMB e NFS exibirão o nome do arquivo como `text.txt`. No entanto, se um usuário SMB tentar criar mais tarde `Test.txt` , o nome não será permitido porque, para o cliente SMB, esse nome existe atualmente. Se um usuário NFS criar mais tarde um arquivo `Test.txt` chamado , clientes NFS e SMB exibirão o nome do arquivo de forma diferente, da seguinte forma:

- Em clientes NFS, você verá ambos os nomes de arquivos à medida que foram criados e `test.txt` `Test.txt` , porque os nomes de arquivos são sensíveis a maiúsculas e minúsculas.
- Os clientes SMB usam os nomes 8,3 para distinguir entre os dois arquivos. Um arquivo tem o nome do arquivo base. Os ficheiros adicionais recebem um nome de ficheiro 8,3.
  - Em clientes SMB, você verá `test.txt` e `TEST~1.TXT`.
  - O ONTAP cria o `TEST~1.TXT` nome do arquivo para diferenciar os dois arquivos.

> Se você tiver ativado ou modificado o mapeamento de carateres usando os comandos SVM CIFS de mapeamento de carateres, uma pesquisa Windows normalmente insensível a maiúsculas e minúsculas torna-se sensível a maiúsculas e minúsculas.

Como o ONTAP cria nomes de arquivo e diretório

O ONTAP cria e mantém dois nomes para arquivos ou diretórios em qualquer diretório que tenha acesso de um cliente SMB: O nome longo original e um nome no formato 8,3.

Para nomes de arquivo ou diretório que excedam o nome de oito carateres ou o limite de extensão de três carateres (para arquivos), o ONTAP gera um nome de formato 8,3 da seguinte forma:

- Ele trunca o nome do arquivo ou diretório original para seis carateres, se o nome exceder seis carateres.
- Ele adiciona um til (…) e um número, um a cinco, aos nomes de arquivo ou diretório que não são mais exclusivos depois de serem truncados.

  Se ele ficar sem números porque há mais de cinco nomes semelhantes, ele cria um nome exclusivo que não tem relação com o nome original.

- No caso dos arquivos, ele trunca a extensão do nome do arquivo para três carateres.

Por exemplo, se um cliente NFS criar um arquivo chamado `specifications.html`, o nome do arquivo de formato 8,3 criado pelo ONTAP será `specif~1.htm`. Se esse nome já existir, o ONTAP usará um número diferente no final do nome do arquivo. Por exemplo, se um cliente NFS criar outro arquivo chamado `specifications_new.html`, o formato 8,3 do `specifications_new.html` é `specif~2.htm`.

Como o ONTAP lida com nomes de arquivos, diretórios e qtree de vários bytes

Começando com ONTAP 9.5, o suporte para nomes codificados UTF-8 de 4 bytes permite a criação e exibição de nomes de arquivos, diretórios e árvores que incluem carateres suplementares Unicode fora do plano multilíngue básico (BMP). Em versões anteriores, esses carateres suplementares não foram exibidos corretamente em ambientes multiprotocolo.

Para ativar o suporte para nomes codificados UTF-8 de 4 bytes, um novo código de linguagem *utf8mb4* está disponível para as `vserver` famílias de comandos e `volume` .

Você deve criar um novo volume de uma das seguintes maneiras:

- Definir a opção de volume `-language` explicitamente: `volume create -language utf8mb4 {…}`
- Herdando a opção de volume `-language` de uma SVM que foi criada ou modificada para a opção: `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- No ONTAP 9.6 e anteriores, não é possível modificar volumes existentes para suporte a utf8mb4; é necessário criar um novo volume pronto para utf8mb4 e migrar os dados usando ferramentas de cópia baseadas em cliente.

  Você pode atualizar SVMs para suporte a utf8mb4, mas os volumes existentes mantêm seus códigos de idioma originais.

  Se você estiver usando o ONTAP 9.7P1 ou posterior, poderá modificar volumes existentes para o utf8mb4 com uma solicitação de suporte. Para obter mais informações, "O idioma do volume pode ser alterado após a criação no ONTAP?"consulte .

- Começando com ONTAP 9.8, você pode usar o `[-language <Language code>]` parâmetro para alterar o idioma do volume de *.UTF-8 para utf8mb4. Para alterar o idioma de um volume, "Suporte à NetApp"contacte .

  Nomes LUN com carateres UTF-8 de 4 bytes não são suportados atualmente.

- Os dados de carateres Unicode são normalmente representados em aplicações de sistemas de ficheiros Windows utilizando o formato de transformação Unicode de 16 bits (UTF-16) e em sistemas de ficheiros NFS utilizando o formato de transformação Unicode de 8 bits (UTF-8).

  Em versões anteriores ao ONTAP 9.5, nomes incluindo carateres suplementares UTF-16 que foram criados por clientes Windows foram exibidos corretamente para outros clientes Windows, mas não foram traduzidos corretamente para UTF-8 para clientes NFS. Da mesma forma, nomes com carateres suplementares UTF-8 por clientes NFS criados não foram traduzidos corretamente para UTF-16 para clientes Windows.

- Quando você cria nomes de arquivo em sistemas que executam o ONTAP 9.4 ou anteriores que contêm carateres suplementares válidos ou inválidos, o ONTAP rejeita o nome do arquivo e retorna um erro de nome de arquivo inválido.

  Para evitar esse problema, use apenas carateres BMP em nomes de arquivo e evite usar carateres suplementares ou atualize para o ONTAP 9.5 ou posterior.

Começando com ONTAP 9, carateres Unicode são permitidos em nomes de qtree.

- Você pode usar a `volume qtree` família de comandos ou o System Manager para definir ou modificar nomes de qtree.
- Os nomes de qtree podem incluir carateres de vários bytes no formato Unicode, como carateres japoneses e chineses.
- Em versões anteriores ao ONTAP 9.5, apenas os carateres BMP (ou seja, aqueles que poderiam ser representados em 3 bytes) foram suportados.

> Em versões anteriores ao ONTAP 9.5, o caminho de junção do volume pai da qtree pode conter nomes de qtree e diretório com carateres Unicode. O `volume show` comando exibe esses nomes corretamente quando o volume pai tem uma configuração de idioma UTF-8. No entanto, se o idioma do volume pai não for uma das configurações de idioma UTF-8, algumas partes do caminho de junção serão exibidas usando um nome alternativo NFS numérico.

- Em versões 9,5 e posteriores, os carateres de 4 bytes são suportados em nomes de qtree, desde que a qtree esteja em um volume habilitado para utf8mb4.

Configure o mapeamento de carateres para a tradução de nomes de arquivo SMB em volumes

Os clientes NFS podem criar nomes de arquivos que contêm carateres que não são válidos para clientes SMB e determinados aplicativos do Windows. Você pode configurar o mapeamento de carateres para a tradução de nome de arquivo em volumes para permitir que clientes SMB acessem arquivos com nomes NFS que, de outra forma, não seriam válidos.

Sobre esta tarefa

Quando os arquivos criados por clientes NFS são acessados por clientes SMB, o ONTAP examina o nome do arquivo. Se o nome não for um nome de arquivo SMB válido (por exemplo, se ele tiver um caractere de dois pontos "':'" incorporado), o ONTAP retornará o nome de arquivo 8,3 que é mantido para cada arquivo. No entanto, isso causa problemas para aplicativos que codificam informações importantes em nomes de arquivos longos.

Portanto, se você estiver compartilhando um arquivo entre clientes em sistemas operacionais diferentes, você deve usar carateres nos nomes de arquivo que são válidos em ambos os sistemas operacionais.

No entanto, se você tiver clientes NFS que criam nomes de arquivo contendo carateres que não são nomes de arquivo válidos para clientes SMB, você poderá definir um mapa que converte os carateres NFS inválidos em carateres Unicode que tanto SMB quanto determinados aplicativos do Windows aceitam. Por exemplo, essa funcionalidade suporta os aplicativos CATIA MCAD e Mathematica, bem como outros aplicativos que têm esse requisito.

Você pode configurar o mapeamento de carateres em uma base volume por volume.

Você deve ter em mente o seguinte ao configurar o mapeamento de carateres em um volume:

- O mapeamento de carateres não é aplicado em pontos de junção.

  Você deve configurar explicitamente o mapeamento de carateres para cada volume de junção.

- Você deve certificar-se de que os carateres Unicode que são usados para representar carateres inválidos ou ilegais são carateres que normalmente não aparecem em nomes de arquivos; caso contrário, mapeamentos indesejados ocorrem.

Por exemplo, se você tentar mapear dois pontos (:) para um hífen (-), mas o hífen (-) foi usado no nome do arquivo corretamente, um cliente Windows tentando acessar um arquivo chamado "'a-b'" teria sua solicitação mapeada para o nome NFS de "'a:b'" (não o resultado desejado).

- Depois de aplicar o mapeamento de carateres, se o mapeamento ainda contiver um caractere Windows inválido, o ONTAP volta para os nomes de arquivos do Windows 8,3.
- Em notificações FPolicy, logs de auditoria nas e mensagens de rastreamento de segurança, os nomes de arquivo mapeados são exibidos.
- Quando uma relação SnapMirror do tipo DP é criada, o mapeamento de carateres do volume de origem não é replicado no volume DP de destino.
- Sensibilidade do caso: Como os nomes mapeados do Windows se transformam em nomes NFS, a pesquisa dos nomes segue semântica de NFS. Isso inclui o fato de que pesquisas NFS são sensíveis a maiúsculas e minúsculas. Isso significa que os aplicativos que acessam compartilhamentos mapeados não devem depender de comportamento insensível a maiúsculas e minúsculas do Windows. No entanto, o nome 8,3 está disponível, e isso é insensível a maiúsculas e minúsculas.
- Mapeamentos parciais ou inválidos: Depois de mapear um nome para retornar aos clientes fazendo enumeração de diretórios ("dir"), o nome Unicode resultante é verificado para a validade do Windows. Se esse nome ainda tiver carateres inválidos nele, ou se for inválido para o Windows (por exemplo, termina em "." ou em branco), o nome 8,3 será retornado em vez do nome inválido.

Passo

1. Configurar mapeamento de carateres

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, …` E

O mapeamento consiste em uma lista de pares de carateres fonte-alvo separados por "':'". Os carateres são carateres Unicode inseridos usando dígitos hexadecimais. Por exemplo: 3c:E03C. E

O primeiro valor de cada `mapping_text` par que é separado por dois pontos é o valor hexadecimal do caractere NFS que você deseja traduzir, e o segundo valor é o valor Unicode que SMB usa. Os pares de mapeamento devem ser únicos (deve existir um mapeamento um-para-um).

- Mapeamento de origem

A tabela a seguir mostra o conjunto de carateres Unicode permissível para mapeamento de fontes:

E

Caractere Unicode	Caráter impresso	Descrição
0x01-0x19	Não aplicável	Caracteres de controle não-impressão
0x5C		Barra invertida
0x3A	:	Cólon
0x2A	*	Asterisco

Caractere Unicode	Caráter impresso	Descrição
0x3F	?	Ponto de interrogação
0x22	"	Marca de cotação
0x3C	*	Menos de
0x3E	>	Superior a.
0x7C		
Linha vertical	0xB1	±

- Mapeamento de alvos

  Você pode especificar carateres de destino na ""Área de uso privado"" do Unicode no seguinte intervalo: U-E0000…U-F8FF.

Exemplo

O comando a seguir cria um mapeamento de carateres para um volume chamado "data" na máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

Informações relacionadas

Criação e gerenciamento de volumes de dados em namespaces nas

Comandos para gerenciar mapeamentos de carateres para a tradução de nome de arquivo SMB

É possível gerenciar o mapeamento de carateres criando, modificando, exibindo informações ou excluindo mapeamentos de carateres de arquivo usados para a tradução de nomes de arquivo SMB em volumes FlexVol.

Se você quiser…	Use este comando…
Criar novos mapeamentos de carateres de arquivo	`vserver cifs character-mapping create`
Exibir informações sobre mapeamentos de carateres de arquivo	`vserver cifs character-mapping show`

Se você quiser…	Use este comando…
Modificar mapeamentos de carateres de arquivo existentes	`vserver cifs character-mapping modify`
Excluir mapeamentos de carateres de arquivo	`vserver cifs character-mapping delete`

Para obter mais informações, consulte a página man para cada comando.

Informações relacionadas

Configurando o mapeamento de carateres para a tradução de nome de arquivo SMB em volumes

Fornecer acesso de cliente S3 aos dados nas

Suporte multiprotocolo S3 no ONTAP

A partir do ONTAP 9.12,1, é possível permitir que os clientes que executam o protocolo S3 acessem os mesmos dados que estão sendo atendidos aos clientes que usam os protocolos NFS e SMB sem reformatação. Esse recurso permite que os dados nas continuem sendo servidos a clientes nas, enquanto apresentam dados de objetos a clientes S3 que executam aplicações S3 (como data mining e inteligência artificial).

A funcionalidade multiprotocolo S3 aborda dois casos de uso:

1. Acesso a dados nas existentes usando clientes S3

   Se os dados existentes tiverem sido criados usando clientes nas tradicionais (NFS ou SMB) e estiverem localizados em volumes nas (volumes FlexVol ou FlexGroup), agora você poderá usar ferramentas de análise em clientes do S3 para acessar esses dados.

2. Storage de back-end para clientes modernos com capacidade para executar e/S usando protocolos nas e S3

   Agora você pode fornecer acesso integrado para aplicativos como Spark e Kafka que podem ler e gravar os mesmos dados usando protocolos nas e S3.

Como funciona o suporte multiprotocolo S3

O suporte multiprotocolo ONTAP permite que você apresente o mesmo conjunto de dados que uma hierarquia de arquivos ou objetos em um bucket. Para fazer isso, o ONTAP cria "S3 buckets nas" que permitem que os clientes do S3 criem, leiam, excluam e enumerem arquivos no storage nas usando solicitações de objetos do S3. Este mapeamento está em conformidade com a configuração de segurança nas, observando permissões de acesso a arquivos e diretórios, bem como gravar na trilha de auditoria de segurança, conforme necessário.

Esse mapeamento é realizado apresentando uma hierarquia de diretórios nas especificada como um bucket S3. Cada arquivo na hierarquia de diretórios é representado como um objeto S3 cujo nome é relativo do diretório mapeado para baixo, com limites de diretório representados pelo caractere de barra ('/').

Os usuários do S3 definidos pela ONTAP podem acessar esse storage, conforme governado pelas políticas de bucket definidas para o bucket que é mapeado para o diretório nas. Para que isso seja possível, mapeamentos devem ser definidos entre os usuários S3 e os usuários SMB/NFS. As credenciais do usuário

SMB/NFS serão usadas para a verificação de permissões nas e incluídas em todos os Registros de auditoria resultantes desses acessos.

Quando criado por clientes SMB ou NFS, um arquivo é colocado imediatamente em um diretório e, portanto, visível para clientes, antes que qualquer dado seja gravado nele. Os clientes S3 esperam semântica diferente, na qual o novo objeto não é visível no namespace até que todos os seus dados tenham sido escritos. Esse mapeamento do S3 para o armazenamento nas cria arquivos usando semântica S3, mantendo os arquivos invisíveis externamente até que o comando de criação S3 seja concluído.

Proteção de dados para buckets do nas S3

S3 "buckets" nas são simplesmente mapeamentos de dados nas para clientes S3, e não são buckets do S3 padrão. Portanto, não há necessidade de proteger buckets do nas S3 usando a funcionalidade do NetApp SnapMirror S3. Em vez disso, você pode proteger volumes que contêm S3 buckets do nas usando a replicação de volume assíncrona do SnapMirror. A recuperação de desastres síncrona SnapMirror e SVM não é compatível.

A partir do ONTAP 9.14,1, os buckets nas de S3 GB são compatíveis com agregados espelhados e sem espelhamento para configurações MetroCluster IP e FC.

Saiba mais "Assíncrono com SnapMirror"sobre .

Auditoria para buckets do nas S3

Como os buckets do nas S3 não são buckets do S3 convencionais, a auditoria do S3 não pode ser configurada para auditar o acesso neles. Saiba mais "Auditoria S3"sobre o .

No entanto, os arquivos e diretórios nas mapeados em buckets do nas S3 podem ser auditados para eventos de acesso usando procedimentos de auditoria convencionais do ONTAP. As operações S3 podem, portanto, acionar eventos de auditoria nas, com as seguintes exceções:

- Se o acesso de cliente S3 for negado pela configuração de diretiva S3 (política de grupo ou bucket), a auditoria nas para o evento não será iniciada. Isso ocorre porque as permissões do S3 são verificadas antes que as verificações de auditoria SVM possam ser feitas.
- Se o arquivo de destino de uma solicitação de S3 GET for de tamanho 0, o conteúdo 0 será retornado à solicitação de GET e o acesso de leitura não será registrado.
- Se o arquivo de destino de uma solicitação de S3 GET estiver em uma pasta para a qual o usuário não tenha permissão de avanço, a tentativa de acesso falhará e o evento não será registrado.

Saiba mais "Auditoria de eventos nas em SVMs"sobre .

Upload multipart de objeto

A partir do ONTAP 9.16,1, o upload de várias partes de objetos é suportado quando "balanceamento de capacidade avançado" o FlexGroup volumes está ativado.

O upload multipart de objeto no armazenamento de arquivos nas permite que um cliente de protocolo S3 carregue um objeto grande como partes menores. O upload de várias partes do objeto tem os seguintes benefícios:

- Ele permite que objetos sejam carregados em paralelo.
- Em caso de falha ou pausa no upload, apenas as partes que ainda não foram carregadas precisarão ser carregadas. O upload de todo o objeto não precisa ser reiniciado.

- Se o tamanho do objeto não for conhecido antecipadamente (por exemplo, quando um objeto grande ainda está sendo escrito), os clientes podem começar a carregar partes do objeto imediatamente e concluir o upload após o objeto inteiro ter sido criado.

O upload multipart suporta as seguintes ações S3:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Interoperabilidade do S3 e nas

Os buckets do ONTAP S3 nas suportam a funcionalidade nas e S3 padrão, exceto conforme listado aqui.

Funcionalidade nas atualmente não suportada por buckets do nas S3

Camada de capacidade do FabricPool

Os buckets do nas S3 não podem ser configurados como uma camada de capacidade para o FabricPool.

S3 ações e funcionalidade não compatíveis atualmente com buckets do nas S3

Ações

- ByPassGovernanceRetention
- CopyObject
- GetBucketObjectLockConfiguration
- GetBucketControle de versão
- GetObjectRetention
- PutBucketControle de versão
- PutObjectLockConfiguration
- Retenção PutObjectRetention
- ListBucketControle de versão
- ListObjectVersions

Essas S3 ações não são especificamente suportadas ao usar o S3 em buckets do nas S3. Ao usar buckets nativos do S3, essas ações são "suportado como normal".

Metadados de usuários da AWS

- Os pares de valores-chave recebidos como parte dos metadados de usuário do S3 não são armazenados no disco juntamente com os dados de objeto na versão atual.
- Cabeçalhos de solicitação com o prefixo "x-amz-meta" são ignorados.

Tags da AWS

- Em pedidos PUT object e Multipart Initiate, cabeçalhos com o prefixo "x-amz-tagging" são ignorados.
- As solicitações para atualizar tags em um arquivo existente (ou seja, um put, get e Delete Requests com a string de consulta ?tagging) são rejeitadas com um erro.

Controle de versão

Não é possível especificar o controle de versão na configuração de mapeamento de bucket.

- Solicitações que incluem especificações de versão não null (a query-string) recebem respostas de erro.
- As solicitações para afetar o estado de controle de versão de um bucket são rejeitadas com erros.

Requisitos de dados nas para acesso ao cliente S3

É importante entender que existem algumas incompatibilidades inerentes ao mapeamento de arquivos e diretórios nas para acesso S3. Pode ser necessário ajustar hierarquias de arquivos nas antes de servi-los usando buckets do nas S3.

Um bucket do S3 nas fornece acesso S3 a um diretório nas mapeando esse diretório usando a sintaxe do bucket do S3, e os arquivos na árvore de diretórios são vistos como objetos. Os nomes de objeto são os nomes de caminho delimitados por barra dos arquivos em relação ao diretório especificado na configuração de bucket S3.

Esse mapeamento impõe alguns requisitos quando arquivos e diretórios são servidos usando buckets do nas S3:

- Os nomes S3 são limitados a 1024 bytes, portanto os arquivos com pathnames mais longos não são acessíveis usando S3.
- Os nomes de arquivo e diretório estão limitados a 255 carateres, portanto, um nome de objeto não pode ter mais de 255 carateres consecutivos sem barra ('/')
- Um nome de caminho SMB delimitado por carateres de barra invertida ('") aparecerá em S3 como um nome de objeto contendo carateres de barra direta ('/') em vez disso.
- Alguns pares de nomes de objetos S3 legais não podem coexistir na árvore de diretórios nas mapeada. Por exemplo, os nomes de objetos S3 legais "part1/part2" e "part1/part2/part3" mapeiam para arquivos que não podem existir simultaneamente na árvore de diretórios nas, pois "part1/part2" é um arquivo no primeiro nome e um diretório no outro.
  - Se "part1/part2" for um arquivo existente, uma criação S3 de "part1/part2/part3" falhará.
  - Se "part1/part2/part3" for um arquivo existente, uma criação ou exclusão S3 de "part1/part2" falhará.
  - Uma criação de objeto S3 que corresponde ao nome de um objeto existente substitui o objeto pré-existente (em buckets não versionados); que se mantém no nas, mas requer uma correspondência exata. Os exemplos acima não causarão a remoção do objeto existente porque enquanto os nomes colidem, eles não coincidem.

Embora um armazenamento de objetos seja projetado para suportar um número muito grande de nomes arbitrários, uma estrutura de diretório nas pode experimentar problemas de desempenho se um número muito grande de nomes for colocado em um diretório. Em particular, nomes sem carateres de barra ('/') serão todos colocados no diretório raiz do mapeamento nas. As aplicações que fazem uso extensivo de nomes que não são "amigáveis ao nas" seriam mais bem hospedadas em um bucket de armazenamento de objetos real em vez de um mapeamento nas.

Habilite o acesso de protocolo S3 a dados nas

A habilitação do acesso ao protocolo S3 consiste em garantir que um SVM habilitado para nas atenda aos mesmos requisitos que um servidor habilitado para S3, incluindo a adição de um servidor de armazenamento de objetos e a verificação dos requisitos de

rede e autenticação.

Para novas instalações do ONTAP, é recomendável habilitar o acesso de protocolo S3 a um SVM depois de configurá-lo para fornecer dados nas aos clientes. Para saber mais sobre a configuração do protocolo nas, consulte:

- "Configuração NFS"
- "Configuração SMB"

Antes de começar

É necessário configurar o seguinte antes de ativar o protocolo S3:

- O protocolo S3 e os protocolos nas desejados - NFS, SMB ou ambos - são licenciados.
- Um SVM é configurado para os protocolos nas desejados.
- Existem servidores NFS e/ou SMB.
- DNS e quaisquer outros serviços necessários estão configurados.
- Os dados nas estão sendo exportados ou compartilhados para sistemas cliente.

Sobre esta tarefa

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. Os certificados CA de três fontes podem ser usados:

- Um novo certificado auto-assinado da ONTAP no SVM.
- Certificado auto-assinado existente do ONTAP no SVM.
- Um certificado de terceiros.

Você pode usar os mesmos LIFs de dados para o bucket do S3/nas que você usa para fornecer dados nas. Se forem necessários endereços IP específicos, "Crie LIFs de dados"consulte . Uma política de dados de serviço do S3 é necessária para habilitar o tráfego de dados do S3 nos LIFs. Você pode modificar a política de serviços existente da SVM para incluir o S3.

Quando você cria o servidor de objetos S3, você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

System Manager

1. Habilite o S3 em uma VM de storage com protocolos nas configurados.
   a. Clique em **armazenamento > armazenamento VMs**, selecione uma VM de armazenamento pronta para nas, clique em Configurações e, em seguida, clique em S3.
   b. Selecione o tipo de certificado. Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.
   c. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
   - A chave secreta não será exibida novamente.
   - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o protocolo S3 é permitido no SVM
   `vserver show -fields allowed-protocols`
2. Registre o certificado de chave pública deste SVM. Se for necessário um novo certificado auto-assinado do ONTAP, "Crie e instale um certificado de CA no SVM"consulte .
3. Atualize a política de dados de serviço
   a. Exibir a política de dados de serviço do SVM
      `network interface service-policy show -vserver svm_name`
   b. Adicione o `data-core` e `data-s3-server services` se não estiverem presentes. E
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. Verifique se as LIFs de dados no SVM atendem aos seus requisitos
   `network interface show -vserver svm_name`
5. Crie o servidor S3
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

- O HTTPS é ativado por padrão na porta 443. Você pode alterar o número da porta com a opção -secure-listener-port. Quando o HTTPS está ativado, os certificados de CA são necessários para uma integração adequada com SSL/TLS. A partir do ONTAP 9.15,1, o TLS 1,3 é compatível com armazenamento de objetos S3.
- O HTTP está desativado por padrão; quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a opção -is-http-enabled ou alterar o número da porta com a opção -listener-port. Quando o HTTP está ativado, todas as solicitações e respostas são enviadas pela rede em texto não criptografado.

1. Verifique se S3 está configurado como desejado
   `vserver object-store-server show`

O seguinte comando verifica os valores de configuração de todos os servidores de armazenamento de objetos

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Crie um bucket do nas S3

Um buckets do nas S3 é um mapeamento entre um nome de bucket do S3 e um caminho nas. Os buckets nas do S3 permitem que você forneça acesso S3 a qualquer parte do namespace SVM com volumes e estrutura de diretórios existentes.

Antes de começar

- Um servidor de objetos S3 é configurado em uma SVM que contém dados nas.
- Os dados nas estão em conformidade com a "Requisitos para acesso ao cliente S3".

Sobre esta tarefa

Você pode configurar buckets do S3 nas para especificar qualquer conjunto de arquivos e diretórios no diretório raiz do SVM.

Você também pode definir políticas de bucket que permitem ou não permitem o acesso aos dados do nas com base em qualquer combinação desses parâmetros:

- Arquivos e diretórios
- Permissões de usuário e grupo
- S3 operações

Por exemplo, você pode querer políticas de bucket separadas que concedem acesso somente leitura a um grande grupo de usuários e outra que permita que um grupo limitado execute operações em um subconjunto desses dados.

Como os "buckets" do nas S3 são mapeamentos e não buckets do S3, as seguintes propriedades dos buckets do S3 padrão não se aplicam aos buckets do nas S3.

- * aggr-list-multiplicador / storage-Service-level / volume / exclude-aggr-list / qos-policy-group * não são criados volumes ou qtree ao configurar buckets do S3 nas.
- **A função é -protegida/está -protegida/está -protegida-na-ONTAP** mais de S3 buckets nas não são protegidos ou espelhados usando o SnapMirror S3, mas em vez disso estarão usando a proteção

SnapMirror regular disponível na granularidade do volume.

- **Os volumes nas de estado de versionamento** geralmente têm a tecnologia Snapshot disponível para salvar versões diferentes. No entanto, o controle de versão não está disponível atualmente em buckets do nas S3.
- *As estatísticas equivalentes usadas em lógica estão disponíveis para volumes nas através dos comandos de volume.

System Manager

Adicione um novo bucket do S3 nas em uma VM de storage habilitada para nas.

1. Clique em **armazenamento > baldes** e, em seguida, clique em **Adicionar**.
2. Insira um nome para o bucket do nas S3 e selecione a VM de armazenamento, não insira um tamanho e clique em **mais Opções**.
3. Introduza um nome de caminho válido ou clique em Procurar para selecionar a partir de uma lista de nomes de caminho válidos. Quando você insere um pathname válido, as opções que não são relevantes para a configuração do nas S3 são ocultadas.
4. Se você já mapeou usuários do S3 para usuários do nas e grupos criados, você pode configurar suas permissões e clique em **Salvar**. Você já deve ter mapeado S3 usuários para usuários nas antes de configurar permissões nesta etapa.

Caso contrário, clique em **Save** para concluir a configuração do bucket do nas do S3.

CLI

Crie um bucket do nas S3 em um SVM que contenha sistemas de arquivos nas. E
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name -type nas -nas-path junction_path [-comment text]`

Exemplo
```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type nas -path /vol1
```

Ative S3 usuários de cliente

Para permitir que os usuários de cliente S3 acessem dados nas, você deve mapear nomes de usuário S3 para os usuários nas correspondentes e conceder permissão para acessar os dados nas usando políticas de serviço de bucket.

Antes de começar

Os nomes de usuário para acesso ao cliente – usuários clientes LINUX/UNIX, Windows e S3 – já devem existir.

Você deve estar ciente de que alguma funcionalidade do S3 é "Não compatível com buckets do nas S3".

Sobre esta tarefa

Mapear um nome de usuário S3 para um USUÁRIO LINUX/UNIX ou Windows correspondente permite que verificações de autorização nos arquivos nas sejam honradas quando esses arquivos são acessados por clientes S3. Os mapeamentos S3 para nas são especificados fornecendo um nome de usuário S3 *pattern*, que pode ser expresso como um único nome ou uma expressão regular POSIX, e um nome de usuário

LINUX/UNIX ou Windows *Replacement*.

Caso não haja nenhum mapeamento de nomes presente, será usado o mapeamento de nomes padrão, onde o próprio nome de usuário S3 será usado como o nome de usuário UNIX e o nome de usuário do Windows. Você pode modificar os mapeamentos de nome de usuário padrão UNIX e Windows com o `vserver object-store-server modify` comando.

Apenas a configuração de mapeamento de nomes local é suportada; o LDAP não é suportado.

Depois que os usuários do S3 são mapeados para usuários nas, você pode conceder permissões aos usuários especificando os recursos (diretórios e arquivos) aos quais eles têm acesso e as ações que eles têm permissão ou não podem executar lá.

System Manager

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos).
   a. Clique em **Storage > Buckets** (armazenamento > baldes*) e selecione a VM de armazenamento habilitada para S3/nas.
   b. Selecione **Configurações** e clique → em **Mapeamento de nomes** (em **usuários e grupos de hosts**).
   c. Nos blocos **S3 para Windows** ou **S3 para UNIX** (ou ambos), clique em **Add** e, em seguida, insira os nomes de usuário **Pattern** (S3) e **Replacement** (nas) desejados.
2. Crie uma política de bucket para fornecer acesso ao cliente.
   a. Clique em **armazenamento > baldes**, clique ⋮ em junto ao balde S3 pretendido e, em seguida, clique em **Editar**.
   b. Clique em **Add** e forneça os valores desejados.
      - **Principal** - forneça S3 nomes de usuário ou use o padrão (todos os usuários).
      - **Efeito** - Selecione **permitir** ou **Negar**.
      - **Ações** - Digite as ações para esses usuários e recursos. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeletObject, ListBucketAcl, GetObjectTagging, PutObjectTagging, DeletObjectTagging, GetBucketLocation, GetBucketVerketversioning, PutBucketVerketverversions e ListBucketsions. Wildcards são aceitos para este parâmetro.
      - **Resources** - Insira caminhos de pasta ou arquivo nos quais as ações são permitidas ou negadas, ou use os padrões (diretório raiz do bucket).

CLI

1. Crie mapeamentos de nomes locais para clientes UNIX ou Windows (ou ambos). E `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - número de prioridade para a avaliação do mapeamento; introduza 1 ou 2.
   - `-pattern` - Um nome de usuário S3 ou uma expressão regular
   - `-replacement` - um nome de usuário do windows ou unix

Exemplos

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Crie uma política de bucket para fornecer acesso ao cliente. E `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - especifica se o acesso é permitido ou negado quando um usuário solicita uma ação.
   - `-action <Action>, …` - especifica operações de recursos que são permitidas ou negadas. O conjunto de operações de recursos que o servidor de armazenamento de objetos suporta atualmente para buckets do nas S3 são: GetObject, PutObject, DeleteObject, ListBucket,

GetBucketAcl, GetObjectAcl e GetBucketLocation. Wildcards são aceitos para este parâmetro.

- `-principal <Objectstore Principal>, …` - valida o usuário que solicita acesso aos usuários ou grupos de servidores de armazenamento de objetos especificados neste parâmetro.
  - Um grupo de servidores de armazenamento de objetos é especificado adicionando um grupo de prefixo/ ao nome do grupo.
  - `-principal` - (o caractere hífen) concede acesso a todos os usuários.
- `-resource <text>, …` - especifica o bucket, pasta ou objeto para o qual permissões de permissão/negação são definidas. Wildcards são aceitos para este parâmetro.
- `[-sid <SID>]` - especifica um comentário de texto opcional para a declaração de política de bucket do servidor de armazenamento de objetos.

Exemplos

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Configuração SMB para Microsoft Hyper-V e SQL Server

Descrição geral da configuração SMB para Microsoft Hyper-V e SQL Server

Os recursos do ONTAP permitem que você ative operações ininterruptas para duas aplicações Microsoft através do protocolo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Use esses procedimentos se quiser implementar operações ininterruptas SMB nas seguintes circunstâncias:

- O acesso básico ao ficheiro de protocolo SMB foi configurado.
- Você deseja habilitar compartilhamentos de arquivo SMB 3,0 ou posteriores residentes em SVMs para armazenar os seguintes objetos:
  - Arquivos de máquina virtual Hyper-V.
  - Bancos de dados do sistema do SQL Server

Informações relacionadas

Para obter informações adicionais sobre a tecnologia ONTAP e a interação com serviços externos, consulte estes relatórios técnicos (TRs): "Relatório técnico da NetApp 4172: Microsoft Hyper-V sobre SMB 3,0 com práticas recomendadas da ONTAP" ** "Relatório técnico do NetApp 4369: Práticas recomendadas para Microsoft SQL Server e SnapManager 7,2 para SQL Server com Clustered Data ONTAP"

Configure o ONTAP para as soluções Microsoft Hyper-V e SQL Server em SMB

Você pode usar compartilhamentos de arquivos SMB 3,0 e posteriores disponíveis

continuamente para armazenar arquivos de máquina virtual Hyper-V ou bancos de dados de sistema SQL Server e bancos de dados de usuários em volumes residentes em SVMs, ao mesmo tempo em que fornece operações ininterruptas (NDOs) para eventos planejados e não planejados.

Microsoft Hyper-V sobre SMB

Para criar uma solução Hyper-V sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de armazenamento para servidores Microsoft Hyper-V. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster), servidores Hyper-V, conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS e, opcionalmente, serviços de backup para proteger os arquivos de máquina virtual armazenados em volumes SVM.

> Os servidores Hyper-V devem ser configurados no Windows 2012 Server ou posterior. As configurações de servidor Hyper-V independentes e em cluster são suportadas.

- Para obter informações sobre como criar clusters da Microsoft e servidores Hyper-V, consulte o site da Microsoft.
- O SnapManager para Hyper-V é uma aplicação baseada em host que facilita os serviços de backup rápidos baseados em cópia Snapshot, projetados para se integrar às configurações do Hyper-V em SMB.

  Para obter informações sobre como usar o SnapManager com Hyper-V em configurações SMB, consulte *SnapManager para Guia de Instalação e Administração do Hyper-V*.

Microsoft SQL Server sobre SMB

Para criar uma solução SQL Server sobre SMB, primeiro você deve configurar o ONTAP para fornecer serviços de storage para a aplicação Microsoft SQL Server. Além disso, você também deve configurar clusters da Microsoft (se estiver usando uma configuração em cluster). Em seguida, você instalaria e configuraria o SQL Server nos servidores Windows e criaria conexões SMB 3,0 continuamente disponíveis para os compartilhamentos hospedados pelo servidor CIFS. Opcionalmente, você pode configurar serviços de backup para proteger os arquivos de banco de dados armazenados em volumes SVM.

> O SQL Server deve ser instalado e configurado no Windows 2012 Server ou posterior. Configurações autônomas e em cluster são compatíveis.

- Para obter informações sobre como criar clusters da Microsoft e instalar e configurar o SQL Server, consulte o site da Microsoft.
- O plug-in do SnapCenter para Microsoft SQL Server é uma aplicação baseada em host que facilita serviços de backup rápidos e baseados em cópias snapshot, projetados para serem integrados a configurações do SQL Server em SMB.

  Para obter informações sobre como usar o plug-in do SnapCenter para Microsoft SQL Server, consulte o "Plug-in do SnapCenter para Microsoft SQL Server" documento.

Operações ininterruptas para Hyper-V e SQL Server em SMB

O que significam operações ininterruptas para Hyper-V e SQL Server em SMB

Operações ininterruptas para Hyper-V e SQL Server sobre SMB referem-se à

combinação de funcionalidades que permitem que os servidores de aplicações e as máquinas virtuais ou bancos de dados contidos permaneçam on-line e forneçam disponibilidade contínua durante muitas tarefas administrativas. Isso inclui tempo de inatividade planejado e não planejado da infraestrutura de storage.

Operações ininterruptas compatíveis para servidores de aplicações em SMB incluem o seguinte:

- Takeover planejado e giveback
- Takeover não planejado
- Atualização
- Realocação de agregados planejada (ARL)
- Migração de LIF e failover
- Movimentação de volume planejada

Protocolos que permitem operações ininterruptas em SMB

Juntamente com o lançamento do SMB 3,0, a Microsoft lançou novos protocolos para fornecer os recursos necessários para dar suporte a operações ininterruptas para Hyper-V e SQL Server sobre SMB.

A ONTAP usa esses protocolos ao fornecer operações ininterruptas para servidores de aplicações em SMB:

- SMB 3,0
- Testemunha

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Há certos conceitos sobre operações ininterruptas (NDOs) que você deve entender antes de configurar sua solução Hyper-V ou SQL Server sobre SMB.

- **Partilha continuamente disponível**

  Um compartilhamento SMB 3,0 que tem o conjunto de propriedades de compartilhamento continuamente disponível. Os clientes que se conetam por meio de compartilhamentos disponíveis continuamente podem sobreviver a eventos disruptivos, como aquisição, giveback e realocação agregada.

- **Nó**

  Um único controlador que é membro de um cluster. Para distinguir entre os dois nós em um par de SFO, um nó é às vezes chamado de *nó local* e o outro nó é às vezes chamado de *nó parceiro* ou *nó remoto*. O principal proprietário do storage é o nó local. O proprietário secundário, que controla o storage quando o proprietário principal falha, é o nó do parceiro. Cada nó é o principal proprietário do storage e o proprietário secundário do storage do parceiro.

- * Realocação de agregados sem interrupções*

  Capacidade de mover um agregado entre nós de parceiros dentro de um par de SFO em um cluster sem interromper as aplicações de clientes.

- **Failover sem interrupções**

Veja *Takeover*.

- **Migração de LIF sem interrupções**

  A capacidade de realizar uma migração de LIF sem interromper aplicativos clientes conectados ao cluster por meio desse LIF. Para conexões SMB, isso só é possível para clientes que se conetam usando SMB 2,0 ou posterior.

- **Operações ininterruptas**

  Capacidade de executar grandes operações de gerenciamento e atualização do ONTAP, bem como resistir a falhas de nós sem interromper as aplicações dos clientes. Esse termo se refere à coleção de funcionalidades de aquisição sem interrupções, atualização sem interrupções e migração sem interrupções como um todo.

- **Atualização sem interrupções**

  Capacidade de atualizar o hardware ou o software do nó sem interrupção da aplicação.

- * Movimento de volume sem interrupções*

  Capacidade de mover um volume livremente pelo cluster sem interromper as aplicações que estão usando o volume. Para conexões SMB, todas as versões do SMB são compatíveis com movimentos de volume sem interrupções.

- * Alças persistentes*

  Uma propriedade do SMB 3,0 que permite que conexões continuamente disponíveis se reconetem de forma transparente ao servidor CIFS em caso de desconexão. Semelhante aos manipuladores duráveis, os manipuladores persistentes são mantidos pelo servidor CIFS por um período de tempo após a perda da comunicação com o cliente de conexão. No entanto, alças persistentes têm mais resiliência do que alças duráveis. Além de dar ao cliente a chance de recuperar o identificador dentro de uma janela de 60 segundos após a reconexão, o servidor CIFS nega acesso a quaisquer outros clientes que solicitem acesso ao arquivo durante essa janela de 60 segundos.

  As informações sobre alças persistentes são espelhadas no armazenamento persistente do parceiro SFO, o que permite que os clientes com alças persistentes desconetadas recuperem as alças duráveis após um evento em que o parceiro SFO assuma a propriedade do armazenamento do nó. Além de fornecer operações ininterruptas no caso de mudanças de LIF (que são duráveis lidar com o suporte), as alças persistentes fornecem operações ininterruptas para takeover, giveback e realocação de agregados.

- **SFO**

  Retorno de agregados para seus locais de origem ao se recuperar de um evento de aquisição.

- **Par SFO**

  Um par de nós cujos controladores estão configurados para servir dados entre si se um dos dois nós deixar de funcionar. Dependendo do modelo do sistema, ambos os controladores podem estar em um único chassi ou os controladores podem estar em um chassi separado. Conhecido como um par de HA em um cluster de dois nós.

- **Aquisição**

  O processo pelo qual o parceiro assume o controle do storage quando o proprietário principal desse storage falha. No contexto de SFO, failover e aquisição são sinônimos.

Como a funcionalidade SMB 3,0 dá suporte a operações ininterruptas por compartilhamentos SMB

O SMB 3,0 fornece funcionalidade crucial que permite o suporte a operações ininterruptas para compartilhamentos Hyper-V e SQL Server em SMB. Isso inclui a `continuously-available` propriedade compartilhar e um tipo de identificador de arquivo conhecido como *identificador persistente* que permite que os clientes SMB recuperem o estado aberto do arquivo e restabeleçam conexões SMB de forma transparente.

Identificadores persistentes podem ser concedidos a clientes compatíveis com SMB 3,0 que se conetam a um compartilhamento com o conjunto de propriedades de compartilhamento continuamente disponível. Se a sessão SMB for desconetada, o servidor CIFS retém informações sobre o estado de identificador persistente. O servidor CIFS bloqueia outras solicitações de cliente durante o período de 60 segundos em que o cliente pode se reconetar, permitindo assim que o cliente com o identificador persistente recupere o identificador após uma desconexão da rede. Os clientes com alças persistentes podem se reconetar usando uma das LIFs de dados na máquina virtual de storage (SVM), seja reconetando pelo mesmo LIF ou por meio de um LIF diferente.

A realocação agregada, a aquisição e a giveback ocorrem entre pares de SFO. Para gerenciar de forma otimizada a desconexão e a reconexão de sessões com arquivos com alças persistentes, o nó do parceiro mantém uma cópia de todas as informações de bloqueio de identificador persistente. Independentemente de o evento ser planejado ou não planejado, o parceiro SFO pode gerenciar as reconexões de identificador persistente sem interrupções. Com essa nova funcionalidade, as conexões SMB 3,0 ao servidor CIFS podem fazer failover de forma transparente e sem interrupções para outro LIF de dados atribuído à SVM em eventos que tradicionalmente têm sido disruptivos.

Embora o uso de alças persistentes permita que o servidor CIFS faça failover transparente em conexões SMB 3,0, se uma falha fizer com que o aplicativo Hyper-V faça failover para outro nó no cluster do Windows Server, o cliente não terá como recuperar as alças de arquivo dessas alças desconetadas. Nesse cenário, os manipuladores de arquivos no estado desconetado podem potencialmente bloquear o acesso do aplicativo Hyper-V se ele for reiniciado em um nó diferente. "'Cluster de failover'" é uma parte do SMB 3,0 que aborda esse cenário fornecendo um mecanismo para invalidar manipulações obsoletas e conflitantes. Usando esse mecanismo, um cluster Hyper-V pode se recuperar rapidamente quando os nós de cluster Hyper-V falham.

O que o protocolo Witness faz para melhorar o failover transparente

O protocolo Witness fornece recursos aprimorados de failover de cliente para compartilhamentos continuamente disponíveis (compartilhamentos CA) SMB 3,0. O Witness facilita o failover mais rápido porque ignora o período de recuperação de failover de LIF. Ele notifica os servidores de aplicativos quando um nó não está disponível sem a necessidade de esperar que a conexão SMB 3,0 expire.

O failover é contínuo, com as aplicações em execução no cliente não cientes de que ocorreu um failover. Se a testemunha não estiver disponível, as operações de failover ainda ocorrem com sucesso, mas o failover sem testemunha é menos eficiente.

O failover aprimorado de testemunhas é possível quando os seguintes requisitos são atendidos:

- Ele só pode ser usado com servidores CIFS compatíveis com SMB 3,0 que tenham SMB 3,0 habilitado.
- Os compartilhamentos devem usar o SMB 3,0 com o conjunto de propriedades de compartilhamento de disponibilidade contínua.

- O parceiro SFO do nó ao qual os servidores de aplicativos estão conetados deve ter pelo menos um LIF de dados operacional atribuído à máquina virtual de armazenamento (SVM) que hospeda dados para os servidores de aplicativos.

> O protocolo testemunha opera entre pares SFO. Como os LIFs podem migrar para qualquer nó dentro do cluster, qualquer nó pode precisar ser a testemunha de seu parceiro SFO. O protocolo Witness não pode fornecer failover rápido de conexões SMB em um determinado nó se os dados de hospedagem SVM para os servidores de aplicações não tiverem um LIF de dados ativo no nó de parceiro. Portanto, cada nó no cluster precisa ter pelo menos um data LIF para cada SVM que hospeda uma dessas configurações.

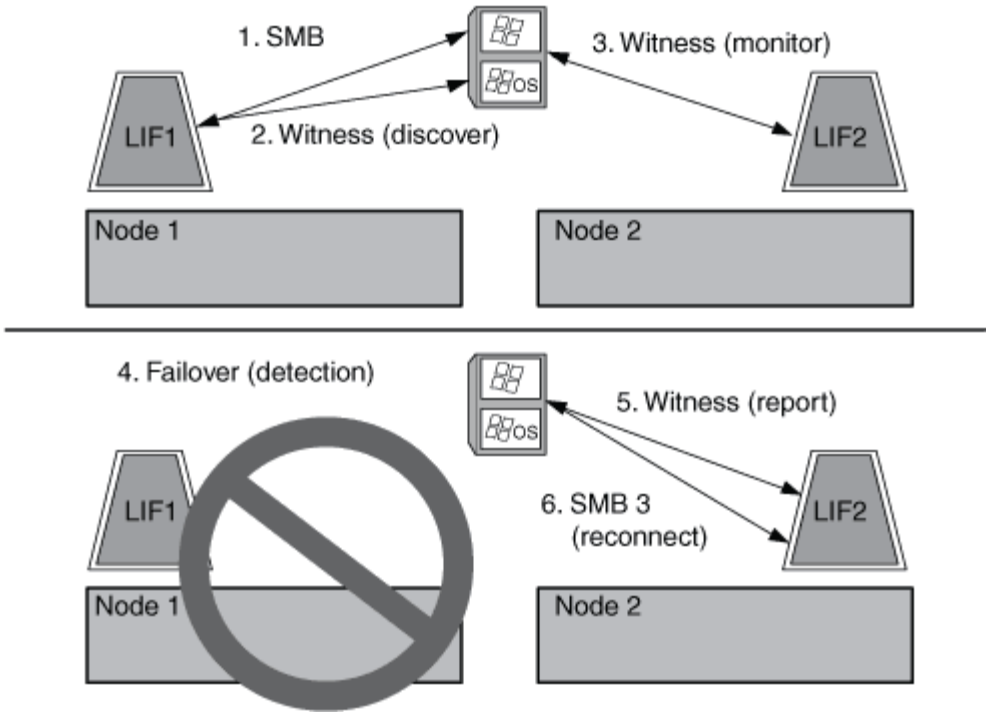
- Os servidores de aplicativos devem se conetar ao servidor CIFS usando o nome do servidor CIFS que é armazenado no DNS em vez de usando endereços IP de LIF individuais.

Como funciona o protocolo testemunha

O ONTAP implementa o protocolo Witness usando o parceiro SFO de um nó como testemunha. Em caso de falha, o parceiro deteta rapidamente a falha e notifica o cliente SMB.

O protocolo Witness fornece failover aprimorado usando o seguinte processo:

1. Quando o servidor de aplicativos estabelece uma conexão SMB continuamente disponível ao Node1, o servidor CIFS informa ao servidor de aplicativos que a testemunha está disponível.
2. O servidor do aplicativo solicita os endereços IP do servidor testemunha de Node1 e recebe uma lista de Node2 (o parceiro SFO) endereços IP de LIF de dados atribuídos à máquina virtual de armazenamento (SVM).
3. O servidor de aplicativos escolhe um dos endereços IP, cria uma conexão testemunha com o Node2 e se Registra para ser notificado se a conexão continuamente disponível no Node1 precisar se mover.
4. Se um evento de failover ocorrer no Node1, o Witness facilita os eventos de failover, mas não está envolvido com a giveback.
5. O Witness deteta o evento de failover e notifica o servidor de aplicativos por meio da conexão Witness que a conexão SMB deve ser movida para Node2.
6. O servidor de aplicativos move a sessão SMB para Node2 e recupera a conexão sem interrupção ao acesso do cliente.



Backups baseados em compartilhamento com VSS remoto

Backups baseados em compartilhamento com a visão geral do VSS remoto

Você pode usar o VSS remoto para executar backups baseados em compartilhamento de arquivos de máquina virtual Hyper-V armazenados em um servidor CIFS.

Microsoft Remote VSS (volume Shadow Copy Services) é uma extensão da infraestrutura Microsoft VSS existente. Com o VSS remoto, a Microsoft estendeu a infraestrutura VSS para dar suporte à cópia sombra de compartilhamentos SMB. Além disso, aplicativos de servidor, como o Hyper-V, podem armazenar arquivos VHD em compartilhamentos de arquivos SMB. Com essas extensões, é possível fazer cópias de sombra consistentes de aplicativos para máquinas virtuais que armazenam dados e arquivos de configuração em compartilhamentos.

Conceitos VSS remotos

Você deve estar ciente de certos conceitos que são necessários para entender como o VSS remoto (volume Shadow Copy Service) é usado por serviços de backup com configurações Hyper-V em SMB.

- **VSS (Serviço de cópia sombra de volume)**

  Uma tecnologia da Microsoft usada para fazer cópias de backup ou snapshots de dados em um volume específico em um determinado momento. O VSS coordena entre servidores de dados, aplicações de backup e software de gerenciamento de storage para dar suporte à criação e gerenciamento de backups consistentes.

- * VSS remoto (Serviço de cópia de sombra de volume remoto)*

  Uma tecnologia da Microsoft usada para fazer cópias de backup baseadas em compartilhamento de dados que estão em um estado consistente com dados em um momento específico em que os dados são acessados por compartilhamentos SMB 3,0. Também conhecido como *volume Shadow Copy Service*.

- **Cópia sombra**

  Um conjunto duplicado de dados contidos no compartilhamento em um instante bem definido no tempo. As cópias de sombra são usadas para criar backups consistentes de dados pontuais, permitindo que o sistema ou as aplicações continuem atualizando os dados nos volumes originais.

- * Conjunto de cópias de sombra*

  Uma coleção de uma ou mais cópias de sombra, com cada cópia de sombra correspondente a um compartilhamento. As cópias de sombra dentro de um conjunto de cópias de sombra representam todos os compartilhamentos que precisam ser copiados na mesma operação. O cliente VSS no aplicativo habilitado para VSS identifica quais cópias de sombra incluir no conjunto.

- * Recuperação automática do conjunto de cópias sombra*

  A parte do processo de backup para aplicativos de backup remotos habilitados para VSS, em que o diretório de réplica que contém as cópias sombra é consistente ponto no tempo. No início do backup, o cliente VSS no aplicativo aciona o aplicativo para fazer pontos de verificação de software sobre os dados programados para backup (os arquivos de máquina virtual no caso do Hyper-V). Em seguida, o cliente VSS permite que os aplicativos continuem. Depois que o conjunto de cópias de sombra é criado, o VSS remoto torna o conjunto de cópias de sombra gravável e expõe a cópia gravável para os aplicativos. O aplicativo prepara o conjunto de cópias de sombra para backup executando uma recuperação automática usando o ponto de verificação de software feito anteriormente. A recuperação automática traz as cópias de sombra para um estado consistente, desrolando as alterações feitas nos arquivos e diretórios desde que o ponto de verificação foi criado. A recuperação automática é uma etapa opcional para backups habilitados para VSS.

- **ID de cópia sombra**

  Um GUID que identifica exclusivamente uma cópia de sombra.

- **ID do conjunto de cópias sombra**

  Um GUID que identifica exclusivamente uma coleção de IDs de cópia de sombra para o mesmo servidor.

- **SnapManager para Hyper-V**

  O software que automatiza e simplifica as operações de backup e restauração para o Microsoft Windows Server 2012 Hyper-V. o SnapManager para Hyper-V usa o VSS remoto com recuperação automática para fazer backup de arquivos Hyper-V em compartilhamentos SMB.

Informações relacionadas

Conceitos-chave sobre operações ininterruptas para Hyper-V e SQL Server sobre SMB

Backups baseados em compartilhamento com VSS remoto

Exemplo de uma estrutura de diretório usada pelo VSS remoto

O VSS remoto percorre a estrutura de diretórios que armazena arquivos de máquina virtual Hyper-V enquanto cria cópias de sombra. É importante entender o que é uma estrutura de diretório apropriada, para que você possa criar com sucesso backups de arquivos de máquina virtual.

Uma estrutura de diretório suportada para a criação bem-sucedida de cópias sombra está em conformidade

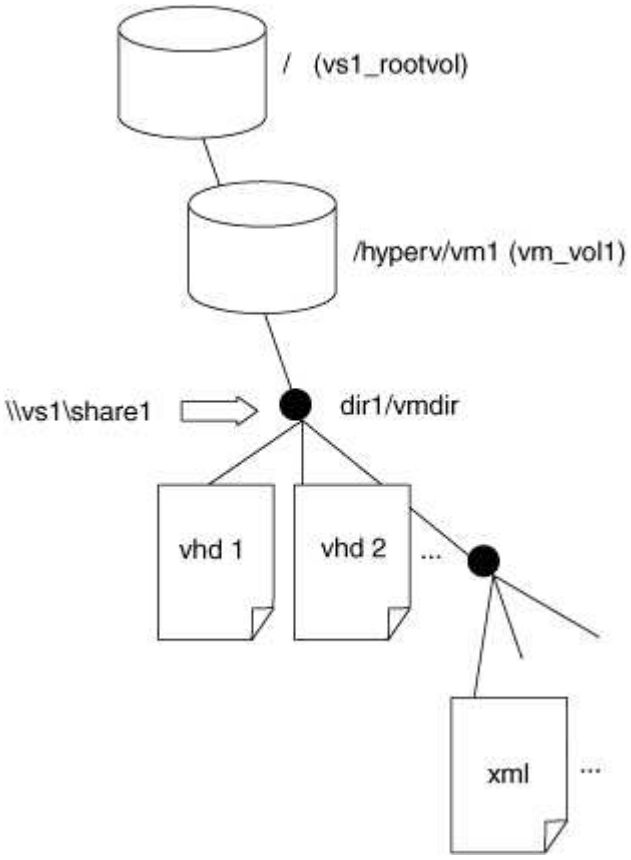
com os seguintes requisitos:

- Somente diretórios e arquivos regulares estão presentes dentro da estrutura de diretórios que é usada para armazenar arquivos de máquina virtual.

  A estrutura de diretórios não contém junções, links ou arquivos não regulares.

- Todos os arquivos de uma máquina virtual residem em um único compartilhamento.
- A estrutura de diretórios que é usada para armazenar arquivos de máquina virtual não excede a profundidade configurada do diretório de cópia de sombra.
- O diretório raiz do compartilhamento contém apenas arquivos ou diretórios de máquina virtual.

Na ilustração a seguir, o volume chamado VM_vol1 é criado com um ponto de junção em `/hyperv/vm1` na máquina virtual de armazenamento (SVM) VS1. Subdiretórios para conter os arquivos da máquina virtual são criados sob o ponto de junção. Os arquivos de máquina virtual do servidor Hyper-V são acessados em share1 que tem o `/hyperv/vm1/dir1/vmdir` caminho . O serviço de cópia de sombra cria cópias de sombra de todos os arquivos de máquina virtual que estão contidos na estrutura de diretórios sob share1 (até a profundidade configurada do diretório de cópia de sombra).



Como o SnapManager para Hyper-V gerencia backups remotos baseados em VSS para Hyper-V em SMB

Você pode usar o SnapManager para Hyper-V para gerenciar serviços de backup baseados em VSS remoto. Há benefícios de usar o serviço de backup gerenciado do SnapManager para Hyper-V para criar conjuntos de backup com uso eficiente de espaço.

As otimizações para o SnapManager para backups gerenciados do Hyper-V incluem o seguinte:

- A integração do SnapDrive com o ONTAP oferece otimização de performance ao descobrir o local de compartilhamento SMB.

  O ONTAP fornece ao SnapDrive o nome do volume em que o compartilhamento reside.

- O SnapManager para Hyper-V especifica a lista de arquivos de máquina virtual nos compartilhamentos SMB que o serviço de cópia sombra precisa copiar.

  Ao fornecer uma lista segmentada de arquivos de máquina virtual, o serviço de cópia de sombra não precisa criar cópias de sombra de todos os arquivos no compartilhamento.

- A máquina virtual de storage (SVM) retém as cópias Snapshot do SnapManager para Hyper-V a serem usadas para restaurações.

  Não há fase de backup. O backup é a cópia Snapshot com uso eficiente de espaço.

O SnapManager para Hyper-V fornece recursos de backup e restauração para o HyperV em SMB usando o seguinte processo:

1. Preparação para a operação de cópia de sombra

   O cliente VSS do aplicativo SnapManager para Hyper-V configura o conjunto de cópias de sombra. O cliente VSS reúne informações sobre quais compartilhamentos incluir no conjunto de cópias de sombra e fornece essas informações ao ONTAP. Um conjunto pode conter uma ou mais cópias de sombra, e uma cópia de sombra corresponde a um compartilhamento.

2. Criando o conjunto de cópias de sombra (se a recuperação automática for usada)

   Para cada compartilhamento incluído no conjunto de cópias de sombra, o ONTAP cria uma cópia de sombra e torna a cópia de sombra gravável.

3. Expondo o conjunto de cópias de sombra

   Depois que o ONTAP cria as cópias de sombra, elas são expostas ao SnapManager para Hyper-V para que os escritores VSS do aplicativo possam executar a recuperação automática.

4. Recuperar automaticamente o conjunto de cópias de sombra

   Durante a criação do conjunto de cópias de sombra, há um período de tempo em que as alterações ativas estão ocorrendo nos arquivos incluídos no conjunto de backup. Os escritores VSS do aplicativo devem atualizar as cópias sombra para garantir que estejam em um estado completamente consistente antes do backup.

   > A forma como a recuperação automática é feita é específica da aplicação. VSS remoto não está envolvido nesta fase.

5. Completar e limpar o conjunto de cópias de sombra

   O cliente VSS notifica o ONTAP após concluir a recuperação automática. O conjunto de cópias de sombra é feito somente leitura e, em seguida, está pronto para backup. Ao usar o SnapManager para Hyper-V para backup, os arquivos em uma cópia Snapshot tornam-se o backup; portanto, para a fase de backup, uma cópia Snapshot é criada para cada volume que contém compartilhamentos no conjunto de backup. Após a conclusão do backup, o conjunto de cópias de sombra é removido do servidor CIFS.

Como a descarga de cópia ODX é usada com Hyper-V e SQL Server em compartilhamentos SMB

A transferência de dados descarregados (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host. A descarga de cópia ODX da ONTAP fornece benefícios de desempenho ao executar operações de cópia no servidor de aplicações através da instalação SMB.

Em transferências de arquivos não ODX, os dados são lidos do servidor CIFS de origem e são transferidos através da rede para o computador cliente. O computador cliente transfere os dados de volta pela rede para o servidor CIFS de destino. Em resumo, o computador cliente lê os dados da origem e grava-os no destino. Com as transferências de arquivos ODX, os dados são copiados diretamente da origem para o destino.

Como as cópias descarregadas do ODX são realizadas diretamente entre o armazenamento de origem e destino, há benefícios significativos de desempenho. Os benefícios de desempenho obtidos incluem tempo de cópia mais rápido entre a origem e o destino, utilização reduzida de recursos (CPU, memória) no cliente e utilização reduzida da largura de banda de e/S de rede.

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:
```

- Intra-volume

  Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e mesma máquina virtual de storage (SVM)

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

  Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

  O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

Casos de uso específicos para descarga de cópia ODX com soluções Hyper-V incluem o seguinte:

- Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conetados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o armazenamento de origem e destino estiver no mesmo cluster.

> Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

Casos de uso específicos para descarga de cópia ODX com soluções SQL Server incluem o seguinte:

- Você pode usar a descarga de cópia ODX para exportar e importar bancos de dados SQL Server entre compartilhamentos SMB mapeados ou entre compartilhamentos SMB e LUNs iSCSI conetados no mesmo cluster.
- A descarga de cópia ODX é usada para exportações e importações de banco de dados se o armazenamento de origem e destino estiver no mesmo cluster.

Requisitos e considerações de configuração

Requisitos de ONTAP e licenciamento

Você precisa estar ciente de certos requisitos de licenciamento e ONTAP ao criar soluções SQL Server ou Hyper-V em SMB para operações ininterruptas em SVMs.

Requisitos de versão do ONTAP

- Hyper-V em SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para Hyper-V executados no Windows 2012 ou posterior.

- SQL Server sobre SMB

  O ONTAP é compatível com operações ininterruptas por compartilhamentos SMB para SQL Server 2012 ou posterior executados no Windows 2012 ou posterior.

Para obter as informações mais recentes sobre versões com suporte do ONTAP, Windows Server e SQL Server para operações ininterruptas em compartilhamentos SMB, consulte a Matriz de interoperabilidade.

"Ferramenta de Matriz de interoperabilidade do NetApp"

Requisitos de licenciamento

São necessárias as seguintes licenças:

- CIFS
- FlexClone (somente para Hyper-V em SMB)

  Esta licença é necessária se o VSS remoto for usado para backups. O serviço de cópia de sombra usa o

FlexClone para criar cópias pontuais de arquivos que são então usados ao criar um backup.

Uma licença do FlexClone é opcional se você usar um método de backup que não use o VSS remoto.

A licença FlexClone está incluída no "ONTAP One". Se não tiver o ONTAP One, deverá "verifique se as licenças necessárias estão instaladas", e, se necessário"instale-os", .

Requisitos de LIF de rede e dados

Você precisa estar ciente de certos requisitos de rede e de LIF de dados ao criar configurações do SQL Server ou Hyper-V em SMB para operações ininterruptas).

Requisitos de protocolo de rede

- São suportadas redes IPv4G e IPv6G.
- SMB 3,0 ou posterior é necessário.

  O SMB 3,0 fornece a funcionalidade necessária para criar as conexões SMB continuamente disponíveis necessárias para oferecer operações ininterruptas.

- Os servidores DNS devem conter entradas que mapeiam o nome do servidor CIFS para os endereços IP atribuídos aos LIFs de dados na máquina virtual de armazenamento (SVM).

  Os servidores de aplicativos Hyper-V ou SQL Server normalmente fazem várias conexões em várias LIFs de dados ao acessar arquivos de máquina virtual ou banco de dados. Para uma funcionalidade adequada, os servidores de aplicativos devem fazer essas várias conexões SMB usando o nome do servidor CIFS em vez de fazer várias conexões com vários endereços IP exclusivos.

  Witness também requer o uso do nome DNS do servidor CIFS em vez de endereços IP LIF individuais.

  A partir do ONTAP 9.4, você pode melhorar a taxa de transferência e a tolerância a falhas para as configurações Hyper-V e SQL Server em SMB, ativando o Multichannel SMB. Para fazer isso, você deve ter várias NICs de 1G, 10G ou maiores implantados no cluster e nos clientes.

Requisitos de LIF de dados

- O SVM que hospeda a solução de servidor de aplicações em SMB precisa ter pelo menos um LIF de dados operacionais em cada nó do cluster.

  Os LIFs de dados do SVM podem fazer failover para outras portas de dados no cluster, incluindo nós que não estão hospedando dados acessados pelos servidores de aplicações. Além disso, como o nó testemunha é sempre o parceiro SFO de um nó ao qual o servidor de aplicativos está conetado, cada nó no cluster é um nó de testemunha potencial.

- Os LIFs de dados não devem ser configurados para reverter automaticamente.

  Após um evento de aquisição ou giveback, você deve reverter manualmente os LIFs de dados para suas portas domésticas.

- Todos os endereços IP de LIF de dados devem ter uma entrada no DNS e todas as entradas devem ser resolvidas para o nome do servidor CIFS.

  Os servidores de aplicativos devem se conetar a compartilhamentos SMB usando o nome do servidor CIFS. Não configure os servidores de aplicativos para fazer conexões usando os endereços IP LIF.

- Se o nome do servidor CIFS for diferente do nome SVM, as entradas DNS deverão ser resolvidas para o nome do servidor CIFS.

Requisitos de volume e servidor SMB para Hyper-V em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações Hyper-V em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de máquina do Hyper-V, crie um SVM separado para esses dados.

- A autenticação Kerberos e NTLM devem ser permitidas no domínio ao qual o servidor SMB pertence.

  O ONTAP não anuncia o serviço Kerberos para VSS remoto; portanto, o domínio deve ser definido para permitir NTLM.

- A funcionalidade de cópia sombra deve estar ativada.

  Esta funcionalidade está ativada por predefinição.

- A conta de domínio do Windows que o serviço de cópia de sombra usa ao criar cópias de sombra deve ser membro do grupo de administradores locais do servidor SMB ou operadores de backup.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de

segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Para que as operações de cópia de sombra sejam bem-sucedidas, você precisa ter espaço disponível suficiente no volume.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos de volume e servidor SMB para SQL Server em SMB

Você precisa estar ciente de certos requisitos de volume e servidor SMB ao criar configurações do SQL Server em SMB para operações ininterruptas.

Requisitos de servidor SMB

- O SMB 3,0 deve estar ativado.

  Esta opção está ativada por predefinição.

- A opção de servidor CIFS de usuário UNIX padrão deve ser configurada com uma conta de usuário UNIX válida.

  Os servidores de aplicativos usam a conta de máquina ao criar uma conexão SMB. Como todo o acesso SMB requer que o usuário do Windows mapeie com êxito para uma conta de usuário UNIX ou para a conta de usuário UNIX padrão, o ONTAP deve ser capaz de mapear a conta de máquina do servidor de aplicativos para a conta de usuário UNIX padrão.

  Além disso, o SQL Server usa um usuário de domínio como a conta de serviço do SQL Server. A conta de serviço também deve ser mapeada para o usuário UNIX padrão.

- As referências de nó automáticas devem ser desativadas (esta funcionalidade está desativada por predefinição).

  Se você quiser usar referências de nó automáticas para acesso a dados que não sejam arquivos de banco de dados do SQL Server, você deve criar um SVM separado para esses dados.

- A conta de usuário do Windows usada para instalar o SQL Server no ONTAP deve ser atribuída ao privilégio SeSecurityPrivilege.

  Este privilégio é atribuído ao grupo de administradores/BUILTIN local do servidor SMB.

Requisitos de volume

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer NDOs para servidores de aplicativos usando conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Não é possível alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para NDOs em

compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para NDOs em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que as operações de backup do SnapCenter Plug-in para Microsoft SQL Server sejam bem-sucedidas, você deve ter espaço disponível suficiente no volume.

  O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

Informações relacionadas

"Microsoft TechNet Library: technet.microsoft.com/en-us/library/"

Requisitos e considerações de compartilhamento continuamente disponíveis para Hyper-V sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos disponíveis continuamente para configurações do Hyper-V em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Se você quiser usar serviços de backup habilitados para VSS remoto, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham junções.

  No caso de recuperação automática, a criação de cópia sombra falha se uma junção for encontrada ao atravessar o compartilhamento. No caso não auto-recuperação, a criação de cópia sombra não falha, mas a junção não aponta para nada.

- Se você quiser usar serviços de backup habilitados para VSS remoto com recuperação automática, não será possível colocar arquivos Hyper-V em compartilhamentos que contenham o seguinte:
  - Links simbólicos, hardlinks ou widelinks
  - Arquivos não regulares

    A criação de cópia sombra falha se houver links ou arquivos não regulares na cópia compartilhar para sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

  - Para que as operações de cópia sombra tenham sucesso, você deve ter espaço disponível suficiente

no volume (somente para Hyper-V sobre SMB).

O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra. Esse requisito só se aplica a cópias sombra com recuperação automática.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos continuamente disponíveis usados pelos servidores de aplicativos:
  - Diretório base
  - Armazenamento em cache de atributos
  - BranchCache

Considerações

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações Hyper-V em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` parâmetro definido como `Yes`.

Requisitos e considerações de compartilhamento continuamente disponíveis para SQL Server sobre SMB

Você precisa estar ciente de certos requisitos e considerações ao configurar compartilhamentos continuamente disponíveis para configurações do SQL Server em SMB que dão suporte a operações ininterruptas.

Compartilhar requisitos

- Os volumes usados para armazenar arquivos de máquina virtual devem ser criados como volumes de estilo de segurança NTFS.

  Para fornecer operações ininterruptas para servidores de aplicações que usam conexões SMB continuamente disponíveis, o volume que contém o compartilhamento deve ser um volume NTFS. Além disso, deve sempre ter sido um volume NTFS. Você não pode alterar um volume de estilo de segurança misto ou um volume de estilo de segurança UNIX para um volume de estilo de segurança NTFS e usá-lo diretamente para operações ininterruptas em compartilhamentos SMB. Se você alterar um volume de estilo de segurança misto para um volume de estilo de segurança NTFS e pretender usá-lo para operações ininterruptas em compartilhamentos SMB, você deverá colocar manualmente uma ACL na parte superior do volume e propagar essa ACL para todos os arquivos e pastas contidos. Caso contrário, migrações de máquinas virtuais ou exportações e importações de arquivos de banco de dados onde os arquivos são movidos para outro volume podem falhar se os volumes de origem ou de destino foram criados inicialmente como volumes mistos ou de estilo de segurança UNIX e posteriormente alterados para o estilo de segurança NTFS.

- Os compartilhamentos usados pelos servidores de aplicativos devem ser configurados com o conjunto de propriedades continuamente disponível.

  Os servidores de aplicações que se conectam a compartilhamentos continuamente disponíveis recebem alças persistentes que lhes permitem se reconectarem sem interrupções aos compartilhamentos de SMB

e recuperarem bloqueios de arquivos após eventos disruptivos, como takeover, giveback e realocação de agregados.

- Embora o volume que contém os arquivos do banco de dados possa conter junções, o SQL Server não cruza junções ao criar a estrutura do diretório do banco de dados.
- Para que o plug-in do SnapCenter para operações do Microsoft SQL Server seja bem-sucedido, você deve ter espaço disponível suficiente no volume.

  O volume no qual os arquivos de banco de dados do SQL Server residem deve ser grande o suficiente para manter a estrutura de diretório de banco de dados e todos os arquivos contidos dentro do compartilhamento.

- As seguintes propriedades de compartilhamento não devem ser definidas em compartilhamentos continuamente disponíveis usados pelos servidores de aplicativos:
  - Diretório base
  - Armazenamento em cache de atributos
  - BranchCache

Considerações sobre compartilhamento

- As cotas são suportadas em ações continuamente disponíveis.
- A seguinte funcionalidade não é suportada para configurações do SQL Server em SMB:
  - Auditoria
  - FPolicy
- A verificação de vírus não é realizada em compartilhamentos SMB com o `continuously-availability` conjunto de propriedades de compartilhamento.

Considerações sobre VSS remoto para configurações Hyper-V em SMB

Você precisa estar ciente de certas considerações ao usar soluções de backup habilitadas para VSS remotas para configurações Hyper-V sobre SMB.

Considerações gerais sobre o VSS remoto

- Um máximo de 64 compartilhamentos pode ser configurado por servidor de aplicativos da Microsoft.

  A operação de cópia de sombra falha se houver mais de 64 compartilhamentos em um conjunto de cópias de sombra. Este é um requisito da Microsoft.

- Apenas é permitido um conjunto de cópias de sombra ativo por servidor CIFS.

  Uma operação de cópia sombra falhará se houver uma operação de cópia sombra contínua no mesmo servidor CIFS. Este é um requisito da Microsoft.

- Nenhuma junção é permitida dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.
  - No caso de recuperação automática, a criação de cópia de sombra falhará se uma junção for encontrada ao atravessar o compartilhamento.
  - No caso de recuperação não automática, a criação de cópia sombra não falha, mas a junção não aponta para nada.

Considerações do VSS remoto que se aplicam somente a cópias de sombra com recuperação automática

Certos limites se aplicam apenas a cópias sombra com recuperação automática.

- Uma profundidade máxima de diretório de cinco subdiretórios é permitida para a criação de cópias de sombra.

  Esta é a profundidade do diretório sobre a qual o serviço de cópia sombra cria um conjunto de backup de cópia sombra. A criação de cópia de sombra falhará se os diretórios que contêm arquivo de máquina virtual estiverem aninhados mais profundamente do que cinco níveis. Isto destina-se a limitar a travessia de diretório ao clonar o compartilhamento. A profundidade máxima do diretório pode ser alterada usando uma opção de servidor CIFS.

- A quantidade de espaço disponível no volume deve ser adequada.

  O espaço disponível deve ser pelo menos tão grande quanto o espaço combinado usado por todos os arquivos, diretórios e subdiretórios contidos nos compartilhamentos incluídos no conjunto de backup de cópia sombra.

- Não são permitidos links ou arquivos não regulares dentro da estrutura de diretórios na qual o VSS remoto cria uma cópia de sombra.

  A criação de cópia sombra falha se houver links ou arquivos não regulares no compartilhamento para a cópia sombra. O processo de clone não os suporta.

- Não são permitidas ACLs NFSv4 nos diretórios.

  Embora a criação de cópia sombra retenha NFSv4 ACLs em arquivos, as ACLs NFSv4 nos diretórios são perdidas.

- Um máximo de 60 segundos é permitido criar um conjunto de cópias de sombra.

  As especificações da Microsoft permitem um máximo de 60 segundos para criar o conjunto de cópias de sombra. Se o cliente VSS não puder criar o conjunto de cópias de sombra dentro desse tempo, a operação de cópia de sombra falhará; portanto, isso limita o número de arquivos em um conjunto de cópias de sombra. O número real de arquivos ou máquinas virtuais que podem ser incluídos em um conjunto de backup varia; esse número depende de muitos fatores e deve ser determinado para cada ambiente de cliente.

Requisitos de descarga de cópia ODX para SQL Server e Hyper-V sobre SMB

A descarga de cópia ODX deve ser ativada se você quiser migrar arquivos de máquina virtual ou exportar e importar arquivos de banco de dados diretamente da origem para o local de armazenamento de destino sem enviar dados através dos servidores de aplicativos. Há certos requisitos que você deve entender sobre o uso de descarga de cópia ODX com soluções SQL Server e Hyper-V sobre SMB.

O uso de descarga de cópia ODX proporciona um benefício significativo de desempenho. Esta opção de servidor CIFS está ativada por predefinição.

- O SMB 3,0 deve estar habilitado para usar a descarga de cópia ODX.
- Os volumes de origem devem ter no mínimo 1,25 GB.
- A deduplicação deve ser habilitada em volumes usados com descarga de cópia.

- Se você usar volumes compatados, o tipo de compactação deve ser adaptável e somente o tamanho do grupo de compactação 8K é suportado.

  O tipo de compressão secundária não é suportado

- Para usar a descarga de cópia ODX para migrar convidados Hyper-V dentro e entre discos, os servidores Hyper-V devem ser configurados para usar discos SCSI.

  O padrão é configurar discos IDE, mas a descarga de cópia ODX não funciona quando os convidados são migrados se os discos são criados usando discos IDE.

Recomendações para configurações do SQL Server e Hyper-V em SMB

Para ter certeza de que as configurações do SQL Server e do Hyper-V sobre SMB são robustas e operacionais, você precisa estar familiarizado com as práticas recomendadas ao configurar as soluções.

Recomendações gerais

- Separe os arquivos do servidor de aplicativos dos dados gerais do usuário.

  Se possível, dedique uma máquina virtual de storage inteira (SVM) e seu armazenamento aos dados do servidor de aplicativos.

- Para obter o melhor desempenho, não ative a assinatura SMB em SVMs que são usadas para armazenar os dados do servidor de aplicativos.
- Para melhor desempenho e melhor tolerância a falhas, ative o multicanal SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB.
- Não crie compartilhamentos continuamente disponíveis em compartilhamentos diferentes daqueles usados na configuração Hyper-V ou SQL Server sobre SMB.
- Desative o Change Notify em compartilhamentos usados para disponibilidade contínua.
- Não realize uma movimentação de volume ao mesmo tempo que o ARL (Aggregate Relocation) porque o ARL tem fases que pausam algumas operações.
- Para soluções Hyper-V sobre SMB, use unidades iSCSI convidadas ao criar máquinas virtuais em cluster. Os arquivos compartilhados `.VHDX` não são compatíveis com Hyper-V em SMB em compartilhamentos SMB do ONTAP.

Planeje a configuração Hyper-V ou SQL Server em SMB

Conclua a Planilha de configuração de volume

A Planilha fornece uma maneira fácil de Registrar os valores de que você precisa ao criar volumes para configurações do SQL Server e do Hyper-V em SMB.

Para cada volume, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

  O nome do SVM é o mesmo para todos os volumes.

- Nome do volume
- Nome agregado

  É possível criar volumes em agregados localizados em qualquer nó do cluster.

- Tamanho
- Caminho de junção

Você deve ter em mente o seguinte ao criar volumes usados para armazenar dados do servidor de aplicativos:

- Se o volume raiz não tiver um estilo de segurança NTFS, deve especificar o estilo de segurança como NTFS quando criar o volume.

  Por padrão, os volumes herdam o estilo de segurança do volume raiz da SVM.

- Os volumes devem ser configurados com a garantia de espaço de volume padrão.
- Opcionalmente, você pode configurar a configuração de gerenciamento de espaço de dimensionamento automático.
- Você deve definir a opção que determina a reserva de espaço de cópia Snapshot como `0`.
- A política Snapshot aplicada ao volume deve ser desativada.

  Se a política SVM Snapshot estiver desativada, você não precisará especificar uma política de Snapshot para os volumes. Os volumes herdam a política Snapshot da SVM. Se a política Snapshot do SVM não estiver desativada e estiver configurada para criar cópias Snapshot, você precisará especificar uma política de Snapshot no nível de volume e essa política deverá ser desativada. Os backups habilitados para o serviço de cópia sombra e os backups do SQL Server gerenciam a criação e exclusão de cópias Snapshot.

- Não é possível configurar espelhos de compartilhamento de carga para os volumes.

Os caminhos de junção nos quais você planeja criar compartilhamentos que os servidores de aplicativos usam devem ser escolhidos para que não haja volumes juntados abaixo do ponto de entrada de compartilhamento.

Por exemplo, se você quiser armazenar arquivos de máquina virtual em quatro volumes denominados "'vol1"", "'vol2", "'vol3" e "'vol4"", você pode criar o namespace mostrado no exemplo. Em seguida, é possível criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/data1/vol1`, `/data1/vol2`, `/data2/vol3` E `/data2/vol4`.

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- -------------------    -----------
vs1     data1        true     /data1                RW_volume
vs1     vol1         true     /data1/vol1           RW_volume
vs1     vol2         true     /data1/vol2           RW_volume
vs1     data2        true     /data2                RW_volume
vs1     vol3         true     /data2/vol3           RW_volume
vs1     vol4         true     /data2/vol4           RW_volume
```

Tipos de informação	Valores
Volume 1: Nome do volume, agregado, tamanho, caminho de junção	
Volume 2: Nome do volume, agregado, tamanho, caminho de junção	
Volume 3: Nome do volume, agregado, tamanho, caminho de junção	
Volume 4: Nome do volume, agregado, tamanho, caminho de junção	
Volume 5: Nome do volume, agregado, tamanho, caminho de junção	
Volume 6: Nome do volume, agregado, tamanho, caminho de junção	
Volumes adicionais: Nome do volume, agregado, tamanho, caminho de junção	

Conclua a Planilha de configuração do compartilhamento SMB

Use esta Planilha para Registrar os valores de que você precisa ao criar compartilhamentos SMB continuamente disponíveis para configurações do SQL Server e do Hyper-V sobre SMB.

Informações sobre as propriedades de compartilhamentos SMB e configurações

Para cada compartilhamento, você deve especificar as seguintes informações:

- Nome da máquina virtual de storage (SVM)

  O nome do SVM é o mesmo para todos os compartilhamentos

- Nome da partilha
- Caminho
- Compartilhar propriedades

  Você deve configurar as duas propriedades de compartilhamento a seguir:

  - `oplocks`
  - `continuously-available`

As seguintes propriedades de compartilhamento não devem ser definidas:

- `homedirectory attributecache`

- `branchcache`
- `access-based-enumeration`
  - Links simbólicos devem ser desativados (o valor para o `-symlink-properties` parâmetro deve ser nulo ["]).

Informações sobre caminhos de compartilhamento

Se você estiver usando o VSS remoto para fazer backup de arquivos Hyper-V, a escolha de caminhos de compartilhamento a serem usados ao fazer conexões SMB dos servidores Hyper-V para os locais de armazenamento onde os arquivos da máquina virtual são armazenados é importante. Embora os compartilhamentos possam ser criados em qualquer ponto do namespace, os caminhos para compartilhamentos que os servidores Hyper-V usam não devem conter volumes juntados. As operações de cópia sombra não podem ser executadas em caminhos de partilha que contenham pontos de junção.

O SQL Server não pode cruzar junções ao criar a estrutura do diretório do banco de dados. Você não deve criar caminhos de compartilhamento para o servidor SQL que contenham pontos de junção.

Por exemplo, dado o namespace mostrado, se você quiser armazenar arquivos de máquina virtual ou arquivos de banco de dados nos volumes "'vol1", "'vol2", "'vol3"" e "'vol4", você deve criar compartilhamentos para os servidores de aplicativos nos seguintes caminhos: `/data1/vol1`, , `/data1/vol2`, `/data2/vol3` E `/data2/vol4`.

```
                    Junction                       Junction
Vserver Volume      Active   Junction Path         Path Source
------- ----------- -------- -------------------   -----------
vs1     data1        true     /data1               RW_volume
vs1     vol1         true     /data1/vol1          RW_volume
vs1     vol2         true     /data1/vol2          RW_volume
vs1     data2        true     /data2               RW_volume
vs1     vol3         true     /data2/vol3          RW_volume
vs1     vol4         true     /data2/vol4          RW_volume
```

Embora seja possível criar compartilhamentos `/data1` nos caminhos e `/data2` para gerenciamento administrativo, não configure os servidores de aplicativos para usar esses compartilhamentos para armazenar dados.

Folha de trabalho de planeamento

Tipos de informação	Valores
Volume 1: Nome e caminho do compartilhamento SMB	
Volume 2: Nome e caminho do compartilhamento SMB	
Volume 3: Nome e caminho do compartilhamento SMB	

Tipos de informação	Valores
Volume 4: Nome e caminho do compartilhamento SMB	
Volume 5: Nome e caminho do compartilhamento SMB	
Volume 6: Nome e caminho do compartilhamento SMB	
Volume 7: Nome e caminho do compartilhamento SMB	
Volumes adicionais: Nomes e caminhos de compartilhamento SMB	

Crie configurações de ONTAP para operações ininterruptas com Hyper-V e SQL Server em SMB

Crie configurações do ONTAP para operações ininterruptas com a visão geral do Hyper-V e do SQL Server sobre SMB

Há várias etapas de configuração do ONTAP que você deve executar para se preparar para instalações do Hyper-V e SQL Server que fornecem operações ininterruptas em SMB.

Antes de criar a configuração do ONTAP para operações ininterruptas com o Hyper-V e o SQL Server em SMB, as seguintes tarefas devem ser concluídas:

- Os serviços de tempo devem ser configurados no cluster.
- É necessário configurar uma rede para o SVM.
- É necessário criar o SVM.
- As interfaces de LIF de dados devem ser configuradas na SVM.
- O DNS deve ser configurado na SVM.
- Os serviços de nomes desejados devem ser configurados para o SVM.
- O servidor SMB deve ser criado.

Informações relacionadas

Planeje a configuração Hyper-V ou SQL Server em SMB

Requisitos e considerações de configuração

Verifique se a autenticação Kerberos e NTLMv2 são permitidas (Hyper-V sobre compartilhamentos SMB)

Operações ininterruptas para Hyper-V em SMB exigem que o servidor CIFS em um SVM de dados e o servidor Hyper-V permitam a autenticação Kerberos e NTLMv2. Você deve

verificar as configurações no servidor CIFS e nos servidores Hyper-V que controlam quais métodos de autenticação são permitidos.

Sobre esta tarefa

A autenticação Kerberos é necessária ao fazer uma conexão de compartilhamento continuamente disponível. Parte do processo VSS remoto usa autenticação NTLMv2.1X. Portanto, conexões usando ambos os métodos de autenticação devem ser suportadas para configurações Hyper-V em SMB.

As seguintes configurações devem ser configuradas para permitir a autenticação Kerberos e NTLMv2:

- As políticas de exportação para SMB devem ser desativadas na máquina virtual de storage (SVM).

A autenticação Kerberos e NTLMv2 estão sempre ativadas em SVMs, mas as políticas de exportação podem ser usadas para restringir o acesso com base no método de autenticação.

As políticas de exportação para SMB são opcionais e estão desativadas por padrão. Se as políticas de exportação estiverem desativadas, a autenticação Kerberos e NTLMv2 serão permitidas em um servidor CIFS por padrão.

- O domínio ao qual o servidor CIFS e os servidores Hyper-V pertencem deve permitir a autenticação Kerberos e NTLMv2.

A autenticação Kerberos é ativada por padrão em domínios do ative Directory. No entanto, a autenticação NTLMv2.1X pode ser desativada, utilizando as definições de Política de Segurança ou políticas de Grupo.

Passos

1. Execute o seguinte procedimento para verificar se as políticas de exportação estão desativadas no SVM:
   a. Defina o nível de privilégio como avançado:

      ```
      set -privilege advanced
      ```

   b. Verifique se a `-is-exportpolicy-enabled` opção de servidor CIFS está definida como `false`:

      ```
      vserver cifs options show -vserver vserver_name -fields vserver,is-
      exportpolicy-enabled
      ```

   c. Voltar ao nível de privilégio de administrador:

      ```
      set -privilege admin
      ```

2. Se as políticas de exportação para SMB não estiverem desativadas, desative-as:

   ```
   vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled
   false
   ```

3. Verifique se a autenticação NTLMv2 e Kerberos são permitidas no domínio.

   Para obter informações sobre como determinar quais métodos de autenticação são permitidos no domínio, consulte a Biblioteca Microsoft TechNet.

4. Se o domínio não permitir a autenticação NTMLv2.1x, ative a autenticação NTLMv2.1x utilizando um dos métodos descritos na documentação da Microsoft.

Exemplo

Os comandos a seguir verificam se as políticas de exportação para SMB estão desativadas no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ----------------------
vs1      false

cluster1::*> set -privilege admin
```

Verifique se as contas de domínio são mapeadas para o usuário UNIX padrão

Hyper-V e SQL Server usam contas de domínio para criar conexões SMB para compartilhamentos continuamente disponíveis. Para criar a conexão com êxito, a conta do computador deve mapear com êxito para um usuário UNIX. A maneira mais conveniente de fazer isso é mapear a conta do computador para o usuário UNIX padrão.

Sobre esta tarefa

Hyper-V e SQL Server usam as contas de computador de domínio para criar conexões SMB. Além disso, o SQL Server usa uma conta de usuário de domínio como a conta de serviço que também faz conexões SMB.

Quando você cria uma máquina virtual de armazenamento (SVM), o ONTAP cria automaticamente o usuário padrão chamado "'pcuser'" (com um UID do `65534`) e o grupo chamado "'pcuser'" (com um GID do `65534`) e adiciona o usuário padrão ao grupo "'pcuser'". Se você estiver configurando uma solução Hyper-V sobre SMB em um SVM que existia antes de atualizar o cluster para o Data ONTAP 8.2, o usuário e o grupo padrão podem não existir. Se não o fizerem, você deverá criá-los antes de configurar o usuário UNIX padrão do servidor CIFS.

Passos

1. Determine se há um usuário UNIX padrão:

   vserver cifs options show -vserver *vserver_name*

2. Se a opção de usuário padrão não estiver definida, determine se há um usuário UNIX que pode ser designado como o usuário UNIX padrão:

   vserver services unix-user show -vserver *vserver_name*

3. Se a opção de usuário padrão não estiver definida e não houver um usuário UNIX que possa ser designado como usuário UNIX padrão, crie o usuário UNIX padrão e o grupo padrão e adicione o usuário padrão ao grupo.

   Geralmente, o usuário padrão recebe o nome de usuário ""pcuser"" e deve ser atribuído o UID de `65534`.

O grupo padrão geralmente recebe o nome do grupo ""pcuser"". O GID atribuído ao grupo deve ser `65534`.

a. Criar o grupo padrão
vserver services unix-group create -vserver *vserver_name* -name pcuser -id 65534

b. Crie o usuário padrão e adicione o usuário padrão ao grupo padrão
vserver services unix-user create -vserver *vserver_name* -user pcuser -id 65534 -primary-gid 65534

c. Verifique se o usuário padrão e o grupo padrão estão configurados corretamente
vserver services unix-user show -vserver *vserver_name*
vserver services unix-group show -vserver *vserver_name* -members

4. Se o usuário padrão do servidor CIFS não estiver configurado, execute o seguinte procedimento:

a. Configurar o utilizador predefinido:

vserver cifs options modify -vserver *vserver_name* `-default-unix-user pcuser*`

b. Verifique se o usuário UNIX padrão está configurado corretamente:

vserver cifs options show -vserver *vserver_name*

5. Para verificar se a conta do computador do servidor de aplicativos mapeia corretamente para o usuário padrão, mapeie uma unidade para um compartilhamento residente no SVM e confirme o mapeamento do usuário do Windows para o UNIX usando o `vserver cifs session show` comando.

Para obter mais informações sobre como usar esse comando, consulte as páginas man.

Exemplo

Os comandos a seguir determinam que o usuário padrão do servidor CIFS não está definido, mas determina que o usuário "'pcuser'" e o grupo "'pcuser'" existem. O usuário "'pcuser'" é atribuído como o usuário padrão do servidor CIFS na SVM VS1.

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
```

```
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

Verifique se o estilo de segurança do volume raiz SVM está definido como NTFS

Para garantir que as operações ininterruptas para Hyper-V e SQL Server sobre SMB sejam bem-sucedidas, os volumes devem ser criados com o estilo de segurança NTFS. Como o estilo de segurança do volume raiz é aplicado por padrão aos volumes criados na máquina virtual de armazenamento (SVM), o estilo de segurança do volume raiz deve ser definido como NTFS.

Sobre esta tarefa

- Você pode especificar o estilo de segurança do volume raiz no momento em que você criar o SVM.
- Se o SVM não for criado com o volume raiz definido como estilo de segurança NTFS, você poderá alterar o estilo de segurança mais tarde usando o `volume modify` comando.

Passos

1. Determine o estilo de segurança atual do volume raiz da SVM:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. Se o volume raiz não for um volume de estilo de segurança NTFS, altere o estilo de segurança para NTFS:

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. Verifique se o volume raiz SVM está definido como estilo de segurança NTFS:

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

Exemplo

Os comandos a seguir verificam se o estilo de segurança do volume raiz é NTFS no SVM VS1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

Verifique se as opções de servidor CIFS necessárias estão configuradas

Você deve verificar se as opções de servidor CIFS necessárias estão habilitadas e configuradas de acordo com os requisitos para operações ininterruptas para Hyper-V e SQL Server sobre SMB.

Sobre esta tarefa

- O SMB 2.x e o SMB 3,0 devem estar ativados.
- A descarga de cópia ODX deve ser habilitada para usar a descarga de cópia que melhora o desempenho.
- Os serviços VSS Shadow Copy devem estar ativados se a solução Hyper-V over SMB utilizar serviços de cópia de segurança ativados por VSS remoto (apenas Hyper-V).

Passos

1. Verifique se as opções de servidor CIFS necessárias estão ativadas na máquina virtual de armazenamento (SVM):
   a. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

b. Introduza o seguinte comando:

```
vserver cifs options show -vserver vserver_name
```

As seguintes opções devem ser definidas como `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Apenas Hyper-V)

2. Se alguma das opções não estiver definida como `true`, execute o seguinte procedimento:
   a. Defina-os como `true` utilizando o `vserver cifs options modify` comando.
   b. Verifique se as opções estão definidas `true` usando o `vserver cifs options show` comando.
3. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

Os comandos a seguir verificam se as opções necessárias para a configuração Hyper-V sobre SMB estão habilitadas no SVM VS1. No exemplo, a descarga de cópia ODX deve estar habilitada para atender aos requisitos de opção.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

Configure o SMB Multichannel para desempenho e redundância

A partir do ONTAP 9.4, você pode configurar o multicanais SMB para fornecer várias conexões entre o ONTAP e os clientes em uma única sessão SMB. Isso melhora a taxa de transferência e a tolerância a falhas para configurações Hyper-V e SQL Server em SMB.

Antes de começar

Você pode usar a funcionalidade de multicanal SMB somente quando os clientes negociam em versões SMB 3,0 ou posteriores. Por padrão, o SMB 3,0 e posterior está habilitado no servidor SMB do ONTAP.

Sobre esta tarefa

Os clientes SMB detetam e usam automaticamente várias conexões de rede se uma configuração adequada for identificada no cluster ONTAP.

O número de conexões simultâneas em uma sessão SMB depende das NICs que você implantou:

- **1G NICs em cliente e cluster ONTAP**

  O cliente estabelece uma conexão por NIC e liga a sessão a todas as conexões.

- **10G e placas de rede de maior capacidade no cluster cliente e ONTAP**

  O cliente estabelece até quatro conexões por NIC e liga a sessão a todas as conexões. O cliente pode estabelecer conexões em várias NICs de 10G GB e maior capacidade.

Você também pode modificar os seguintes parâmetros (privilégio avançado):

- `-max-connections-per-session`

  O número máximo de conexões permitido por sessão multicanal. O padrão é 32 conexões.

  Se você quiser habilitar mais conexões do que o padrão, você deve fazer ajustes comparáveis à configuração do cliente, que também tem um padrão de 32 conexões.

- `-max-lifs-per-session`

  O número máximo de interfaces de rede anunciadas por sessão multicanal. O padrão é 256 interfaces de rede.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Ative SMB Multichannel no servidor SMB:

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. Verifique se o ONTAP está relatando sessões multicanais SMB:

```
vserver cifs session show
```

4. Voltar ao nível de privilégio de administrador:

```
set -privilege admin
```

Exemplo

O exemplo a seguir exibe informações sobre todas as sessões SMB, mostrando várias conexões para uma única sessão:

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User         Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

O exemplo a seguir exibe informações detalhadas sobre uma sessão SMB com session-id 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                          Node: node1
                    Session ID: 1
                Connection IDs: 138683,138684,138685
              Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
       Workstation IP Address: 10.1.1.1
      Authentication Mechanism: NTLMv1
         User Authenticated as: domain-user
                  Windows User: DOMAIN\administrator
                     UNIX User: root
                   Open Shares: 2
                    Open Files: 5
                    Open Other: 0
                Connected Time: 5s
                     Idle Time: 5s
              Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

Criar volumes de dados NTFS

Você deve criar volumes de dados NTFS na máquina virtual de armazenamento (SVM) antes de poder configurar compartilhamentos continuamente disponíveis para uso com

Hyper-V ou SQL Server em servidores de aplicativos SMB. Use a Planilha de configuração de volume para criar seus volumes de dados.

Sobre esta tarefa

Há parâmetros opcionais que você pode usar para personalizar um volume de dados. Para obter mais informações sobre a personalização de volumes, consulte "Gerenciamento de storage lógico".

À medida que você cria seus volumes de dados, você não deve criar pontos de junção dentro de um volume que contenha o seguinte:

- Arquivos Hyper-V para os quais o ONTAP faz cópias de sombra
- Arquivos de banco de dados do SQL Server que são copiados usando o SQL Server

> Se você inadvertidamente criar um volume que usa estilo de segurança misto ou UNIX, não poderá alterar o volume para um volume de estilo de segurança NTFS e usá-lo diretamente para criar compartilhamentos continuamente disponíveis para operações ininterruptas. Operações ininterruptas para Hyper-V e SQL Server em SMB não funcionam corretamente, a menos que os volumes usados na configuração sejam criados como volumes de estilo de segurança NTFS. Você deve excluir o volume e recriar o volume com estilo de segurança NTFS, ou pode mapear o volume em um host Windows e aplicar uma ACL na parte superior do volume e propagar a ACL para todos os arquivos e pastas no volume.

Passos

1. Crie o volume de dados inserindo o comando apropriado:

Se você quiser criar um volume em um SVM onde o estilo de segurança do volume raiz é…	Digite o comando…
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
Não NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. Verifique se a configuração do volume está correta:

   `volume show -vserver vserver_name -volume volume_name`

Crie compartilhamentos SMB continuamente disponíveis

Depois de criar seus volumes de dados, você pode criar os compartilhamentos continuamente disponíveis que os servidores de aplicativos usam para acessar a máquina virtual Hyper-V e os arquivos de configuração e os arquivos de banco de dados do SQL Server. Você deve usar a Planilha de configuração de compartilhamento ao criar

compartilhamentos SMB.

Passos

1. Apresenta informações sobre os volumes de dados existentes e os respetivos caminhos de junção:

   volume show -vserver *vserver_name* -junction

2. Crie um compartilhamento SMB continuamente disponível:

   vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

   - Opcionalmente, você pode adicionar um comentário à configuração de compartilhamento.
   - Por padrão, a propriedade de compartilhamento de arquivos off-line é configurada no compartilhamento e está definida como `manual`.
   - O ONTAP cria o compartilhamento com a permissão de compartilhamento padrão do Windows de `Everyone` / `Full Control`.

3. Repita a etapa anterior para todos os compartilhamentos na Planilha de configuração de compartilhamento.
4. Verifique se sua configuração está correta usando o `vserver cifs share show` comando.
5. Configure permissões de arquivo NTFS nos compartilhamentos continuamente disponíveis mapeando uma unidade para cada compartilhamento e configurando permissões de arquivo usando a janela **Propriedades do Windows**.

Exemplo

Os comandos a seguir criam um compartilhamento continuamente disponível chamado "ata2" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os links simbólicos são desativados definindo o `-symlink` parâmetro para `""`:

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

Adicionar o privilégio SeSecurityPrivilege à conta de usuário (para SQL Server de compartilhamentos SMB)

A conta de usuário do domínio usada para instalar o servidor SQL deve ser atribuída ao privilégio ""SeSecurityPrivilege"" para executar determinadas ações no servidor CIFS que exigem Privileges não atribuído por padrão aos usuários do domínio.

O que você vai precisar

A conta de domínio usada para instalar o SQL Server já deve existir.

Sobre esta tarefa

Ao adicionar o privilégio à conta do instalador do SQL Server, o ONTAP pode validar a conta entrando em Contato com o controlador de domínio. O comando pode falhar se o ONTAP não puder entrar em Contato com o controlador de domínio.

Passos

1. Adicione o privilégio "SeSecurityPrivilege":

   vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

   O valor para o `-user-or-group-name` parâmetro é o nome da conta de usuário do domínio usada para instalar o SQL Server.

2. Verifique se o privilégio é aplicado à conta:

   vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

Exemplo

O comando a seguir adiciona o privilégio "'SeSecurityPrivilege" à conta do instalador do SQL Server no domínio DE EXEMPLO para máquina virtual de armazenamento (SVM) VS1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

Configurar a profundidade do diretório de cópia de sombra VSS (para compartilhamentos Hyper-V sobre SMB)

Opcionalmente, você pode configurar a profundidade máxima de diretórios em compartilhamentos SMB nos quais criar cópias sombra. Este parâmetro é útil se você quiser controlar manualmente o nível máximo de subdiretórios nos quais o ONTAP deve criar cópias de sombra.

O que você vai precisar

O recurso de cópia de sombra VSS deve estar ativado.

Sobre esta tarefa

O padrão é criar cópias de sombra para um máximo de cinco subdiretórios. Se o valor estiver definido como `0`, o ONTAP criará cópias de sombra para todos os subdiretórios.

> Embora você possa especificar que a profundidade do diretório do conjunto de cópias de sombra inclua mais de cinco subdiretórios ou todos os subdiretórios, há um requisito da Microsoft de que a criação do conjunto de cópias de sombra deve ser concluída em 60 segundos. A criação do conjunto de cópias de sombra falhará se não puder ser concluída dentro deste período de tempo. A profundidade do diretório de cópia sombra escolhida não deve fazer com que o tempo de criação exceda o limite de tempo.

Passos

1. Defina o nível de privilégio como avançado:

   set -privilege advanced

2. Defina a profundidade do diretório de cópia de sombra VSS para o nível desejado:

   vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

   vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6

3. Voltar ao nível de privilégio de administrador:

   set -privilege admin

Gerenciar configurações do Hyper-V e do SQL Server em SMB

Configurar compartilhamentos existentes para disponibilidade contínua

Você pode modificar compartilhamentos existentes para se tornarem compartilhamentos continuamente disponíveis que os servidores de aplicativos Hyper-V e SQL Server usam para acessar arquivos de configuração e máquina virtual Hyper-V sem interrupções e arquivos de banco de dados do SQL Server.

Sobre esta tarefa

Você não pode usar um compartilhamento existente como um compartilhamento continuamente disponível para operações ininterruptas com servidores de aplicações em SMB se o compartilhamento tiver as seguintes características:

- Se a `homedirectory` propriedade share estiver definida nesse compartilhamento
- Se o compartilhamento contiver links simbólicos ou widelinks habilitados
- Se o compartilhamento contiver volumes juntados abaixo da raiz do compartilhamento

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

As seguintes propriedades de compartilhamento devem ser configuradas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas. Se eles estiverem presentes na lista de propriedades de compartilhamento atuais, eles precisam ser removidos do compartilhamento continuamente disponível:

- `attributecache`
- `branchcache`

Passos

1. Exiba as configurações atuais de parâmetros de compartilhamento e a lista atual de propriedades de compartilhamento configuradas:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. Se necessário, modifique os parâmetros de compartilhamento para desativar links simbólicos e defina arquivos off-line para manual usando o `vserver cifs share modify` comando.
   - Pode desativar os links simbólicos definindo o valor do `-symlink` parâmetro para `""`.
   - Pode definir o `-offline-files` parâmetro para a definição correta especificando `manual`.
3. Adicione a `continuously-available` propriedade da ação e, se necessário, a `oplocks` propriedade da ação:

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

   Se a `oplocks` propriedade share ainda não estiver definida, você deve adicioná-la juntamente com a `continuously-available` propriedade share.

4. Remova quaisquer propriedades de compartilhamento que não sejam suportadas em compartilhamentos disponíveis continuamente:

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

   Você pode remover uma ou mais propriedades de compartilhamento especificando as propriedades de compartilhamento com uma lista delimitada por vírgulas.

5. Verifique se `-symlink` os parâmetros e `-offline-files` estão definidos corretamente:

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. Verifique se a lista de propriedades de compartilhamento configuradas está correta:

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

Exemplos

O exemplo a seguir mostra como configurar um compartilhamento existente chamado "share1" na máquina virtual de armazenamento (SVM) "VS1" para NDOs com um servidor de aplicativos sobre SMB:

- Os links simbólicos são desativados no compartilhamento definindo o `-symlink` parâmetro como `""`.
- O `-offline-file` parâmetro é modificado e definido para `manual`.
- A `continuously-available` propriedade share é adicionada à ação.
- A `oplocks` propriedade da ação já está na lista de propriedades da ação; portanto, ela não precisa ser adicionada.
- A `attributecache` propriedade share é removida da ação.
- A `browsable` propriedade de compartilhamento é opcional para um compartilhamento continuamente disponível usado para NDOs com servidores de aplicativos em SMB e é mantido como uma das propriedades de compartilhamento.

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

Ative ou desative cópias de sombra VSS para backups Hyper-V em SMB

Se você usar um aplicativo de backup com reconhecimento VSS para fazer backup de arquivos de máquina virtual Hyper-V armazenados em compartilhamentos SMB, a cópia de sombra VSS deve estar habilitada. Você pode desativar a cópia de sombra do VSS se não usar aplicativos de backup com reconhecimento VSS. O padrão é ativar a cópia de sombra VSS.

Sobre esta tarefa

Você pode ativar ou desativar cópias de sombra VSS a qualquer momento.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser que cópias de sombra VSS sejam…	Digite o comando…
Ativado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true`
Desativado	`vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false`

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplo

Os comandos a seguir habilitam cópias de sombra do VSS no SVM VS1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

Use estatísticas para monitorar a atividade do Hyper-V e do SQL Server em SMB

Determine quais objetos e contadores de estatísticas estão disponíveis

Antes de obter informações sobre as estatísticas de hash CIFS, SMB, auditoria e BranchCache e monitorar o desempenho, você deve saber quais objetos e contadores estão disponíveis a partir dos quais você pode obter dados.

Passos

1. Defina o nível de privilégio como avançado:

   ```
   set -privilege advanced
   ```

2. Execute uma das seguintes ações:

Se você quiser determinar…	Digite…
Quais objetos estão disponíveis	`statistics catalog object show`
Objetos específicos que estão disponíveis	`statistics catalog object show object` *`object_name`*
Quais contadores estão disponíveis	`statistics catalog counter show object` *`object_name`*

   Consulte as páginas man para obter mais informações sobre quais objetos e contadores estão disponíveis.

3. Voltar ao nível de privilégio de administrador:

   ```
   set -privilege admin
   ```

Exemplos

O comando a seguir exibe descrições de objetos estatísticos selecionados relacionados ao acesso CIFS e SMB no cluster, como visto no nível avançado de privilégio:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

O comando a seguir exibe informações sobre alguns dos contadores para o `cifs` objeto, como visto no nível de privilégio avançado:

> Este exemplo não exibe todos os contadores disponíveis para o `cifs` objeto; a saída é truncada.

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                              vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

Exibir estatísticas SMB no ONTAP

Você pode exibir várias estatísticas SMB para monitorar o desempenho e diagnosticar

problemas.

Passos

1. Use os `statistics start` comandos e opcionais `statistics stop` para coletar uma amostra de dados.
2. Execute uma das seguintes ações:

Se você quiser exibir estatísticas para…	Digite o seguinte comando…
Todas as versões do SMB	**`statistics show -object cifs`**
SMB 1,0	**`statistics show -object smb1`**
SMB 2.x e SMB 3,0	**`statistics show -object smb2`**
Subsistema SMB do nó	**`statistics show -object nblade_cifs`**

Saiba mais sobre os comandos link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-show.html[`statistics show`(em inglês), link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-start.html[`statistics start`(em inglês) e link:https://docs.NetApp.com/US-en/ONTAP-cli/statistics-stop.html[`statistics stop`(em inglês) na referência de comando ONTAP.

Verifique se a configuração é capaz de operações ininterruptas

Use o monitoramento de integridade para determinar se o status de operação sem interrupções está íntegro

O monitoramento de integridade fornece informações sobre o status de integridade do sistema em todo o cluster. O monitor de integridade monitora as configurações Hyper-V e SQL Server em SMB para garantir operações ininterruptas (NDOs) para os servidores de aplicações. Se o estado estiver degradado, pode visualizar detalhes sobre o problema, incluindo a causa provável e as ações de recuperação recomendadas.

Existem vários monitores de saúde. O ONTAP monitora a integridade e a integridade geral do sistema para monitores de integridade individuais. O monitor de integridade da conetividade do nó contém o subsistema CIFS-NDO. O monitor tem um conjunto de políticas de integridade que acionam alertas se certas condições físicas podem causar interrupções e, se houver uma condição disruptiva, gera alertas e fornece informações sobre ações corretivas. Para configurações NDO sobre SMB, alertas são gerados para as duas condições a seguir:

ID de alerta	Gravidade	Condição
HaNotReadyCifsNdo_Alert	Maior	Um ou mais arquivos hospedados por um volume em um agregado no nó foram abertos por meio de um compartilhamento SMB continuamente disponível com a promessa de persistência em caso de falha. No entanto, o relacionamento de HA com o parceiro não está configurado ou não está íntegro.
NoStandbyLifCifsNdo_Alert	Menor	A máquina virtual de storage (SVM) está fornecendo dados ativamente sobre SMB por meio de um nó e há arquivos SMB abertos persistentemente por compartilhamentos disponíveis continuamente. No entanto, seu nó de parceiro não expõe LIFs de dados ativos para o SVM.

Exibir o status de operação sem interrupções usando o monitoramento de integridade do sistema

Você pode usar os `system health` comandos para exibir informações sobre a integridade geral do sistema do cluster e a integridade do subsistema CIFS-NDO, responder a alertas, configurar alertas futuros e exibir informações sobre como o monitoramento de integridade está configurado.

Passos

1. Monitore o status de integridade executando a ação apropriada:

Se você quiser exibir…	Digite o comando…
O estado de saúde do sistema, que reflete o estado geral dos monitores de saúde individuais	**system health status show**
Informações sobre o estado de funcionamento do subsistema CIFS-NDO	**system health subsystem show -subsystem CIFS-NDO -instance**

2. Exiba informações sobre como o monitoramento de alerta CIFS-NDO é configurado executando as ações apropriadas:

Se você quiser exibir informações sobre…	Digite o comando…
A configuração e o status do monitor de integridade do subsistema CIFS-NDO, como nós monitorados, estado de inicialização e status	**system health config show -subsystem CIFS-NDO**

Se você quiser exibir informações sobre…	Digite o comando…
O CIFS-NDO alerta que um monitor de integridade pode gerar	**system health alert definition show -subsystem CIFS-NDO**
Políticas do monitor de integridade CIFS-NDO, que determinam quando os alertas são gerados	**system health policy definition show -monitor node-connect**

Use o `-instance` parâmetro para exibir informações detalhadas.

Exemplos

A saída a seguir mostra informações sobre o status geral de integridade do cluster e do subsistema CIFS-NDO:

```
cluster1::> system health status show
Status
---------------
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

A saída a seguir mostra informações detalhadas sobre a configuração e o status do monitor de integridade do subsistema CIFS-NDO:

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                          Node: node1
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                          Node: node2
                       Monitor: node-connect
                     Subsystem: SAS-connect, HA-health, CIFS-NDO
                        Health: ok
               Monitor Version: 2.0
           Policy File Version: 1.0
                       Context: node_context
                    Aggregator: system-connect
                      Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

Verifique a configuração de compartilhamento SMB continuamente disponível

Para dar suporte a operações ininterruptas, os compartilhamentos SMB do Hyper-V e do SQL Server devem ser configurados como compartilhamentos disponíveis continuamente. Além disso, existem certas outras configurações de compartilhamento que você deve verificar. Você deve verificar se os compartilhamentos estão configurados corretamente para fornecer operações ininterruptas contínuas para os servidores de aplicações, se houver eventos disruptivos planejados ou não planejados.

Sobre esta tarefa

Você deve verificar se os dois parâmetros de compartilhamento a seguir estão definidos corretamente:

- O `-offline-files` parâmetro é definido como `manual` (o padrão) ou `none`.
- Os links simbólicos devem ser desativados.

Para operações ininterruptas adequadas, as seguintes propriedades de compartilhamento devem ser definidas:

- `continuously-available`
- `oplocks`

As seguintes propriedades de compartilhamento não devem ser definidas:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

Passos

1. Verifique se os arquivos off-line estão definidos como `manual` ou `disabled` e se os links simbólicos estão desativados:

   vserver cifs shares show -vserver *vserver_name*

2. Verifique se os compartilhamentos SMB estão configurados para disponibilidade contínua:

   vserver cifs shares properties show -vserver *vserver_name*

Exemplos

O exemplo a seguir exibe a configuração de compartilhamento para um compartilhamento chamado "hare1" na máquina virtual de armazenamento (SVM, anteriormente conhecido como SVM) VS1. Os arquivos offline são definidos como `manual` e os links simbólicos são desativados (designados por um hífen na `Symlink Properties` saída do campo):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: VS1
                         Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

O exemplo a seguir exibe as propriedades de compartilhamento de um compartilhamento chamado "hare1" no SVM VS1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

Verifique o status do LIF

Mesmo que você configure máquinas virtuais de armazenamento (SVMs) com configurações Hyper-V e SQL Server sobre SMB para ter LIFs em cada nó em um cluster, durante operações diárias, alguns LIFs podem se mover para portas em outro nó. Você deve verificar o status do LIF e tomar todas as ações corretivas necessárias.

Sobre esta tarefa

Para oferecer suporte contínuo a operações ininterruptas e sem interrupções, cada nó em um cluster precisa ter pelo menos um LIF para a SVM e todos os LIFs precisam estar associados a uma porta inicial. Se algumas LIFs configuradas não estiverem associadas atualmente à porta inicial, você deverá corrigir quaisquer problemas de porta e reverter os LIFs para a porta inicial.

Passos

1. Exibir informações sobre LIFs configuradas para o SVM:

   `network interface show -vserver` *`vserver_name`*

   Neste exemplo, "'lif1'" não está localizado na porta inicial.

```
network interface show -vserver vs1
```

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node2      e0d
false
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

2. Se alguns dos LIFs não estiverem em suas portas residenciais, execute as seguintes etapas:

   a. Para cada LIF, determine qual é a porta inicial do LIF:

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

      network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

      ```
      vserver lif  home-node  home-port
      ------- ---- ---------- ---------
      vs1     lif1 node1      e0d
      ```

   b. Para cada LIF, determine se a porta inicial do LIF está ativa:

      network port show -node *node_name* -port *port* -fields port,link

      ```
      network port show -node node1 -port e0d -fields port,link
      ```

      ```
      node       port link
      ---------- ---- ----
      node1      e0d  up
      ```

      +
      Neste exemplo, "'lif1" deve ser migrado de volta para sua porta de origem, `node1:e0d`.

3. Se qualquer uma das interfaces de rede de porta inicial às quais os LIFs devem estar associados não estiver no `up` estado, resolva o problema para que essas interfaces estejam ativas.
4. Se necessário, reverta os LIFs para suas portas residenciais:

   network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

5. Verifique se cada nó no cluster tem um LIF ativo para o SVM:

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network          Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

Determine se as sessões SMB estão continuamente disponíveis

Exibir informações de sessão SMB

Você pode exibir informações sobre sessões SMB estabelecidas, incluindo a conexão SMB e Session ID e o endereço IP da estação de trabalho usando a sessão. Você pode exibir informações sobre a versão do protocolo SMB da sessão e o nível de proteção continuamente disponível, o que ajuda a identificar se a sessão é compatível com operações ininterruptas.

Sobre esta tarefa

É possível exibir informações de todas as sessões no SVM no formulário de resumo. No entanto, em muitos casos, a quantidade de saída que é retornada é grande. Você pode personalizar quais informações são exibidas na saída especificando parâmetros opcionais:

- Você pode usar o parâmetro opcional `-fields` para exibir a saída sobre os campos que você escolher.

  Você pode inserir `-fields ?` para determinar quais campos você pode usar.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre sessões SMB estabelecidas.
- Você pode usar o `-fields` parâmetro ou o `-instance` parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
Para todas as sessões no SVM de forma resumida	**vserver cifs session show -vserver *vserver_name***
Em um ID de conexão especificado	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
A partir de um endereço IP de estação de trabalho especificado	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***
Em um endereço IP de LIF especificado	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
Em um nó especificado	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	De um usuário do Windows especificado
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* O formato para `user_name` é `[domain]\user`.	Com um mecanismo de autenticação especificado

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism O valor para `-auth -mechanism` pode ser um dos seguintes: • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	Com uma versão de protocolo especificada

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version O valor para `-protocol-version` pode ser um dos seguintes: • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1`	Com um nível especificado de proteção continuamente disponível

Se você quiser exibir informações de sessão SMB…	Digite o seguinte comando…
`vserver cifs session show -vserver vserver_name -continuously -available continuously_available_protection_level` O valor para `-continuously -available` pode ser um dos seguintes: • `No` • `Yes` • `Partial` Se o status continuamente disponível for `Partial`, isso significa que a sessão contém pelo menos um arquivo aberto continuamente disponível, mas a sessão tem alguns arquivos que não estão abertos com proteção continuamente disponível. Você pode	Com um status de sessão de assinatura SMB especificado

Exemplos

O comando a seguir exibe informações de sessão para as sessões no SVM VS1 estabelecidas a partir de uma estação de trabalho com endereço IP 10,1.1,1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281 1       10.1.1.1         DOMAIN\joe          2          23s
```

O comando a seguir exibe informações detalhadas da sessão para sessões com proteção continuamente disponível no SVM VS1. A conexão foi feita usando a conta de domínio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

O comando a seguir exibe informações de sessão em uma sessão usando SMB 3,0 e SMB Multichannel no SVM VS1. No exemplo, o usuário conetado a esse compartilhamento a partir de um cliente compatível com SMB 3,0 usando o endereço IP LIF; portanto, o mecanismo de autenticação padrão é NTLMv2. A conexão deve ser feita usando a autenticação Kerberos para se conetar com a proteção continuamente disponível.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

Exibir informações sobre arquivos SMB abertos

Você pode exibir informações sobre arquivos SMB abertos, incluindo a conexão SMB e Session ID, o volume de hospedagem, o nome do compartilhamento e o caminho do compartilhamento. Você também pode exibir informações sobre o nível de proteção continuamente disponível de um arquivo, o que é útil para determinar se um arquivo aberto está em um estado compatível com operações ininterruptas.

Sobre esta tarefa

Você pode exibir informações sobre arquivos abertos em uma sessão SMB estabelecida. As informações exibidas são úteis quando você precisa determinar informações de sessão SMB para arquivos específicos em uma sessão SMB.

Por exemplo, se você tiver uma sessão SMB em que alguns dos arquivos abertos estão abertos com proteção continuamente disponível e alguns não estão abertos com proteção continuamente disponível (o valor para o `-continuously-available` campo na `vserver cifs session show` saída de comando é `Partial`), você pode determinar quais arquivos não estão disponíveis continuamente usando este comando.

Você pode exibir informações de todos os arquivos abertos em sessões SMB estabelecidas em máquinas virtuais de armazenamento (SVMs) em forma de resumo usando o `vserver cifs session file show` comando sem quaisquer parâmetros opcionais.

No entanto, em muitos casos, a quantidade de saída retornada é grande. Você pode personalizar quais

informações são exibidas na saída especificando parâmetros opcionais. Isso pode ser útil quando você deseja exibir informações para apenas um pequeno subconjunto de arquivos abertos.

- Você pode usar o parâmetro opcional `-fields` para exibir a saída nos campos que você escolher.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

- Você pode usar o `-instance` parâmetro para exibir informações detalhadas sobre arquivos SMB abertos.

  Você pode usar este parâmetro sozinho ou em combinação com outros parâmetros opcionais.

Passos

1. Execute uma das seguintes ações:

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
No SVM no formulário de resumo	**vserver cifs session file show -vserver *vserver_name***
Em um nó especificado	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	Em um ID de arquivo especificado
vserver cifs session file show -vserver *vserver_name* -file-id integer	Em uma ID de conexão SMB especificada
vserver cifs session file show -vserver *vserver_name* -connection-id integer	Em um SMB Session ID especificado
vserver cifs session file show -vserver *vserver_name* -session-id integer	No agregado de hospedagem especificado
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	No volume especificado
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	No compartilhamento SMB especificado
vserver cifs session file show -vserver *vserver_name* -share *share_name*	No caminho SMB especificado

Se você quiser exibir arquivos SMB abertos…	Digite o seguinte comando…
vserver cifs session file show -vserver *vserver_name* -path *path*	Com o nível especificado de proteção continuamente disponível
vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status* O valor para `-continuously-available` pode ser um dos seguintes: • `No` • `Yes` Se o status continuamente disponível for `No`, isso significa que esses arquivos abertos não serão capazes de se recuperar sem interrupções da aquisição e da giveback. Eles também não podem se recuperar da realocação geral agregada entre parceiros em um relacionamento de alta disponibilidade.	Com o estado de reconexão especificado

Existem parâmetros opcionais adicionais que você pode usar para refinar os resultados de saída. Consulte a página de manual para obter mais informações.

Exemplos

O exemplo a seguir exibe informações sobre arquivos abertos no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting              Continuously
ID      Type      Mode Volume    Share      Available
------- --------- ---- --------- ---------- ------------
41      Regular   r    data      data       Yes
Path: \mytest.rtf
```

O exemplo a seguir exibe informações detalhadas sobre arquivos SMB abertos com ID de arquivo 82 no SVM VS1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

Informações sobre direitos autorais

Informações sobre marcas comerciais