Entenda o acesso a arquivos nas

ONTAP 9

NetApp
January 17, 2025

Índice

Entenda o acesso a arquivos nas

Namespaces e pontos de junção

Visão geral de namespaces e pontos de junção

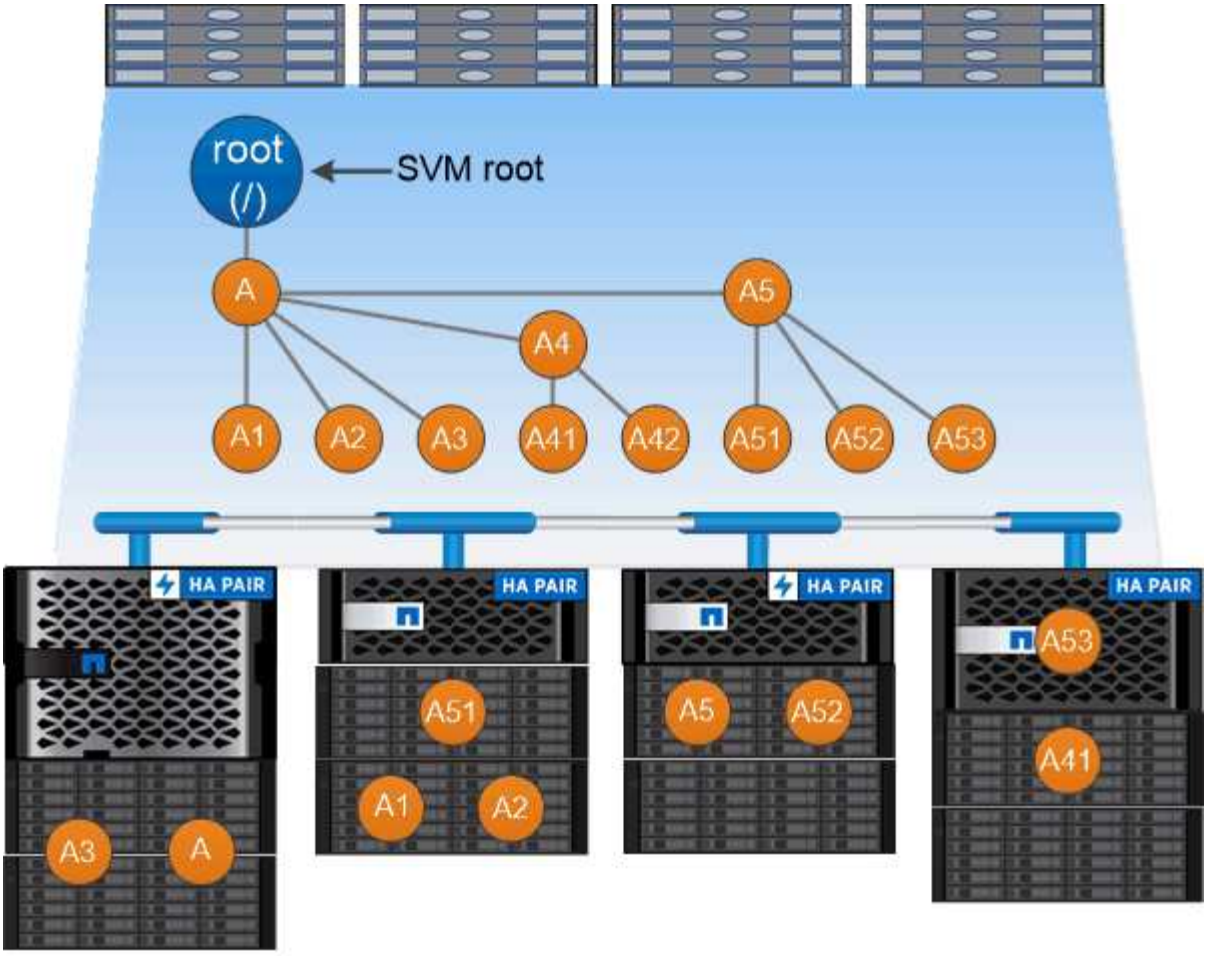
Um nas *namespace* é um agrupamento lógico de volumes Unidos em *pontos de junção* para criar uma única hierarquia de sistema de arquivos. Um cliente com permissões suficientes pode acessar arquivos no namespace sem especificar a localização dos arquivos no armazenamento. Os volumes Junctioned podem 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.

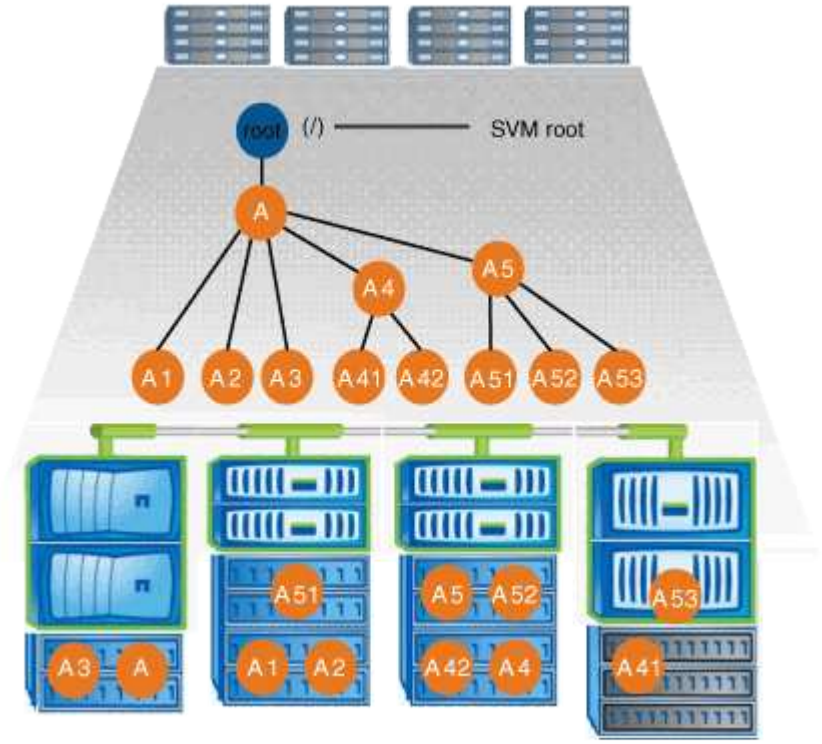
A parte superior do namespace é sempre o volume raiz, que é representado por uma barra (/). A arquitetura de namespace sob a raiz se enquadra em três categorias básicas:

- 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).

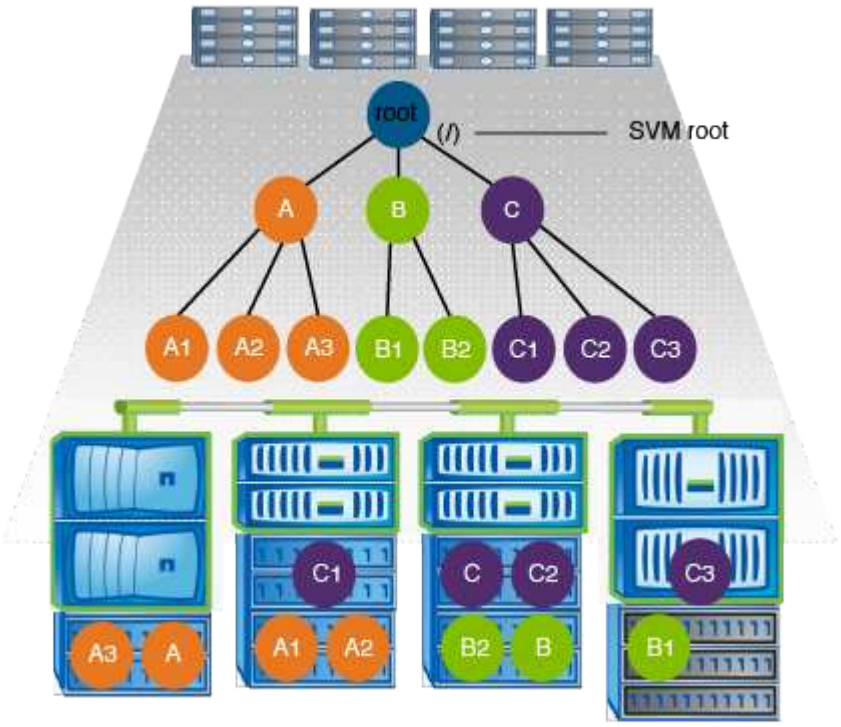


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde todos os volumes são juntados abaixo do ponto de inserção único, que é um diretório chamado "data":

```
                    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).

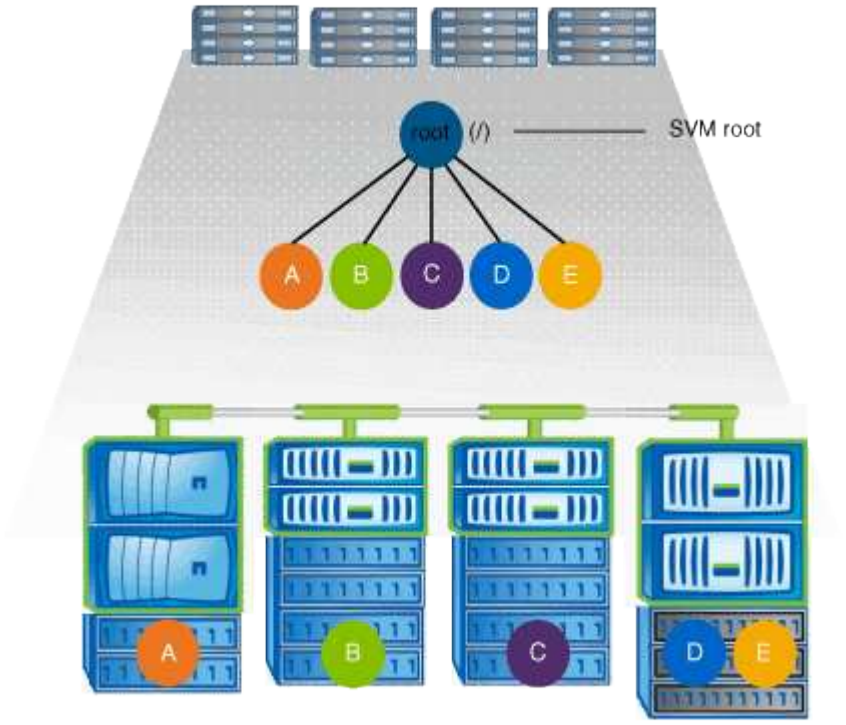


Por exemplo, uma configuração típica de junção de volume com a arquitetura de namespace acima pode parecer com a seguinte configuração, onde há três pontos de inserção para o volume raiz do SVM. Dois pontos de inserção são diretórios denominados "data" e "projetos". Um ponto de inserção é um volume juntado 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.

Informações sobre direitos autorais

Informações sobre marcas comerciais