Autenticação e controle de acesso

ONTAP 9

NetApp
January 17, 2025

Índice

Autenticação e controle de acesso

Visão geral do controle de acesso e autenticação

Você pode gerenciar a autenticação de cluster do ONTAP e o controle de acesso aos serviços da Web do ONTAP.

Com o System Manager ou a CLI, você pode controlar e proteger o acesso do cliente e do administrador ao cluster e ao storage.

Se você estiver usando o Gerenciador de sistema clássico (disponível somente no ONTAP 9.7 e anterior), consulte "System Manager Classic (ONTAP 9 9,7.0 a 0)"

Autenticação e autorização do cliente

O ONTAP autentica uma máquina cliente e um usuário verificando suas identidades com uma fonte confiável. O ONTAP autoriza um usuário a acessar um arquivo ou diretório comparando as credenciais do usuário com as permissões configuradas no arquivo ou diretório.

Autenticação de administrador e RBAC

Os administradores usam contas de login locais ou remotas para se autenticar no cluster e na VM de armazenamento. O controle de acesso baseado em função (RBAC) determina os comandos aos quais um administrador tem acesso.

Gerenciar a autenticação do administrador e o RBAC

Visão geral da autenticação do administrador e do RBAC com a CLI

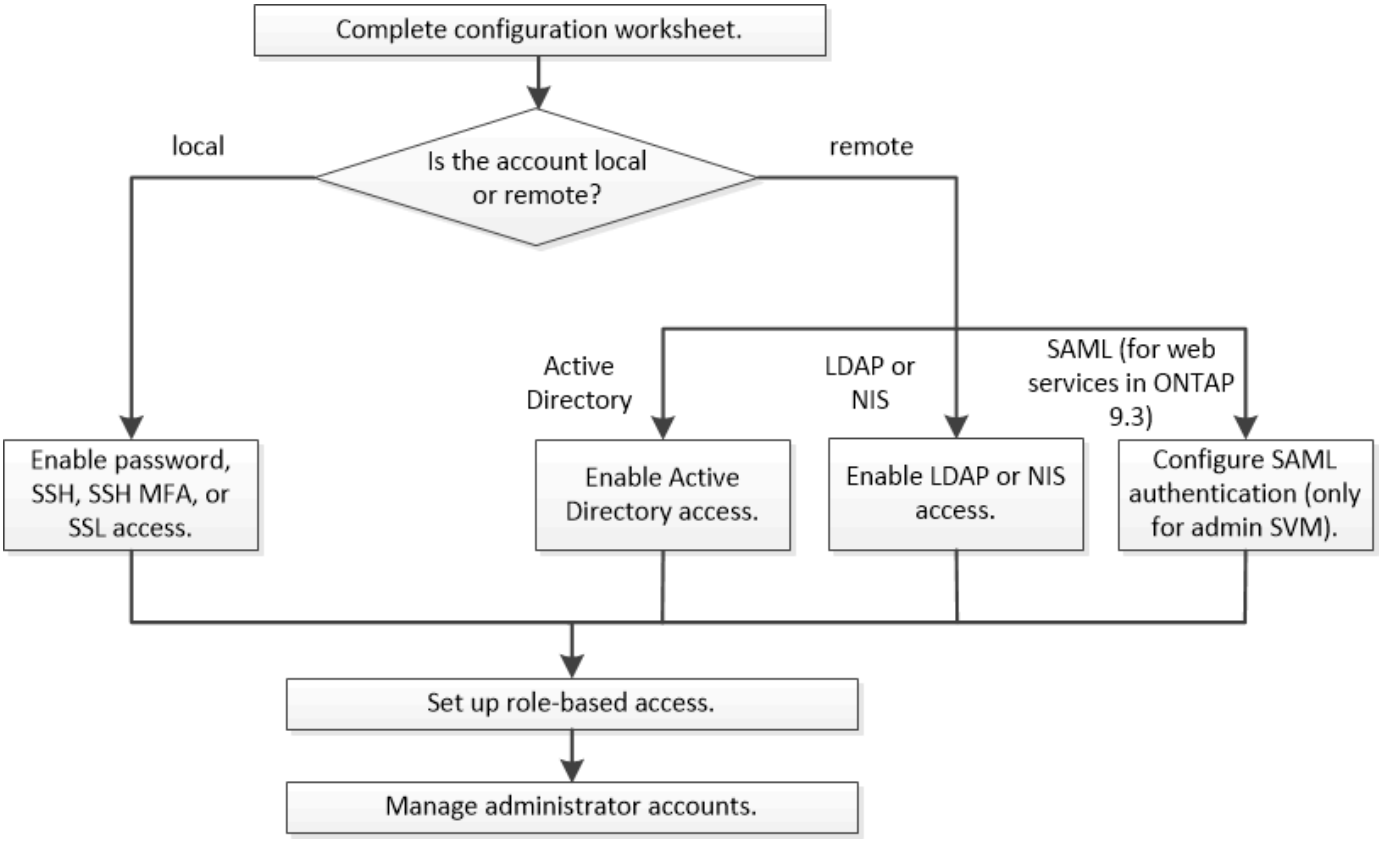
Você pode habilitar contas de login para administradores de cluster do ONTAP e administradores de máquina virtual de storage (SVM). Você também pode usar o controle de acesso baseado em função (RBAC) para definir as funcionalidades dos administradores.

Você ativa as contas de login e o RBAC das seguintes maneiras:

- Você deseja usar a interface de linha de comando (CLI) do ONTAP, não o Gerenciador de sistema ou uma ferramenta de script automatizado.
- Você quer usar as práticas recomendadas, não explorar todas as opções disponíveis.
- Você não está usando SNMP para coletar informações sobre o cluster.

Autenticação de administrador e fluxo de trabalho RBAC

Você pode ativar a autenticação para contas de administrador locais ou contas de administrador remoto. As informações da conta de uma conta local residem no sistema de armazenamento e as informações da conta de uma conta remota residem em outro lugar. Cada conta pode ter uma função predefinida ou uma função personalizada.



Você pode habilitar contas de administrador locais para acessar uma máquina virtual de storage de administrador (SVM) ou um data SVM com os seguintes tipos de autenticação:

- Palavra-passe
- Chave pública SSH
- Certificado SSL
- Autenticação multifator SSH (MFA)

  A partir do ONTAP 9.3, a autenticação com senha e chave pública é suportada.

Você pode habilitar contas de administrador remoto para acessar um SVM admin ou um SVM de dados com os seguintes tipos de autenticação:

- Ative Directory
- Autenticação SAML (somente para SVM de administrador)

  A partir do ONTAP 9.3, a autenticação SAML (Security Assertion Markup Language) pode ser usada para acessar o SVM admin usando qualquer um dos seguintes serviços da Web: Infraestrutura do processador de serviços, APIs ONTAP ou Gerenciador de sistemas.

- A partir do ONTAP 9.4, o SSH MFA pode ser usado para usuários remotos em servidores LDAP ou NIS. A autenticação com nsswitch e chave pública é suportada.

Planilhas para autenticação de administrador e configuração RBAC

Antes de criar contas de login e configurar o controle de acesso baseado em funções (RBAC), você deve coletar informações para cada item nas planilhas de configuração.

Criar ou modificar contas de login

Você fornece esses valores com o `security login create` comando ao habilitar contas de login para acessar uma VM de armazenamento. Você fornece os mesmos valores com o `security login modify` comando quando modifica como uma conta acessa uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento que a conta acessa. O valor padrão é o nome da VM de armazenamento de administrador para o cluster.	
`-user-or-group-name`	O nome de usuário ou nome de grupo da conta. Especificar um nome de grupo permite o acesso a cada usuário no grupo. Você pode associar um nome de usuário ou nome de grupo a vários aplicativos.	
`-application`	O aplicativo usado para acessar a VM de storage: • `http` • `ontapi` • `snmp` • `ssh`	

`-authmethod`	O método utilizado para autenticar a conta: • `cert` Para autenticação de certificado SSL • `domain` Para autenticação do ative Directory • `nsswitch` Para autenticação LDAP ou NIS • `password` para autenticação de senha do usuário • `publickey` para autenticação de chave pública • `community` Para strings de comunidade SNMP • `usm` Para o modelo de segurança do utilizador SNMP • `saml` Para autenticação SAML (Security Assertion Markup Language)	
`-remote-switch-ipaddress`	O endereço IP do interrutor remoto. O switch remoto pode ser um switch de cluster monitorado pelo monitor de integridade do switch de cluster (CSHM) ou um switch Fibre Channel (FC) monitorado pelo monitor de integridade do MetroCluster (MCC-HM). Esta opção é aplicável apenas quando a aplicação é `snmp` e o método de autenticação é `usm`.	
`-role`	A função de controle de acesso atribuída à conta: • Para o cluster (a VM de armazenamento de administrador), o valor padrão é `admin`. • Para uma VM de armazenamento de dados, o valor padrão é `vsadmin`.	
`-comment`	(Opcional) texto descritivo para a conta. Você deve incluir o texto entre aspas duplas (").	

`-is-ns-switch-group`	Se a conta é uma conta de grupo LDAP ou uma conta de grupo NIS (`yes` ou `no`).	
`-second-authentication -method`	Segundo método de autenticação no caso de autenticação multifator: • `none` se não estiver usando autenticação multifator, o valor padrão • `publickey` para autenticação de chave pública quando o `authmethod` é senha ou nsswitch • `password` para autenticação de senha do usuário quando a `authmethod` é chave pública • `nsswitch` para autenticação de senha do usuário quando o authmethod é publikey A ordem de autenticação é sempre a chave pública seguida pela senha.	
`-is-ldap-fastbind`	A partir do ONTAP 9.11,1, quando definido como verdadeiro, ativa a vinculação rápida LDAP para autenticação nsswitch; o padrão é falso. Para utilizar a ligação rápida LDAP, o `-authentication -method` valor tem de ser definido como `nsswitch`. "Saiba mais sobre LDAP fastbind para autenticação nsswitch."	

Configure as informações de segurança do Cisco Duo

Você fornece esses valores com o `security login duo create` comando quando ativa a autenticação de dois fatores do Cisco Duo com logins SSH para uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	A VM de armazenamento (referida como vserver na CLI do ONTAP) à qual as configurações de autenticação Duo se aplicam.	

`-integration-key`	Sua chave de integração, obtida ao Registrar seu aplicativo SSH com Duo.	
`-secret-key`	Sua chave secreta, obtida ao Registrar seu aplicativo SSH com Duo.	
`-api-host`	O nome de host da API, obtido ao Registrar seu aplicativo SSH com Duo. Por exemplo: `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Em erros de serviço ou configuração que impedem a autenticação Duo, `safe` falha (permitir acesso) ou `secure` (negar acesso). O padrão é `safe`, o que significa que a autenticação Duo é ignorada se falhar devido a erros como o servidor de API Duo ficar inacessível.	
`-http-proxy`	Use o proxy HTTP especificado. Se o proxy HTTP exigir autenticação, inclua as credenciais no URL do proxy. Por exemplo: `http-proxy=http://username:password@proxy.example.org:8080`	

-autopush	`true` `false`Ou . A predefinição é `false`. Se `true`o , o Duo enviar automaticamente uma solicitação de login por push para o telefone do usuário, revertendo para uma chamada telefônica se o push não estiver disponível. Observe que isso desabilita efetivamente a autenticação por senha. Se `false`, o usuário for solicitado a escolher um método de autenticação. Quando configurado com `autopush = true`, recomendamos a configuração `max-prompts = 1`.	

`-max-prompts`	Se um usuário não conseguir autenticar com um segundo fator, o Duo solicitará que ele se autentique novamente. Esta opção define o número máximo de prompts que o Duo exibe antes de negar acesso. Deve ser `1`, `2`, `3` ou . O valor padrão é `1`. Por exemplo, quando `max-prompts = 1`o , o usuário precisa se autenticar com êxito no primeiro prompt, enquanto se , se `max-prompts = 2` o usuário inserir informações incorretas no prompt inicial, ele será solicitado a autenticar novamente. Quando configurado com `autopush = true`, recomendamos a configuração `max-prompts = 1`. Para obter a melhor experiência, um usuário com apenas autenticação publickey sempre terá `max-prompts` definido como `1`.	
`-enabled`	Ative a autenticação de dois fatores Duo. Defina como `true` por padrão. Quando ativada, a autenticação de dois fatores Duo é aplicada durante o login SSH de acordo com os parâmetros configurados. Quando Duo está desativado (definido para `false`), a autenticação Duo é ignorada.	
`-pushinfo`	Esta opção fornece informações adicionais na notificação push, como o nome do aplicativo ou serviço que está sendo acessado. Isso ajuda os usuários a verificar se estão fazendo login no serviço correto e fornece uma camada adicional de segurança.	

Definir funções personalizadas

Você fornece esses valores com o `security login role create` comando quando define uma função personalizada.

Campo	Descrição	O seu valor
`-vserver`	(Opcional) o nome da VM de armazenamento (referida como vserver na CLI do ONTAP) que está associado à função.	
`-role`	O nome da função.	
`-cmddirname`	O diretório de comando ou comando ao qual a função dá acesso. Você deve incluir nomes de subdiretório de comando em aspas duplas ("). Por exemplo, `"volume snapshot"`. Você deve digitar `DEFAULT` para especificar todos os diretórios de comando.	
`-access`	(Opcional) o nível de acesso para a função. Para diretórios de comando: • `none` (o valor padrão para funções personalizadas) nega o acesso aos comandos no diretório de comandos • `readonly` concede acesso aos `show` comandos no diretório de comandos e seus subdiretórios • `all` concede acesso a todos os comandos no diretório de comandos e seus subdiretórios Para *comandos não intrínsecos* (comandos que não terminam em `create`, `modify`, , `delete` ou `show`): • `none` (o valor padrão para funções personalizadas) nega o acesso ao comando • `readonly` não é aplicável • `all` concede acesso ao comando Para conceder ou negar acesso a comandos intrínsecos, você deve especificar o diretório de comandos.	

`-query`	(Opcional) o objeto de consulta que é usado para filtrar o nível de acesso, que é especificado na forma de uma opção válida para o comando ou para um comando no diretório de comandos. Você deve incluir o objeto de consulta em aspas duplas ("). Por exemplo, se o diretório de comando for `volume`, o objeto query `"-aggr aggr0"` ativará o acesso somente para `aggr0` o agregado.	

Associar uma chave pública a uma conta de utilizador

Você fornece esses valores com o `security login publickey create` comando ao associar uma chave pública SSH a uma conta de usuário.

Campo	Descrição	O seu valor
`-vserver`	(Opcional) o nome da VM de armazenamento que a conta acessa.	
`-username`	O nome de utilizador da conta. O valor padrão, `admin`, que é o nome padrão do administrador do cluster.	
`-index`	O número de índice da chave pública. O valor padrão é 0 se a chave for a primeira chave criada para a conta; caso contrário, o valor padrão é mais um do que o número de índice mais alto existente para a conta.	
`-publickey`	A chave pública OpenSSH. Você deve incluir a chave entre aspas duplas (").	
`-role`	A função de controle de acesso atribuída à conta.	
`-comment`	(Opcional) texto descritivo para a chave pública. Você deve incluir o texto entre aspas duplas (").	

`-x509-certificate`	(Opcional) começando com ONTAP 9.13,1, permite gerenciar a associação de certificados X,509 com a chave pública SSH. Quando você associa um certificado X,509 à chave pública SSH, o ONTAP verifica o login SSH para ver se esse certificado é válido. Se tiver expirado ou tiver sido revogado, o início de sessão é proibido e a chave pública SSH associada está desativada. Valores possíveis: • `install`: Instale o certificado X,509 codificado PEM especificado e associe-o à chave pública SSH. Inclua o texto completo do certificado que deseja instalar. • `modify`: Atualize o certificado X,509 codificado PEM existente com o certificado especificado e associe-o à chave pública SSH. Inclua o texto completo do novo certificado. • `delete`: Remova a associação de certificado X,509 existente com a chave pública SSH.	

Configure as definições globais de autorização dinâmica

Começando com ONTAP 9.15,1, você fornece esses valores com o `security dynamic-authorization modify` comando. Para obter mais informações sobre a configuração de autorização dinâmica, "descrição geral da autorização dinâmica"consulte .

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual a configuração de pontuação de confiança deve ser modificada. Se você omitir esse parâmetro, a configuração de nível do cluster será usada.	

`-state`	O modo de autorização dinâmica. Valores possíveis: • `disabled`: (Predefinição) a autorização dinâmica está desativada. • `visibility`: Este modo é útil para testar a autorização dinâmica. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas, mas não aplicada. No entanto, qualquer atividade que tenha sido negada ou sujeita a desafios de autenticação adicionais é registrada. • `enforced`: Destinado a ser utilizado depois de ter concluído o teste com `visibility` o modo. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas e as restrições de atividade são aplicadas se as condições de restrição forem cumpridas. O intervalo de supressão também é aplicado, impedindo desafios de autenticação adicionais dentro do intervalo especificado.	
`-suppression-interval`	Impede desafios de autenticação adicionais dentro do intervalo especificado. O intervalo está no formato ISO-8601 e aceita valores de 1 minuto a 1 hora inclusive. Se definido como 0, o intervalo de supressão será desativado e o usuário sempre será solicitado a um desafio de autenticação, se for necessário.	
`-lower-challenge-boundary`	O limite inferior da porcentagem de desafio de autenticação multifator (MFA). O intervalo válido é de 0 a 99. O valor 100 é inválido, pois isso faz com que todas as solicitações sejam negadas. O valor padrão é 0.	

`-upper-challenge-boundary`	O limite superior da porcentagem de desafio do MFA. O intervalo válido é de 0 a 100. Isto deve ser igual ou superior ao valor do limite inferior. Um valor de 100 significa que cada solicitação será negada ou sujeita a um desafio de autenticação adicional; não há solicitações que sejam permitidas sem um desafio. O valor padrão é 90.	

Instale um certificado digital de servidor assinado pela CA

Você fornece esses valores com o `security certificate generate-csr` comando ao gerar uma solicitação de assinatura de certificado digital (CSR) para uso na autenticação de uma VM de armazenamento como um servidor SSL.

Campo	Descrição	O seu valor
`-common-name`	O nome do certificado, que é um nome de domínio totalmente qualificado (FQDN) ou um nome comum personalizado.	
`-size`	O número de bits na chave privada. Quanto maior o valor, mais segura a chave. O valor padrão é `2048`. Os valores possíveis são `512`, `1024`, `1536` `2048` e .	
`-country`	O país da VM de armazenamento, em um código de duas letras. O valor padrão é `US`. Consulte as páginas de manual para obter uma lista de códigos.	
`-state`	O estado ou a província da VM de armazenamento.	
`-locality`	A localidade da VM de armazenamento.	
`-organization`	A organização da VM de storage.	
`-unit`	A unidade na organização da VM de armazenamento.	

`-email-addr`	O endereço de e-mail do administrador do Contato para a VM de armazenamento.	
`-hash-function`	A função de hash criptográfico para assinar o certificado. O valor padrão é `SHA256`. Os valores possíveis são `SHA1`, `SHA256`, e `MD5`.	

Você fornece esses valores com o `security certificate install` comando ao instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou da VM de armazenamento como um servidor SSL. Apenas as opções relevantes para a configuração da conta são mostradas na tabela a seguir.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual o certificado deve ser instalado.	
`-type`	O tipo de certificado: • `server` para certificados de servidor e certificados intermediários • `client-ca` Para o certificado de chave pública da CA raiz do cliente SSL • `server-ca` Para o certificado de chave pública da CA raiz do servidor SSL do qual o ONTAP é um cliente • `client` Para um certificado digital autoassinado ou CA-assinado e chave privada para o ONTAP como cliente SSL	

Configurar o acesso do controlador de domínio do ative Directory

Você fornece esses valores com o `security login domain-tunnel create` comando quando já configurou um servidor SMB para uma VM de armazenamento de dados e deseja configurar a VM de armazenamento como gateway ou *tunnel* para acesso ao controlador de domínio do ative Directory ao cluster.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual o servidor SMB foi configurado.	

Você fornece esses valores com o `vserver active-directory create` comando quando não configurou um servidor SMB e deseja criar uma conta de computador VM de armazenamento no domínio do ative Directory.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a qual você deseja criar uma conta de computador do ative Directory.	
`-account-name`	O nome NetBIOS da conta do computador.	
`-domain`	O nome de domínio totalmente qualificado (FQDN).	
`-ou`	A unidade organizacional no domínio. O valor padrão é `CN=Computers`. O ONTAP anexa esse valor ao nome de domínio para produzir o nome distinto do ative Directory.	

Configurar o acesso ao servidor LDAP ou NIS

Você fornece esses valores com o `vserver services name-service ldap client create` comando ao criar uma configuração de cliente LDAP para a VM de armazenamento.

Apenas as opções relevantes para a configuração da conta são mostradas na tabela a seguir:

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento para a configuração do cliente.	
`-client-config`	O nome da configuração do cliente.	
`-ldap-servers`	Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores LDAP aos quais o cliente se coneta.	
`-schema`	O esquema que o cliente usa para fazer consultas LDAP.	

`-use-start-tls`	Se o cliente usa Iniciar TLS para criptografar a comunicação com o servidor LDAP (`true`ou `false`). Iniciar TLS é compatível apenas para acesso a VMs de armazenamento de dados. Ele não é compatível com acesso a VMs de storage admin.	

Você fornece esses valores com o `vserver services name-service ldap create` comando ao associar uma configuração de cliente LDAP à VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento com a qual a configuração do cliente deve ser associada.	
`-client-config`	O nome da configuração do cliente.	
`-client-enabled`	Se a VM de armazenamento pode usar a configuração do cliente LDAP (`true`ou `false`).	

Você fornece esses valores com o `vserver services name-service nis-domain create` comando ao criar uma configuração de domínio NIS em uma VM de armazenamento.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual a configuração do domínio deve ser criada.	
`-domain`	O nome do domínio.	
`-servers`	**ONTAP 9.0, 9,1**: Uma lista separada por vírgulas de endereços IP para os servidores NIS usados pela configuração do domínio.	

`-nis-servers`	Uma lista separada por vírgulas de endereços IP e nomes de host para os servidores NIS que são usados pela configuração de domínio.	

Você fornece esses valores com o `vserver services name-service ns-switch create` comando quando especifica a ordem de pesquisa para fontes de serviço de nome.

Campo	Descrição	O seu valor
`-vserver`	O nome da VM de armazenamento na qual a ordem de consulta do serviço de nomes deve ser configurada.	
`-database`	O banco de dados do serviço de nomes: • `hosts` Para ficheiros e serviços de nomes DNS • `group` Para arquivos, LDAP e serviços de nomes NIS • `passwd` Para arquivos, LDAP e serviços de nomes NIS • `netgroup` Para arquivos, LDAP e serviços de nomes NIS • `namemap` Para ficheiros e serviços de nomes LDAP	
`-sources`	A ordem pela qual procurar fontes do serviço de nomes (em uma lista separada por vírgulas): • `files` • `dns` • `ldap` • `nis`	

Configurar o acesso SAML

A partir do ONTAP 9.3, você fornece esses valores com o `security saml-sp create` comando para configurar a autenticação SAML.

Campo	Descrição	O seu valor

`-idp-uri`	O endereço FTP ou o endereço HTTP do host do provedor de identidade (IDP) de onde os metadados de IDP podem ser baixados.	
`-sp-host`	O nome do host ou o endereço IP do host do provedor de serviços SAML (sistema ONTAP). Por padrão, o endereço IP do LIF de gerenciamento de cluster é usado.	
`-cert-ca` e `-cert-serial`, ou `-cert-common-name`	Os detalhes do certificado do servidor do host do provedor de serviços (sistema ONTAP). Você pode inserir a autoridade de certificação de emissão de certificado do provedor de serviços (CA) e o número de série do certificado ou o Nome Comum do certificado do servidor.	
`-verify-metadata-server`	Se a identidade do servidor de metadados IDP deve ser validada `true` ou `false`). A melhor prática é sempre definir este valor para `true`.	

Criar contas de login

Criar uma visão geral das contas de login

Você pode habilitar contas de administrador de cluster local ou remoto e SVM. Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento. As informações da conta de ANÚNCIO são armazenadas em um controlador de domínio. As contas LDAP e NIS residem em servidores LDAP e NIS.

Administradores de clusters e SVM

Um *administrador de cluster* acessa o administrador SVM para o cluster. O administrador SVM e um administrador de cluster com o nome reservado `admin` são criados automaticamente quando o cluster é configurado.

Um administrador de cluster com a função padrão `admin` pode administrar todo o cluster e seus recursos. O administrador do cluster pode criar administradores de cluster adicionais com funções diferentes, conforme necessário.

Um *administrador do SVM* acessa um data SVM. O administrador do cluster cria SVMs de dados e administradores de SVM conforme necessário.

Por padrão, os administradores do SVM recebem `vsadmin` a função. O administrador do cluster pode atribuir funções diferentes aos administradores do SVM, conforme necessário.

Convenções de nomenclatura

Os seguintes nomes genéricos não podem ser usados para contas de administrador de cluster remoto e SVM:

- "adm"
- "bin" (caixa)
- "cli"
- "daemon"
- "ftp"
- "jogos"
- "parar"
- "lp"
- "correio"
- "homem"
- "naroot"
- "NetApp"
- "notícias"
- "ninguém"
- "operador"
- "raiz"
- "shutdown" (encerramento)
- "sshd"
- "sincronizar"
- "sys" (sistema)
- "uucp"
- "www"

Funções mescladas

Se você habilitar várias contas remotas para o mesmo usuário, será atribuída ao usuário a união de todas as funções especificadas para as contas. Ou seja, se uma conta LDAP ou NIS for atribuída à `vsadmin` função e a conta do grupo AD para o mesmo usuário for atribuída `vsadmin-volume` à função, o usuário do AD fará logon com os recursos mais inclusivos `vsadmin`. Diz-se que os papéis são *fundidos*.

Ative o acesso à conta local

Ative a visão geral do acesso à conta local

Uma conta local é aquela em que as informações da conta, a chave pública ou o certificado de segurança residem no sistema de armazenamento. Você pode usar o `security login create` comando para habilitar contas locais para acessar um

administrador ou um SVM de dados.

Ativar acesso à conta de palavra-passe

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

Sobre esta tarefa

Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Ative as contas de administrador locais para acessar um SVM usando uma senha:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir habilita a conta de administrador de cluster `admin1` com a função predefinida `backup` para acessar o SVM de administrador`engCluster` usando uma senha. Você será solicitado a digitar a senha depois de digitar o comando.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

Ativar contas de chave pública SSH

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou SVM de dados com uma chave pública SSH.

Sobre esta tarefa

- Você deve associar a chave pública à conta antes que a conta possa acessar o SVM.

  Associar uma chave pública a uma conta de utilizador

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Se quiser ativar o modo FIPS no cluster, as contas de chave pública SSH existentes sem os algoritmos de chave suportados devem ser reconfiguradas com um tipo de chave suportado. As contas devem ser reconfiguradas antes de ativar o FIPS ou a autenticação do administrador falhar.

A tabela a seguir indica algoritmos de tipo de chave de host compatíveis com conexões SSH ONTAP. Esses tipos de chave não se aplicam à configuração da autenticação pública SSH.

Lançamento do ONTAP	Tipos de chave compatíveis no modo FIPS	Tipos de chave compatíveis no modo não FIPS
9.11.1 e mais tarde	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 e rsa-sha2-512 e rsa-sha2-256 e ssh-ed25519 e ssh-dss e ssh-rsa
9.10.1 e anteriores	ecdsa-sha2-nistp256 e ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss e ssh-rsa

O suporte para o algoritmo de chave de host ssh-ed25519 é removido a partir de ONTAP 9.11,1.

Para obter mais informações, "Configurar a segurança da rede usando o FIPS"consulte .

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Habilite as contas de administrador local para acessar um SVM usando uma chave pública SSH:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name user_or_group_name -application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir permite que a conta de administrador SVM `svmadmin1` com a função predefinida `vsadmin-volume` acesse o SVM`engData1` usando uma chave pública SSH:

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

Depois de terminar

Se você não tiver associado uma chave pública à conta de administrador, deverá fazê-lo antes que a conta possa acessar o SVM.

Associar uma chave pública a uma conta de utilizador

Habilitar contas de autenticação multifator (MFA)

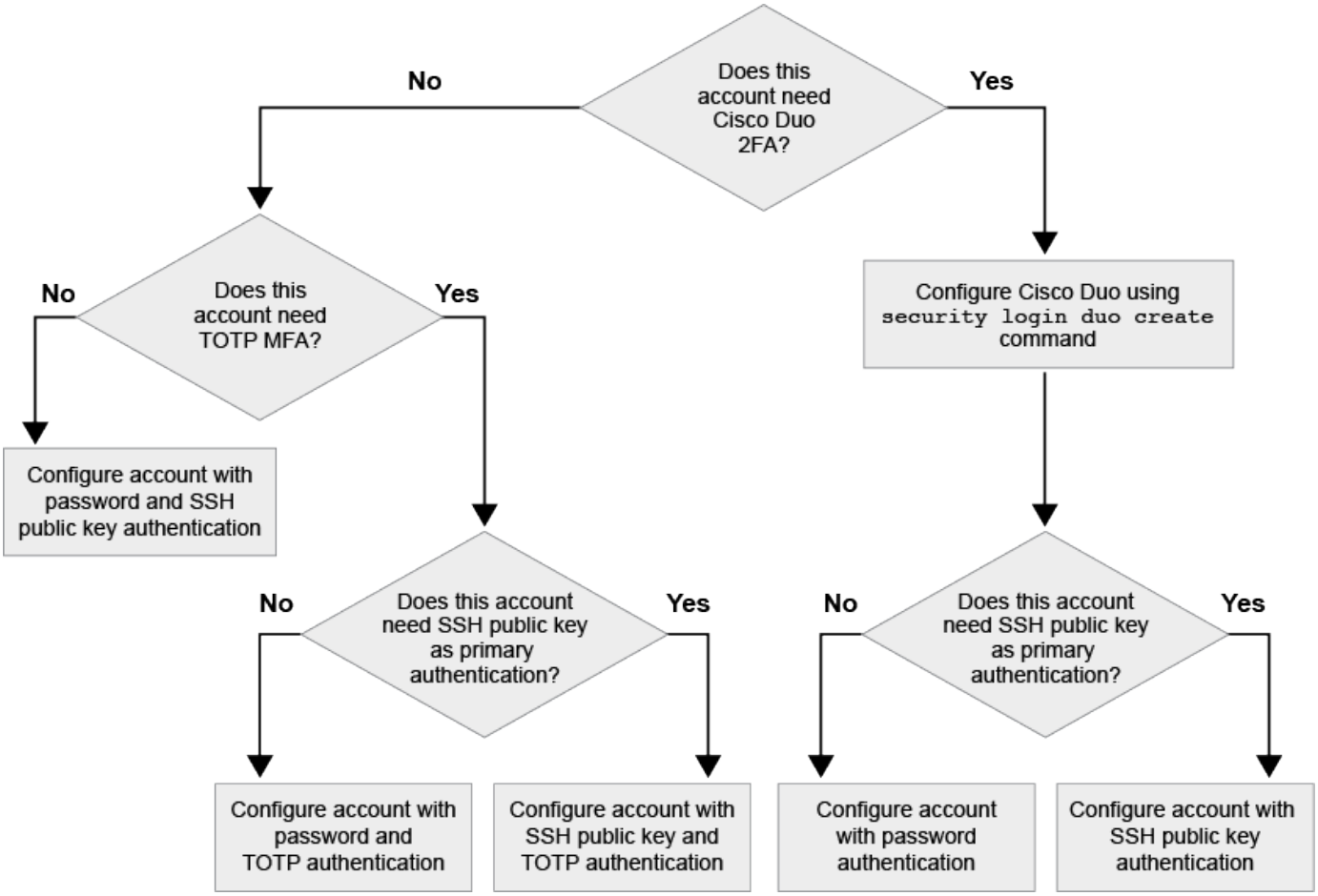
Visão geral da autenticação multifator

A autenticação multifator (MFA) permite aprimorar a segurança, exigindo que os usuários forneçam dois métodos de autenticação para fazer login em um administrador ou uma VM de storage de dados.

Dependendo da sua versão do ONTAP, você pode usar uma combinação de uma chave pública SSH, uma senha de usuário e uma senha única baseada em tempo (TOTP) para autenticação multifator. Quando você ativa e configura o Cisco Duo (ONTAP 9.14,1 e posterior), ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Disponível a partir de…	Primeiro método de autenticação	Segundo método de autenticação
ONTAP 9.14,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
	Chave pública SSH	Cisco Duo
	Palavra-passe do utilizador	Cisco Duo
ONTAP 9.13,1	Chave pública SSH	TOTP
	Palavra-passe do utilizador	TOTP
ONTAP 9,3	Chave pública SSH	Palavra-passe do utilizador

Se o MFA estiver configurado, o administrador do cluster deve primeiro habilitar a conta de usuário local e, em seguida, a conta deve ser configurada pelo usuário local.



Ativar a autenticação multifator

Com a autenticação multifator (MFA), você aumenta a segurança, exigindo que os

usuários forneçam dois métodos de autenticação para fazer login em um administrador ou SVM de dados.

Sobre esta tarefa

- Você deve ser um administrador de cluster para executar esta tarefa.
- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

  "Modificação da função atribuída a um administrador"

- Se você estiver usando uma chave pública para autenticação, associe a chave pública à conta antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- A partir do ONTAP 9.12,1, você pode usar dispositivos de autenticação de hardware Yubikey para o MFA do cliente SSH usando os padrões de autenticação FIDO2 (identidade rápida on-line) ou Verificação de identidade pessoal (PIV).

Habilite o MFA com chave pública SSH e senha do usuário

A partir do ONTAP 9.3, um administrador de cluster pode configurar contas de usuário locais para fazer login com MFA usando uma chave pública SSH e uma senha de usuário.

1. Habilite o MFA em conta de usuário local com chave pública SSH e senha de usuário:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   O comando a seguir exige que a conta de administrador SVM `admin2` com a função predefinida `admin` efetue login no SVM`engData1` com uma chave pública SSH e uma senha de usuário:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

Habilite MFA com TOTP

A partir do ONTAP 9.13,1, você pode melhorar a segurança, exigindo que os usuários locais façam login em um administrador ou SVM de dados com uma chave pública SSH ou senha de usuário e uma senha única

baseada em tempo (TOTP). Depois que a conta estiver habilitada para MFA com TOTP, o usuário local deverá fazer login "conclua a configuração"no .

TOTP é um algoritmo de computador que usa a hora atual para gerar uma senha única. Se o TOTP for usado, é sempre a segunda forma de autenticação após a chave pública SSH ou a senha do usuário.

Antes de começar

Você deve ser um administrador de armazenamento para executar essas tarefas.

Passos

Você pode configurar o MFA para com uma senha de usuário ou uma chave pública SSH como o primeiro método de autenticação e o TOTP como o segundo método de autenticação.

Habilite MFA com senha de usuário e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma senha de usuário e TOTP.

   Para novas contas de usuário

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Para contas de usuário existentes

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verifique se o MFA com TOTP está ativado:

   ```
   security login show
   ```

Habilite MFA com chave pública SSH e TOTP

1. Ative uma conta de usuário para autenticação multifator com uma chave pública SSH e TOTP.

   Para novas contas de usuário

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Para contas de usuário existentes

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Verifique se o MFA com TOTP está ativado:

```
security login show
```

Depois de terminar

- Se você não tiver associado uma chave pública à conta de administrador, deverá fazê-lo antes que a conta possa acessar o SVM.

  "Associar uma chave pública a uma conta de utilizador"

- O usuário local deve fazer login para concluir a configuração de MFA com TOTP.

  "Configurar conta de usuário local para MFA com TOTP"

Informações relacionadas

Saiba mais "Autenticação multifator no ONTAP 9 (TR-4647)"sobre o .

Configurar conta de usuário local para MFA com TOTP

A partir do ONTAP 9.13,1, as contas de usuário podem ser configuradas com autenticação multifator (MFA) usando uma senha única baseada em tempo (TOTP).

Antes de começar

- O administrador de armazenamento tem de "Habilite MFA com TOTP" ser um segundo método de autenticação para a sua conta de utilizador.
- Seu método de autenticação de conta de usuário principal deve ser uma senha de usuário ou uma chave SSH pública.
- Você deve configurar seu aplicativo TOTP para trabalhar com seu smartphone e criar sua chave secreta TOTP.

  Microsoft Authenticator, Google Authenticator, Authy e qualquer outro autenticador compatível com TOTP são suportados.

Passos

1. Inicie sessão na sua conta de utilizador com o método de autenticação atual.

   Seu método de autenticação atual deve ser uma senha de usuário ou uma chave pública SSH.

2. Crie a configuração TOTP na sua conta:

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Repor chave secreta TOTP

Para proteger a segurança da sua conta, se a sua chave secreta TOTP estiver comprometida ou perdida, você deve desativá-la e criar uma nova.

Reponha o TOTP se a sua chave estiver comprometida

Se sua chave secreta TOTP estiver comprometida, mas você ainda tiver acesso a ela, poderá remover a chave comprometida e criar uma nova.

1. Faça login na sua conta de usuário com sua senha de usuário ou chave pública SSH e sua chave secreta TOTP comprometida.
2. Remova a chave secreta TOTP comprometida:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. Crie uma nova chave secreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Reinicie o TOTP se a sua chave for perdida

Se a chave secreta TOTP for perdida, entre em Contato com o administrador de armazenamento para "tenha a chave desativada". Depois que sua chave for desativada, você poderá usar seu primeiro método de autenticação para fazer login e configurar um novo TOTP.

Antes de começar

A chave secreta TOTP deve ser desativada por um administrador de armazenamento. Se não tiver uma conta de administrador de armazenamento, contacte o administrador de armazenamento para desativar a chave.

Passos

1. Depois que o segredo TOTP for desativado por um administrador de armazenamento, use seu método de autenticação principal para fazer login na sua conta local.

2. Crie uma nova chave secreta TOTP:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Verifique se a configuração TOTP está ativada na sua conta:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Desative a chave secreta TOTP para a conta local

Se a chave secreta de uma senha de tempo único (TOTP) de um usuário local for perdida, a chave perdida deve ser desativada por um administrador de armazenamento antes que o usuário possa criar uma nova chave secreta TOTP.

Sobre esta tarefa

Esta tarefa só pode ser executada a partir de uma conta de administrador de cluster.

Passo

1. Desative a chave secreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

Ativar contas de certificado SSL

Você pode usar o `security login create` comando para habilitar contas de administrador para acessar um administrador ou data SVM com um certificado SSL.

Sobre esta tarefa

- Você deve instalar um certificado digital de servidor assinado pela CA antes que a conta possa acessar o SVM.

  Gerando e instalando um certificado de servidor assinado pela CA

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, poderá adicionar a função mais tarde com o `security login modify` comando.

  Modificação da função atribuída a um administrador

Para contas de administrador de cluster, a autenticação de certificado é suportada com os `http` aplicativos , `ontapi` e `rest` . Para contas de administrador da SVM, a autenticação de certificado é compatível apenas com `ontapi` os aplicativos e `rest` .

Passo

1. Ative as contas de administrador local para acessar um SVM usando um certificado SSL:

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Para obter a sintaxe de comando completa, consulte "ONTAP man pages por release".

   O comando a seguir permite que a conta de administrador SVM `svmadmin2` com a função padrão `vsadmin` acesse o SVM`engData2` usando um certificado digital SSL.

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

Depois de terminar

Se você não tiver instalado um certificado digital de servidor assinado pela CA, deverá fazê-lo antes que a conta possa acessar o SVM.

Gerando e instalando um certificado de servidor assinado pela CA

Ative o acesso à conta do ative Directory

Você pode usar o `security login create` comando para habilitar contas de usuário ou grupo do ative Directory (AD) para acessar um administrador ou SVM de dados. Qualquer usuário do grupo AD pode acessar o SVM com a função atribuída ao grupo.

Sobre esta tarefa

- Você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM antes que a conta possa acessar o SVM.

  Configurando o acesso do controlador de domínio do ative Directory

  Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- A partir do ONTAP 9.13,1, você pode usar uma chave pública SSH como seu método de autenticação principal ou secundário com uma senha de usuário do AD.

  Se você optar por usar uma chave pública SSH como sua autenticação principal, nenhuma autenticação AD ocorrerá.

- A partir do ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch" se for suportado pelo servidor LDAP do AD.
- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

Modificação da função atribuída a um administrador

O acesso à conta do GRUPO DE ANÚNCIOS é suportado apenas com os `SSH` aplicativos , `ontapi` e `rest` . Grupos DE ANÚNCIOS não são suportados com autenticação de chave pública SSH, que é comumente usada para autenticação multifator.

Antes de começar

- O tempo do cluster deve ser sincronizado dentro de cinco minutos do tempo no controlador de domínio do AD.
- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Habilite contas de administrador de grupo ou usuário do AD para acessar um SVM:

   Para usuários do AD:

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9.13.1 e mais tarde	Chave pública	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1 e mais tarde	Domínio	Chave pública	**Para um novo usuário**
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			Para um usuário existente
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9,0 e mais tarde	Domínio	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Para grupos AD:

Versão de ONTAP	Autenticação primária	Autenticação secundária	Comando
9,0 e mais tarde	Domínio	Nenhum	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

Para obter a sintaxe de comando completa, consulte "Planilhas para autenticação de administrador e configuração RBAC"

Depois de terminar

Se você não tiver configurado o acesso do controlador de domínio do AD ao cluster ou SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Configurando o acesso do controlador de domínio do ative Directory

Ative o acesso a contas LDAP ou NIS

Você pode usar o `security login create` comando para habilitar contas de usuário LDAP ou NIS para acessar um administrador ou SVM de dados. Se você não tiver configurado o acesso de servidor LDAP ou NIS ao SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Sobre esta tarefa

- As contas de grupo não são suportadas.
- Você deve configurar o acesso de servidor LDAP ou NIS ao SVM antes que a conta possa acessar o SVM.

Configurando o acesso ao servidor LDAP ou NIS

Pode executar esta tarefa antes ou depois de ativar o acesso à conta.

- Se você não tiver certeza da função de controle de acesso que deseja atribuir à conta de login, use o `security login modify` comando para adicionar a função mais tarde.

  Modificação da função atribuída a um administrador

- A partir do ONTAP 9.4, a autenticação multifator (MFA) é compatível com usuários remotos em servidores LDAP ou NIS.
- A partir do ONTAP 9.11,1, você pode usar "Ligação rápida LDAP para autenticação nsswitch" se for suportado pelo servidor LDAP.
- Devido a um problema LDAP conhecido, você não deve usar o `':'` caractere (dois pontos) em nenhum campo de informações de conta de usuário LDAP (por exemplo, `gecos` `userPassword` , e assim por diante). Caso contrário, a operação de pesquisa falhará para esse usuário.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Habilite contas de usuário ou grupo LDAP ou NIS para acessar um SVM:

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   "Criando ou modificando contas de login"

   O comando a seguir habilita a conta de administrador de cluster LDAP ou NIS `guest2` com a função predefinida `backup` para acessar o SVM admin`engCluster` .

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. Ativar login MFA para usuários LDAP ou NIS:

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

   O método de autenticação pode ser especificado como `publickey` e segundo método de autenticação `nsswitch` como .

   O exemplo a seguir mostra a autenticação MFA sendo ativada:

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

Depois de terminar

Se você não tiver configurado o acesso de servidor LDAP ou NIS ao SVM, deverá fazê-lo antes que a conta possa acessar o SVM.

Configurando o acesso ao servidor LDAP ou NIS

Gerenciar funções de controle de acesso

Gerencie a visão geral das funções de controle de acesso

A função atribuída a um administrador determina os comandos aos quais o administrador tem acesso. Você atribui a função ao criar a conta para o administrador. Você pode atribuir uma função diferente ou definir funções personalizadas conforme necessário.

Modifique a função atribuída a um administrador

Você pode usar o `security login modify` comando para alterar a função de uma conta de administrador de cluster ou SVM. Pode atribuir uma função predefinida ou personalizada.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Alterar a função de um administrador de cluster ou SVM:

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   "Criando ou modificando contas de login"

   O comando a seguir altera a função da conta de administrador do cluster do AD `DOMAIN1\guest1` para a função predefinida `readonly`.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   O comando a seguir altera a função das contas de administrador do SVM na conta do grupo AD `DOMAIN1\adgroup` para a função personalizada `vol_role`.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

Definir funções personalizadas

Você pode usar o `security login role create` comando para definir uma função personalizada. Você pode executar o comando quantas vezes for necessário para obter a combinação exata de recursos que deseja associar à função.

Sobre esta tarefa

- Uma função, predefinida ou personalizada, concede ou nega acesso a comandos ou diretórios de comandos do ONTAP.

  Um diretório de comandos (`volume`, por exemplo) é um grupo de comandos e subdiretórios de comandos relacionados. Exceto conforme descrito neste procedimento, conceder ou negar acesso a um diretório de comando concede ou nega acesso a cada comando no diretório e seus subdiretórios.

- O acesso a comandos específicos ou o acesso a subdiretórios substitui o acesso ao diretório pai.

  Se uma função for definida com um diretório de comando e, em seguida, for definida novamente com um nível de acesso diferente para um comando específico ou para um subdiretório do diretório pai, o nível de acesso especificado para o comando ou subdiretório substitui o do pai.

> Não é possível atribuir a um administrador SVM uma função que dê acesso a um diretório de comando ou comando que esteja disponível apenas para o `admin` administrador de cluster - por exemplo, o `security` diretório de comando.

Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Definir uma função personalizada:

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   Os comandos a seguir concedem à `vol_role` função acesso total aos comandos no `volume` diretório de comandos e acesso somente leitura aos comandos `volume snapshot` no subdiretório.

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   Os comandos a seguir concedem à `SVM_storage` função acesso somente leitura aos comandos no `storage` diretório de comandos, sem acesso aos comandos `storage encryption` no subdiretório e acesso total ao `storage aggregate plex offline` comando não intrínseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

Funções predefinidas para administradores de cluster

As funções predefinidas para administradores de cluster devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, um administrador de cluster recebe a função predefinida `admin`.

A tabela a seguir lista as funções predefinidas para administradores de cluster:

Esta função…	Tem este nível de acesso…	Para os seguintes comandos ou diretórios de comandos
administrador	tudo	Todos os diretórios de comando (`DEFAULT`)
admin-no-fsa (disponível a partir de ONTAP 9.12,1)	Leitura/escrita	• Todos os diretórios de comando (`DEFAULT`) • `security login rest-role` • `security login role`

Somente leitura	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	Nenhum
`volume file show-disk-usage`	AutoSupport	tudo
• `set` • `system node autosupport`	nenhum	Todos os outros diretórios de comando (`DEFAULT`)
backup	tudo	`vserver services ndmp`
readonly	`volume`	nenhum
Todos os outros diretórios de comando (`DEFAULT`)	readonly	tudo

• `security login password` Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves • `set`	nenhum	`security`
readonly	Todos os outros diretórios de comando (`DEFAULT`)	SnapLock
tudo	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	nenhum
• `volume move governor` • `volume move recommend`	nenhum	Todos os outros diretórios de comando (`DEFAULT`)
nenhum	nenhum	Todos os diretórios de comando (`DEFAULT`)

A `autosupport` função é atribuída à conta predefinida `autosupport`, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a `autosupport` conta. O ONTAP também impede que você atribua `autosupport` a função a outras contas de usuário.

Funções predefinidas para administradores de SVM

As funções predefinidas para administradores de SVM devem atender à maioria das suas necessidades. Você pode criar funções personalizadas conforme necessário. Por padrão, a função predefinida é atribuída a um administrador SVM `vsadmin`.

A tabela a seguir lista as funções predefinidas para administradores de SVM:

Nome da função	Recursos

vsadmin	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Executando operações SnapLock, exceto exclusão privilegiada • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede • Monitoramento da integridade do SVM
vsadmin-volume	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, incluindo movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Gerenciamento de LUNs • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Monitorização da interface de rede • Monitoramento da integridade do SVM
protocolo vsadmin	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Configuração de protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurando serviços: DNS, LDAP e NIS • Gerenciamento de LUNs • Monitorização da interface de rede • Monitoramento da integridade do SVM

vsadmin-backup	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de operações NDMP • Fazendo uma leitura/gravação de volume restaurada • Gerenciamento de relacionamentos do SnapMirror e cópias Snapshot • Visualização de volumes e informações de rede
vsadmin-SnapLock	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Gerenciamento de volumes, exceto movimentos de volume • Gerenciamento de cotas, qtrees, cópias Snapshot e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurando protocolos: NFS e SMB • Configurando serviços: DNS, LDAP e NIS • Tarefas de monitorização • Monitoramento de conexões de rede e interface de rede
vsadmin-readonly	• Gerir a palavra-passe local da própria conta de utilizador e informações-chave • Monitoramento da integridade do SVM • Monitorização da interface de rede • Visualização de volumes e LUNs • Visualização de serviços e protocolos

Controle o acesso do administrador

A função atribuída a um administrador determina quais funções o administrador pode executar com o System Manager. Funções predefinidas para administradores de cluster e administradores de VM de storage são fornecidas pelo System Manager. Você atribui a função ao criar a conta do administrador ou pode atribuir uma função diferente posteriormente.

Dependendo de como você ativou o acesso à conta, talvez seja necessário executar qualquer um dos seguintes procedimentos:

- Associar uma chave pública a uma conta local.
- Instale um certificado digital de servidor assinado pela CA.

- Configure o acesso AD, LDAP ou NIS.

Você pode executar essas tarefas antes ou depois de ativar o acesso à conta.

Atribuindo uma função a um administrador

Atribua uma função a um administrador, da seguinte forma:

Passos

1. Selecione **Cluster > Settings**.
2. Selecione → ao lado de **usuários e funções**.
3. + Add Selecione em **Users**.
4. Especifique um nome de usuário e selecione uma função no menu suspenso **role**.
5. Especifique um método de login e uma senha para o usuário.

Alterar a função de administrador

Altere a função de um administrador, da seguinte forma:

Passos

1. Clique em **Cluster > Settings**.
2. Selecione o nome do usuário cuja função deseja alterar e clique no ⋮ que aparece ao lado do nome de usuário.
3. Clique em **Editar**.
4. Selecione uma função no menu suspenso **Role**.

Gerenciar contas de administrador

Visão geral das contas de administrador

Dependendo de como você ativou o acesso à conta, talvez seja necessário associar uma chave pública a uma conta local, instalar um certificado digital de servidor assinado pela CA ou configurar o acesso AD, LDAP ou NIS. Você pode executar todas essas tarefas antes ou depois de ativar o acesso à conta.

Associar uma chave pública a uma conta de administrador

Para autenticação de chave pública SSH, você deve associar a chave pública a uma conta de administrador antes que a conta possa acessar o SVM. Você pode usar o `security login publickey create` comando para associar uma chave a uma conta de administrador.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma senha e uma chave pública SSH, a conta será autenticada primeiro com a chave pública.

Antes de começar

- Você deve ter gerado a chave SSH.

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Associar uma chave pública a uma conta de administrador:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-comment` *`comment`*

   Para obter a sintaxe de comando completa, consulte a referência de Planilha para "Associar uma chave pública a uma conta de utilizador".

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir associa uma chave pública à conta de administrador do SVM `svmadmin1` para o `engData1` SVM . A chave pública recebe o número de índice 5.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

Gerenciar chaves públicas SSH e certificados X,509 para uma conta de administrador

Para maior segurança de autenticação SSH com contas de administrador, você pode usar o `security login publickey` conjunto de comandos para gerenciar a chave pública SSH e sua associação com certificados X,509.

Associar uma chave pública e um certificado X,509 a uma conta de administrador

A partir do ONTAP 9.13,1, é possível associar um certificado X,509 à chave pública associada à conta de administrador. Isso dá a você a segurança adicional de verificações de expiração ou revogação de certificados no login SSH para essa conta.

Sobre esta tarefa

Se você autenticar uma conta via SSH com uma chave pública SSH e um certificado X,509, o ONTAP verifica a validade do certificado X,509 antes de autenticar com a chave pública SSH. O login SSH será recusado se esse certificado estiver expirado ou revogado, e a chave pública será automaticamente desativada.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Você deve ter gerado a chave SSH.
- Se você precisar apenas do certificado X,509 para ser verificado para a expiração, você pode usar um certificado autoassinado.
- Se você precisar que o certificado X,509 seja verificado quanto à expiração e revogação:
  - Você deve ter recebido o certificado de uma autoridade de certificação (CA).

- Você deve instalar a cadeia de certificados (certificados de CA intermediária e raiz) usando `security certificate install` comandos.
- Você precisa ativar o OCSP para SSH. "Verifique se os certificados digitais são válidos usando OCSP"Consulte para obter instruções.

Passos

1. Associar uma chave pública e um certificado X,509 a uma conta de administrador:

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   Para obter a sintaxe de comando completa, consulte a referência de Planilha para "Associar uma chave pública a uma conta de utilizador".

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir associa uma chave pública e um certificado X,509 à conta de administrador do SVM `svmadmin2` para o `engData2` SVM . A chave pública recebe o número de índice 6.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

Remova a associação de certificados da chave pública SSH para uma conta de administrador

Você pode remover a associação de certificados atual da chave pública SSH da conta, mantendo a chave pública.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a associação de certificados X,509 de uma conta de administrador e guarde a chave pública SSH existente:

   `security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete`

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir remove a associação de certificado X,509 da conta de administrador SVM `svmadmin2` para SVM `engData2` no índice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

Remova a associação de chave pública e certificado de uma conta de administrador

Você pode remover a chave pública atual e a configuração de certificado de uma conta.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Remova a chave pública e uma associação de certificado X,509 de uma conta de administrador:

   `security login publickey delete -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

2. Verifique a alteração visualizando a chave pública:

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

Exemplo

O comando a seguir remove uma chave pública e um certificado X,509 da conta de administrador do SVM `svmadmin3` para o SVM `engData3` no índice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

Configure o Cisco Duo 2FA para logins SSH com o ONTAP

A partir do ONTAP 9.14,1, você pode configurar o ONTAP para usar o Cisco Duo para autenticação de dois fatores (2FA) durante logins SSH. Você configura o Duo no nível do cluster e se aplica a todas as contas de usuário por padrão. Como alternativa, você pode configurar o Duo no nível da VM de armazenamento (anteriormente chamado de vserver), caso em que ele se aplica apenas aos usuários dessa VM de armazenamento. Se você ativar e configurar o Duo, ele serve como um método de autenticação adicional, complementando os métodos existentes para todos os usuários.

Se você ativar a autenticação Duo para logins SSH, os usuários precisarão Registrar um dispositivo na próxima vez que fizerem login usando SSH. Para obter informações sobre a inscrição, consulte o Cisco "documentação de inscrição" Duo .

Você pode usar a interface de linha de comando ONTAP para executar as seguintes tarefas com o Cisco Duo:

- Configure o Cisco Duo
- Altere a configuração do Cisco Duo
- Remova a configuração do Cisco Duo
- Veja a configuração do Cisco Duo
- Remova um grupo Duo
- Ver grupos Duo
- Ignorar a autenticação Duo para usuários

Configure o Cisco Duo

Você pode criar uma configuração do Cisco Duo para todo o cluster ou para uma VM de armazenamento específica (chamada de vserver na CLI do ONTAP) usando o[`security login duo create` comando. Quando você faz isso, o Cisco Duo é habilitado para logins SSH para esse cluster ou VM de armazenamento. Saiba mais sobre o[`security login duo create` comando ONTAP na referência de comando.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.
2. Aceda a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.
5. Ative a autenticação do Cisco Duo para esta VM de armazenamento, substituindo as informações do seu ambiente pelos valores entre parênteses:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Altere a configuração do Cisco Duo

Você pode alterar a maneira como o Cisco Duo autentica os usuários (por exemplo, quantos prompts de autenticação são fornecidos ou qual proxy HTTP é usado). Se você precisar alterar a configuração do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP), use o[`security login duo modify` comando. Saiba mais sobre o[`security login duo modify` comando ONTAP na referência de comando.

Passos

1. Inicie sessão no Painel de Administração do Cisco Duo.
2. Aceda a **aplicações > aplicação UNIX**.
3. Registre sua chave de integração, chave secreta e nome de host da API.
4. Faça login na sua conta ONTAP usando SSH.
5. Altere a configuração do Cisco Duo para esta VM de armazenamento, substituindo as informações atualizadas do seu ambiente pelos valores entre parênteses:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

Remova a configuração do Cisco Duo

Você pode remover a configuração do Cisco Duo, que removerá a necessidade de os usuários SSH se autenticarem usando o Duo no início de sessão. Para remover a configuração do Cisco Duo para uma VM de armazenamento (conhecida como vserver na CLI do ONTAP), você pode usar o[`security login duo delete` comando. Saiba mais sobre o[`security login duo delete` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Remova a configuração do Cisco Duo para esta VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

Isso exclui permanentemente a configuração do Cisco Duo para essa VM de armazenamento.

Veja a configuração do Cisco Duo

Você pode exibir a configuração existente do Cisco Duo para uma VM de armazenamento (chamada de vserver na CLI do ONTAP) usando o[`security login duo show` comando. Saiba mais sobre o[`security login duo show` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostrar a configuração do Cisco Duo para esta VM de armazenamento. Opcionalmente, você pode usar o `vserver` parâmetro para especificar uma VM de armazenamento, substituindo o nome da VM de armazenamento por `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

Você deve ver saída semelhante ao seguinte:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Crie um grupo Duo

Você pode instruir o Cisco Duo a incluir somente os usuários em um determinado ative Directory, LDAP ou grupo de usuários local no processo de autenticação Duo. Se você criar um grupo Duo, somente os usuários desse grupo serão solicitados a autenticação Duo. Você pode criar um grupo Duo usando o[`security login duo group create` comando. Quando você cria um grupo, você pode excluir usuários específicos desse grupo do processo de autenticação Duo. Saiba mais sobre o[`security login duo group create` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Crie o grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será criado no nível do cluster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-excluded-users` não serão incluídos no processo de autenticação Duo.

Ver grupos Duo

Você pode exibir entradas de grupo existentes do Cisco Duo usando o[`security login duo group show` comando. Saiba mais sobre o[`security login duo group show` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Mostre as entradas do grupo Duo, substituindo as informações do seu ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será mostrado no nível do cluster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o parâmetro opcional `-excluded-users` não serão exibidos.

Remova um grupo Duo

Você pode remover uma entrada de grupo Duo usando o[`security login duo group delete` comando. Se você remover um grupo, os usuários desse grupo não serão mais incluídos no processo de autenticação Duo. Saiba mais sobre o[`security login duo group delete` comando ONTAP na referência de comando.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Remova a entrada do grupo Duo, substituindo as informações do ambiente pelos valores entre parênteses. Se você omitir o `-vserver` parâmetro, o grupo será removido no nível do cluster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local.

Ignorar a autenticação Duo para usuários

Você pode excluir todos os usuários ou usuários específicos do processo de autenticação Duo SSH.

Excluir todos os usuários Duo

Você pode desativar a autenticação SSH do Cisco Duo para todos os usuários.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários SSH, substituindo o nome do SVM para `<STORAGE_VM_NAME>`:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

Excluir usuários do grupo Duo

Você pode excluir certos usuários que fazem parte de um grupo Duo do processo de autenticação Duo SSH.

Passos

1. Faça login na sua conta ONTAP usando SSH.
2. Desative a autenticação Cisco Duo para usuários específicos em um grupo. Substitua o nome do grupo e

a lista de usuários para excluir pelos valores entre parênteses:

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

O nome do grupo Duo tem de corresponder a um grupo ative Directory, LDAP ou local. Os usuários que você especificar com o `-excluded-users` parâmetro não serão incluídos no processo de autenticação Duo.

Excluir usuários locais Duo

Você pode excluir usuários locais específicos do uso da autenticação Duo usando o Painel de Administração do Cisco Duo. Para obter instruções, consulte "Documentação do Cisco Duo" a .

Gere e instale uma visão geral do certificado de servidor assinado pela CA

Em sistemas de produção, é uma prática recomendada instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL. Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da autoridade de certificação.

Gerar uma solicitação de assinatura de certificado

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

   ```
   security certificate generate-csr -common-name FQDN_or_common_name -size
   512|1024|1536|2048 -country country -state state -locality locality
   -organization organization -unit unit -email-addr email_of_contact -hash
   -function SHA1|SHA256|MD5
   ```

   O comando a seguir cria uma CSR com uma chave privada de 2048 bits gerada pela função de hash "'SHA256'" para uso pelo grupo "'Software'" no departamento de TI de uma empresa cujo nome comum personalizado é "erver1.companyname.com`", localizado em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contato da SVM é "'web@example.com". O sistema apresenta a CSR e a chave privada na saída.

Exemplo de criação de uma CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. Copie a solicitação de certificado da saída CSR e envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

   Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA

Você pode usar o `security certificate install` comando para instalar um certificado de servidor assinado pela CA em um SVM. O ONTAP solicita os certificados raiz e intermediário da autoridade de certificação (CA) que formam a cadeia de certificados do certificado do servidor.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Instale um certificado de servidor assinado pela CA:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > O ONTAP solicita os certificados raiz e intermediários da CA que formam a cadeia de certificados do certificado do servidor. A cadeia começa com o certificado da CA que emitiu o certificado do servidor e pode variar até o certificado raiz da CA. Qualquer certificado intermediário ausente resulta na falha da instalação do certificado do servidor.

   O comando a seguir instala o certificado de servidor assinado pela CA e os certificados intermediários na SVM "'engData2".

Exemplo de instalação de certificados intermediários de certificado de servidor assinado pela CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

Gerencie certificados com o System Manager

A partir do ONTAP 9.10,1, você pode usar o Gerenciador do sistema para gerenciar autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais (integradas).

Com o System Manager, você pode gerenciar os certificados recebidos de outros aplicativos para que você possa autenticar as comunicações desses aplicativos. Você também pode gerenciar seus próprios certificados que identificam seu sistema para outros aplicativos.

Exibir informações do certificado

Com o System Manager, é possível exibir autoridades de certificação confiáveis, certificados de cliente/servidor e autoridades de certificação locais armazenadas no cluster.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Role até a área **Segurança**. Na seção **certificados**, os seguintes detalhes são exibidos:
   - O número de autoridades de certificação confiáveis armazenadas.
   - O número de certificados de cliente/servidor armazenados.
   - O número de autoridades locais de certificação armazenadas.
3. Selecione qualquer número para ver detalhes sobre uma categoria de certificados ou → selecione para abrir a página **certificados**, que contém informações sobre todas as categorias. A lista exibe as informações de todo o cluster. Se você quiser exibir informações apenas para uma VM de armazenamento específica, execute as seguintes etapas:
   a. Selecione **Storage > Storage VMs**.
   b. Selecione a VM de armazenamento.
   c. Mude para o separador **Settings**.

d. Selecione um número mostrado na seção **certificado**.

O que fazer a seguir

- Na página **certificados**, você pode Gerar uma solicitação de assinatura de certificado.
- As informações do certificado são separadas em três guias, uma para cada categoria. Você pode executar as seguintes tarefas em cada guia:

Neste separador…	Pode executar estes procedimentos…
Autoridades de certificação confiáveis	• [install-trusted-cert] • Excluir uma autoridade de certificação confiável • Renove uma autoridade de certificação confiável
Certificados de cliente/servidor	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• Autoridades de certificação locais*	• Crie uma nova autoridade de certificação local • Assine um certificado usando uma autoridade de certificação local • Eliminar uma autoridade de certificação local • Renove uma autoridade de certificação local

Gerar uma solicitação de assinatura de certificado

Você pode gerar uma solicitação de assinatura de certificado (CSR) com o System Manager a partir de qualquer guia da página **certificados**. Uma chave privada e uma CSR correspondente são geradas, que podem ser assinadas usando uma autoridade de certificação para gerar um certificado público.

Passos

1. Veja a página **certificados**. Exibir informações do certificadoConsulte .
2. Selecione * gerar CSR*.
3. Preencha as informações para o nome do assunto:
   a. Introduza um **nome comum**.
   b. Selecione um **país**.
   c. Introduza uma **organização**.
   d. Introduza uma **unidade organizacional**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Instale (adicione) uma autoridade de certificação confiável

Você pode instalar autoridades de certificação confiáveis adicionais no System Manager.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .

2. + Add Selecione .
3. No painel **Adicionar autoridade de certificação confiável**, execute o seguinte:
   - Introduza um **nome**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Introduza ou importe **detalhes do certificado**.

Excluir uma autoridade de certificação confiável

Com o System Manager, você pode excluir uma autoridade de certificação confiável.

Não é possível excluir autoridades de certificado confiáveis pré-instaladas com o ONTAP.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione ⋮ ao lado do nome e selecione **Excluir**.

Renove uma autoridade de certificação confiável

Com o System Manager, você pode renovar uma autoridade de certificação confiável que expirou ou está prestes a expirar.

Passos

1. Veja a guia **autoridades de certificados confiáveis**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação fidedigna.
3. Selecione ⋮ ao lado do nome do certificado e depois **Renew**.

Instale (adicione) um certificado cliente/servidor

Com o System Manager, você pode instalar certificados de cliente/servidor adicionais.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. + Add Selecione .
3. No painel **Adicionar certificado de cliente/servidor**, execute o seguinte:
   - Introduza um **nome de certificado**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Introduza ou importe **detalhes do certificado**. Você pode escrever ou copiar e colar os detalhes do certificado de um arquivo de texto ou importar o texto de um arquivo de certificado clicando em **Importar**.

- Introduza a **chave privada**. Você pode escrever ou copiar e colar na chave privada de um arquivo de texto ou pode importar o texto de um arquivo de chave privada clicando em **Importar**.

Gerar (adicionar) um certificado cliente/servidor autoassinado

Com o System Manager, você pode gerar certificados de cliente/servidor autoassinados adicionais.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione * gerar certificado autoassinado*.
3. No painel **Generate Self-signed Certificate** (gerar certificado autoassinado), execute o seguinte procedimento:
   - Introduza um **nome de certificado**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
   - Selecione um **tipo**.
   - Selecione uma função **hash**.
   - Selecione um **tamanho da chave**.
   - Selecione uma **VM de armazenamento**.

Excluir um certificado cliente/servidor

Com o System Manager, pode eliminar certificados de cliente/servidor.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione ⋮ ao lado do nome e clique em **Excluir**.

Renove um certificado cliente/servidor

Com o System Manager, você pode renovar um certificado cliente/servidor que expirou ou está prestes a expirar.

Passos

1. Veja a guia **certificados de cliente/servidor**. Exibir informações do certificadoConsulte .
2. Selecione o nome do certificado cliente/servidor.
3. Selecione ⋮ ao lado do nome e, em seguida, clique em **Renew**.

Crie uma nova autoridade de certificação local

Com o System Manager, você pode criar uma nova autoridade de certificação local.

Passos

1. Veja a guia **autoridades de certificados locais**. Exibir informações do certificadoConsulte .
2. 

Selecione .

3. No painel **Add local Certificate Authority** (Adicionar autoridade de certificação local), execute o seguinte procedimento:
   - Introduza um **nome**.
   - Para o **Escopo**, selecione uma VM de armazenamento.
   - Introduza um **nome comum**.
4. Se você quiser substituir os padrões, selecione **mais opções** e forneça informações adicionais.

Assine um certificado usando uma autoridade de certificação local

No System Manager, você pode usar uma autoridade de certificação local para assinar um certificado.

Passos

1. Veja a guia **autoridades de certificados locais**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e depois **assinar um certificado**.
4. Preencha o formulário **assinar um pedido de assinatura de certificado**.
   - Você pode colar no conteúdo de assinatura de certificado ou importar um arquivo de solicitação de assinatura de certificado clicando em **Importar**.
   - Especifique o número de dias para os quais o certificado será válido.

Eliminar uma autoridade de certificação local

Com o System Manager, pode eliminar uma autoridade de certificação local.

Passos

1. Veja a guia **Autoridade de Certificação local**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e, em seguida, **Excluir**.

Renove uma autoridade de certificação local

Com o System Manager, você pode renovar uma autoridade de certificação local que expirou ou está prestes a expirar.

Passos

1. Veja a guia **Autoridade de Certificação local**. Exibir informações do certificadoConsulte .
2. Selecione o nome da autoridade de certificação local.
3. Selecione ⋮ ao lado do nome e, em seguida, clique em **Renew**.

Configure a visão geral do acesso do controlador de domínio do ative Directory

Você deve configurar o acesso do controlador de domínio do AD ao cluster ou SVM antes que uma conta do AD possa acessar o SVM. Se você já tiver configurado um servidor SMB para um SVM de dados, poderá configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster. Se você não tiver configurado um servidor SMB, poderá criar uma conta de computador para o SVM no domínio AD.

O ONTAP oferece suporte aos seguintes serviços de autenticação de controlador de domínio:

- Kerberos
- LDAP
- NETLOGON
- Autoridade de Segurança local (LSA)

O ONTAP suporta os seguintes algoritmos de chave de sessão para conexões seguras de Netlogon:

Algoritmo da chave de sessão	Disponível a partir de…
HMAC-SHA256, com base no padrão de criptografia avançada (AES) se o cluster estiver executando o ONTAP 9.9,1 ou anterior e o controlador de domínio forçar o AES para serviços de Netlogon seguros, a conexão falhará. Nesse caso, você precisa reconfigurar seu controlador de domínio para aceitar conexões de chave forte com o ONTAP.	ONTAP 9.10,1
DES e HMAC-MD5 (quando a chave forte está definida)	Todos os lançamentos do ONTAP 9

Se você quiser usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon, você precisa verificar se o AES está habilitado no SVM.

- A partir do ONTAP 9.14,1, o AES é ativado por padrão quando você cria um SVM e não precisa modificar as configurações de segurança do seu SVM para usar chaves de sessão AES durante o estabelecimento de canal seguro Netlogon.
- No ONTAP 9.10,1 a 9.13.1, o AES é desativado por padrão quando você cria um SVM. Você precisa ativar o AES usando o seguinte comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

> Quando você atualiza para o ONTAP 9.14,1 ou posterior, a configuração AES para SVMs existentes que foram criadas com versões mais antigas do ONTAP não será alterada automaticamente. Você ainda precisa atualizar o valor dessa configuração para ativar o AES nesses SVMs.

Configurar um túnel de autenticação

Se você já tiver configurado um servidor SMB para um SVM de dados, poderá usar o `security login domain-tunnel create` comando para configurar o SVM como um gateway, ou *tunnel*, para acesso AD ao cluster.

Antes de começar

- Você precisa ter configurado um servidor SMB para um data SVM.
- Você deve ter habilitado uma conta de usuário de domínio do AD para acessar o SVM do administrador do cluster.
- Você deve ser um administrador de cluster para executar esta tarefa.

A partir do ONTAP 9.10,1, se você tiver um gateway SVM (túnel de domínio) para acesso AD, você poderá usar o Kerberos para autenticação de administrador se tiver desabilitado o NTLM no domínio do AD. Em versões anteriores, o Kerberos não era compatível com autenticação de administrador para gateways SVM. Esta funcionalidade está disponível por padrão; nenhuma configuração é necessária.

> A autenticação Kerberos é sempre tentada primeiro. Em caso de falha, a autenticação NTLM é então tentada.

Passo

1. Configure um SVM de dados habilitado para SMB como um túnel de autenticação para acesso do controlador de domínio do AD ao cluster:

   `security login domain-tunnel create -vserver` *`svm_name`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > O SVM deve estar em execução para que o usuário seja autenticado.

   O comando a seguir configura o SVM de dados habilitado para SMB "'engData" como um túnel de autenticação.

   ```
   cluster1::>security login domain-tunnel create -vserver engData
   ```

Crie uma conta de computador SVM no domínio

Se você não tiver configurado um servidor SMB para um SVM de dados, poderá usar o `vserver active-directory create` comando para criar uma conta de computador para o SVM no domínio.

Sobre esta tarefa

Depois de inserir o `vserver active-directory create` comando, você será solicitado a fornecer as credenciais para uma conta de usuário do AD com Privileges suficiente para adicionar computadores à unidade organizacional especificada no domínio. A senha da conta não pode estar vazia.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma conta de computador para um SVM no domínio AD:

   `vserver active-directory create -vserver` *`SVM_name`* `-account-name` *`NetBIOS_account_name`* `-domain` *`domain`* `-ou` *`organizational_unit`*

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir cria uma conta de computador chamada "'ADSERVER1"" no domínio "'example.com`'" para SVM "'engData". Você será solicitado a inserir as credenciais da conta de usuário do AD depois de inserir o comando.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

Configure a visão geral do acesso ao servidor LDAP ou NIS

Você deve configurar o acesso de servidor LDAP ou NIS a um SVM antes que as contas LDAP ou NIS possam acessar o SVM. O recurso de switch permite que você use LDAP ou NIS como fontes alternativas de serviço de nomes.

Configurar o acesso ao servidor LDAP

Você deve configurar o acesso do servidor LDAP a um SVM antes que as contas LDAP possam acessar o SVM. Você pode usar o `vserver services name-service ldap client create` comando para criar uma configuração de cliente LDAP no SVM. Em seguida, você pode usar o `vserver services name-service ldap create` comando para associar a configuração do cliente LDAP ao SVM.

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 2016 e servidores AD posteriores)
- Ad-SFU (Windows 2003 e servidores AD anteriores)
- RFC-2307 (SERVIDORES LDAP UNIX)

É melhor usar os esquemas padrão, a menos que haja um requisito para fazer o contrário. Nesse caso, você pode criar seu próprio esquema copiando um esquema padrão e modificando a cópia. Para obter mais informações, consulte:

- "Configuração NFS"
- "Relatório técnico do NetApp 4835: Como configurar o LDAP no ONTAP"

Antes de começar

- Você precisa ter instalado a "Certificado digital do servidor assinado pela CA"no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Criar uma configuração de cliente LDAP em uma SVM:

`vserver services name-service ldap client create -vserver <SVM_name> -client -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema> -use-start-tls <true|false>`

> Iniciar TLS é compatível apenas para acesso a SVMs de dados. Ele não é compatível com acesso a SVMs administrativas.

Para obter a sintaxe de comando completa, consulte "folha de trabalho".

O comando a seguir cria uma configuração de cliente LDAP chamada `corp` em SVM `engData`. O cliente faz ligações anônimas aos servidores LDAP com os endereços IP 172.160.0.100 e 172.16.0.101. O cliente usa o esquema RFC-2307 para fazer consultas LDAP. A comunicação entre o cliente e o servidor é criptografada usando Iniciar TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

> 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.

2. Associe a configuração do cliente LDAP à SVM: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir associa a configuração do cliente LDAP `corp` ao SVM `engData` e habilita o cliente LDAP no SVM.

   ```
   cluster1::>vserver services name-service ldap create -vserver engData
   -client-config corp -client-enabled true
   ```

   > 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.

3. 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 vs0.

```
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".                                                    |
```

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

Configurar o acesso ao servidor NIS

Você deve configurar o acesso do servidor NIS a um SVM antes que as contas NIS possam acessar o SVM. Você pode usar o `vserver services name-service nis-domain create` comando para criar uma configuração de domínio NIS em um SVM.

Antes de começar

- Todos os servidores configurados devem estar disponíveis e acessíveis antes de configurar o domínio NIS no SVM.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Crie uma configuração de domínio NIS em uma SVM:

   `vserver services name-service nis-domain create -vserver <SVM_name> -domain <client_configuration> -nis-servers <NIS_server_IPs>`

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   > 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.

   O comando a seguir cria uma configuração de domínio NIS no SVM `engData`. O domínio NIS `nisdomain` comunica com um servidor NIS com o endereço IP `192.0.2.180` .

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -nis-servers 192.0.2.180
```

Crie um switch de serviço de nomes

O recurso de switch de serviço de nomes permite que você use LDAP ou NIS como fontes alternativas de serviço de nomes. Você pode usar o `vserver services name-service ns-switch modify` comando para especificar a ordem de pesquisa para fontes de serviço de nome.

Antes de começar

- Tem de ter configurado o acesso ao servidor LDAP e NIS.

- Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passo

1. Especifique a ordem de pesquisa para fontes do serviço de nomes:

   `vserver services name-service ns-switch modify -vserver <SVM_name> -database <name_service_switch_database> -sources <name_service_source_order>`

   Para obter a sintaxe de comando completa, consulte "folha de trabalho".

   O comando a seguir especifica a ordem de pesquisa das fontes de serviço de nomes LDAP e NIS para o `passwd` banco de dados no SVM `engData`.

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

Altere uma senha de administrador no ONTAP

Você deve alterar sua senha inicial imediatamente após fazer login no sistema pela primeira vez. Se você for um administrador SVM, poderá usar o `security login password` comando para alterar sua própria senha. Se for um administrador de cluster, pode utilizar o `security login password` comando para alterar a palavra-passe de qualquer administrador.

Sobre esta tarefa

A nova palavra-passe deve respeitar as seguintes regras:

- Não pode conter o nome de utilizador
- Deve ter pelo menos oito carateres
- Deve conter pelo menos uma letra e um número
- Não pode ser o mesmo que as últimas seis senhas

> Você pode usar o[`security login role config modify` comando para modificar as regras de senha para contas associadas a uma determinada função. Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-login-role-config-modify.html[`security login role config modify` em referência de comando ONTAP.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para alterar sua própria senha.
- Você deve ser um administrador de cluster para alterar a senha de outro administrador.

Passo

1. Alterar uma palavra-passe de administrador: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   O comando a seguir altera a senha do administrador `admin1` do SVM`vs1.example.com`. É-lhe pedido que introduza a palavra-passe atual e, em seguida, introduza e volte a introduzir a nova palavra-passe.

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

Bloquear e desbloquear uma conta de administrador

Você pode usar o `security login lock` comando para bloquear uma conta de administrador e o `security login unlock` comando para desbloquear a conta.

Antes de começar

Você deve ser um administrador de cluster para executar essas tarefas.

Passos

1. Bloquear uma conta de administrador:

   `security login lock -vserver SVM_name -username user_name`

   O comando a seguir bloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. Desbloquear uma conta de administrador:

   `security login unlock -vserver SVM_name -username user_name`

   O comando a seguir desbloqueia a conta de administrador `admin1` do SVM `vs1.example.com`:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

Gerir tentativas de início de sessão falhadas

Tentativas repetidas de login falhadas às vezes indicam que um intruso está tentando acessar o sistema de armazenamento. Você pode executar várias etapas para garantir que não ocorra uma intrusão.

Como você saberá que as tentativas de login falharam

O sistema de Gestão de Eventos (EMS) notifica-o sobre tentativas falhadas de início de sessão a cada hora. Pode encontrar um registo de tentativas de início de sessão falhadas `audit.log` no ficheiro.

O que fazer se tentativas repetidas de login falharem

A curto prazo, você pode executar várias etapas para evitar uma intrusão:

- Exigir que as senhas sejam compostas por um número mínimo de carateres maiúsculos, minúsculos, carateres especiais e/ou dígitos
- Impor um atraso após uma tentativa de início de sessão com falha
- Limite o número de tentativas de início de sessão falhadas permitidas e bloqueie os utilizadores após o número especificado de tentativas falhadas
- Expire e bloqueie contas que estejam inativas por um determinado número de dias

Você pode usar o `security login role config modify` comando para executar essas tarefas.

A longo prazo, você pode seguir estes passos adicionais:

- Use o `security ssh modify` comando para limitar o número de tentativas de login falhadas para todos os SVMs recém-criados.
- Migre contas de algoritmo MD5 existentes para o algoritmo SHA-512 mais seguro, exigindo que os usuários alterem suas senhas.

Aplicar SHA-2 em senhas de conta de administrador

As contas de administrador criadas antes do ONTAP 9.0 continuam a usar senhas MD5 após a atualização, até que as senhas sejam alteradas manualmente. O MD5 é menos seguro do que o SHA-2. Portanto, após a atualização, você deve solicitar aos usuários de contas MD5 que alterem suas senhas para usar a função hash SHA-512 padrão.

Sobre esta tarefa

A funcionalidade hash de senha permite que você faça o seguinte:

- Exibir contas de usuário que correspondem à função hash especificada.
- Expire contas que usam uma função hash especificada (por exemplo, MD5), forçando os usuários a alterar suas senhas em seu próximo login.
- Bloquear contas cujas senhas usam a função hash especificada.
- Ao reverter para uma versão anterior ao ONTAP 9, redefina a própria senha do administrador do cluster para que ela seja compatível com a função hash (MD5) que é suportada pela versão anterior.

O ONTAP aceita senhas SHA-2 pré-hash somente usando o SDK de gerenciamento do NetApp (`security-login-create`e `security-login-modify-password`o).

Passos

1. Migre as contas de administrador do MD5 para a função hash de senha SHA-512:
   a. Expire todas as contas de administrador do MD5: `security login expire-password -vserver * -username * -hash-function md5`

      Isso força os usuários de conta do MD5 a alterar suas senhas no próximo login.

   b. Peça aos usuários de contas do MD5 para fazer login por meio de um console ou sessão SSH.

      O sistema deteta que as contas estão expiradas e solicita aos usuários que alterem suas senhas. Sha-512 é usado por padrão para as senhas alteradas.
2. Para contas do MD5 cujos usuários não fazem login para alterar suas senhas dentro de um período de

tempo, force a migração da conta:

a. Bloquear contas que ainda usam a função hash MD5 (nível de privilégio avançado): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

   Após o número de dias especificado pelo `-lock-after`, os usuários não podem acessar suas contas do MD5.

b. Desbloqueie as contas quando os usuários estiverem prontos para alterar suas senhas: `security login unlock -vserver svm_name -username user_name`

c. Faça com que os usuários façam login em suas contas por meio de uma sessão de console ou SSH e alterem suas senhas quando o sistema solicitar que façam isso.

Diagnosticar e corrigir problemas de acesso a arquivos

Passos

1. No System Manager, selecione **Storage > Storage VMs**.
2. Selecione a VM de armazenamento na qual você deseja executar um rastreamento.
3. Clique ⋮ em **mais**.
4. Clique em **Trace File Access**.
5. Forneça o nome de usuário e o endereço IP do cliente e clique em **Iniciar rastreamento**.

   Os resultados do rastreio são apresentados numa tabela. A coluna **razões** fornece o motivo pelo qual um arquivo não pôde ser acessado.

6. Clique ⌄ na coluna esquerda da tabela de resultados para visualizar as permissões de acesso ao arquivo.

Gerenciar a verificação de vários administradores

Visão geral da verificação de vários administradores do ONTAP

A partir do ONTAP 9.11,1, você pode usar a verificação multiadministrador (MAV) para garantir que certas operações, como a exclusão de volumes ou cópias Snapshot, possam ser executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração da verificação de vários administradores consiste em:

- "Criando um ou mais grupos de aprovação de administrador."
- "Habilitando a funcionalidade de verificação de vários administradores."
- "Adicionar ou modificar regras."

Após a configuração inicial, esses elementos só podem ser modificados por administradores em um grupo de aprovação MAV (administradores MAV).

Quando a verificação multi-admin está ativada, a conclusão de cada operação protegida requer estes passos:

1. Quando um utilizador inicia a operação, a "a solicitação é gerada."
2. Antes que a operação possa ser executada, pelo menos uma "O administrador do MAV deve aprovar."
3. Após a aprovação, o usuário é solicitado e conclui a operação.

> Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

A verificação multiadministrador não se destina a ser usada com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada exigiria aprovação antes que a operação pudesse ser concluída. Se você quiser usar automação e MAV juntos, é recomendável usar consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

> A verificação multi-admin não está disponível com o Cloud Volumes ONTAP.

Como a verificação multi-admin funciona

A verificação multi-admin consiste em:

- Um grupo de um ou mais administradores com poderes de aprovação e veto.
- Um conjunto de operações ou comandos protegidos em uma tabela *rules*.
- Um mecanismo *regras* para identificar e controlar a execução de operações protegidas.

As regras MAV são avaliadas após regras de controle de acesso baseado em função (RBAC). Portanto, os administradores que executam ou aprovam operações protegidas já devem possuir o Privileges RBAC mínimo para essas operações. "Saiba mais sobre o RBAC".

Regras definidas pelo sistema

Quando a verificação multi-admin está ativada, as regras definidas pelo sistema (também conhecidas como regras *guard-rail*) estabelecem um conjunto de operações MAV para conter o risco de contornar o próprio processo MAV. Essas operações não podem ser removidas da tabela de regras. Quando o MAV estiver ativado, as operações designadas por um asterisco (*) requerem aprovação por um ou mais administradores antes da execução, exceto para os comandos **show**.

- `security multi-admin-verify modify` operação `*`

  Controla a configuração da funcionalidade de verificação de vários administradores.

- `security multi-admin-verify approval-group` operações `*`

  Controle a associação no conjunto de administradores com credenciais de verificação multi-admin.

- `security multi-admin-verify rule` operações `*`

  Controle o conjunto de comandos que exigem verificação multi-admin.

- `security multi-admin-verify request` operações

  Controle o processo de aprovação.

Comandos protegidos por regras

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

- `security login password`
- `security login unlock`
- `set`

Cada versão do ONTAP fornece mais comandos que você pode escolher para proteger com regras de verificação de vários administradores. Escolha a versão do ONTAP para obter a lista completa de comandos disponíveis para proteção.

9.16.1

- `cluster date modify` 3
- `cluster log-forwarding create` 3
- `cluster log-forwarding delete` 3
- `cluster log-forwarding modify` 3
- `cluster peer delete`
- `cluster time-service ntp server create` 3
- `cluster time-service ntp server delete` 3
- `cluster time-service ntp server key create` 3
- `cluster time-service ntp server key delete` 3
- `cluster time-service ntp server key modify` 3
- `cluster time-service ntp server modify` 3
- `event config modify`
- `lun delete` 3
- `security anti-ransomware volume attack clear-suspect` 1
- `security anti-ransomware volume disable` 1
- `security anti-ransomware volume event-log modify` 2
- `security anti-ransomware volume pause` 1
- `security anti-ransomware vserver event-log modify` 2
- `security audit modify` 3
- `security ipsec config modify` 3
- `security ipsec policy create` 3
- `security ipsec policy delete` 3
- `security ipsec policy modify` 3
- `security login create`
- `security login delete`
- `security login modify`
- `security key-manager onboard update-passphrase` 3
- `security saml-sp create` 3
- `security saml-sp delete` 3
- `security saml-sp modify` 3
- `snaplock legal-hold end` 3
- `storage aggregate delete` 3

- storage aggregate offline 4
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3
- timezone 3
- volume create 3
- volume delete
- volume encryption conversion start 4
- volume encryption rekey start 4
- volume file privileged-delete 3
- volume flexcache delete
- volume modify 3
- volume recovery-queue modify 2
- volume recovery-queue purge 2

- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot create 3
- volume snapshot delete
- volume snapshot modify 3
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename 3
- volume snapshot restore
- vserver audit create 3
- vserver audit delete 3
- vserver audit disable 3
- vserver audit modify 3
- vserver audit rotate-log 3
- vserver create 2
- vserver consistency-group create 4
- vserver consistency-group delete 4
- vserver consistency-group modify 4
- vserver consistency-group snapshot create 4
- vserver consistency-group snapshot delete 4
- vserver delete 3
- vserver modify 2
- vserver object-store-server audit create 3
- vserver object-store-server audit delete 3
- vserver object-store-server audit disable 3
- vserver object-store-server audit modify 3
- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete

- vserver security file-directory apply 3
- vserver security file-directory remove-slag 3
- vserver stop 4
- vserver vscan disable 3
- vserver vscan on-access-policy create 3
- vserver vscan on-access-policy delete 3
- vserver vscan on-access-policy disable 3
- vserver vscan on-access-policy modify 3
- vserver vscan scanner-pool create 3
- vserver vscan scanner-pool delete 3
- vserver vscan scanner-pool modify 3

9.15.1

- cluster date modify 3
- cluster log-forwarding create 3
- cluster log-forwarding delete 3
- cluster log-forwarding modify 3
- cluster peer delete
- cluster time-service ntp server create 3
- cluster time-service ntp server delete 3
- cluster time-service ntp server key create 3
- cluster time-service ntp server key delete 3
- cluster time-service ntp server key modify 3
- cluster time-service ntp server modify 3
- event config modify
- lun delete 3
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume event-log modify 2
- security anti-ransomware volume pause 1
- security anti-ransomware vserver event-log modify 2
- security audit modify 3
- security ipsec config modify 3
- security ipsec policy create 3

- security ipsec policy delete 3
- security ipsec policy modify 3
- security login create
- security login delete
- security login modify
- security key-manager onboard update-passphrase 3
- security saml-sp create 3
- security saml-sp delete 3
- security saml-sp modify 3
- snaplock legal-hold end 3
- storage aggregate delete 3
- storage encryption disk destroy 3
- storage encryption disk modify 3
- storage encryption disk revert-to-original-state 3
- storage encryption disk sanitize 3
- system bridge run-cli 3
- system controller flash-cache secure-erase run 3
- system controller service-event delete 3
- system health alert delete 3
- system health alert modify 3
- system health policy definition modify 3
- system node autosupport modify 3
- system node autosupport trigger modify 3
- system node coredump delete 3
- system node coredump delete-all 3
- system node hardware nvram-encryption modify 3
- system node run
- system node systemshell
- system script delete 3
- system service-processor ssh add-allowed-addresses 3
- system service-processor ssh remove-allowed-addresses 3
- system smtape restore 3
- system switch ethernet log disable-collection 3
- system switch ethernet log modify 3

- timezone 3
- volume create 3
- volume delete
- volume file privileged-delete 3
- volume flexcache delete
- volume modify 3
- volume recovery-queue modify 2
- volume recovery-queue purge 2
- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot create 3
- volume snapshot delete
- volume snapshot modify 3
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename 3
- volume snapshot restore
- vserver audit create 3
- vserver audit delete 3
- vserver audit disable 3
- vserver audit modify 3
- vserver audit rotate-log 3
- vserver create 2
- vserver delete 3
- vserver modify 2
- vserver object-store-server audit create 3
- vserver object-store-server audit delete 3
- vserver object-store-server audit disable 3
- vserver object-store-server audit modify 3

- vserver object-store-server audit rotate-log 3
- vserver options 3
- vserver peer delete
- vserver security file-directory apply 3
- vserver security file-directory remove-slag 3
- vserver vscan disable 3
- vserver vscan on-access-policy create 3
- vserver vscan on-access-policy delete 3
- vserver vscan on-access-policy disable 3
- vserver vscan on-access-policy modify 3
- vserver vscan scanner-pool create 3
- vserver vscan scanner-pool delete 3
- vserver vscan scanner-pool modify 3

9.14.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume event-log modify 2
- security anti-ransomware volume pause 1
- security anti-ransomware vserver event-log modify 2
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify 2
- volume recovery-queue purge 2
- volume recovery-queue purge-all 2
- volume snaplock modify 1
- volume snapshot autodelete modify

- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create 2
- vserver modify 2
- vserver peer delete

9.13.1

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect 1
- security anti-ransomware volume disable 1
- security anti-ransomware volume pause 1
- security login create
- security login delete
- security login modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify 1
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule

- `volume snapshot restore`
- `vserver peer delete`

9.12.1/9.11.1

- `cluster peer delete`
- `event config modify`
- `security login create`
- `security login delete`
- `security login modify`
- `system node run`
- `system node systemshell`
- `volume delete`
- `volume flexcache delete`
- `volume snapshot autodelete modify`
- `volume snapshot delete`
- `volume snapshot policy add-schedule`
- `volume snapshot policy create`
- `volume snapshot policy delete` *
- `volume snapshot policy modify`
- `volume snapshot policy modify-schedule`
- `volume snapshot policy remove-schedule`
- `volume snapshot restore`
- `vserver peer delete`

1. Novo comando protegido por regras para 9.13.1
2. Novo comando protegido por regras para 9.14.1
3. Novo comando protegido por regras para 9.15.1
4. Novo comando protegido por regras para 9.16.1

*Este comando só está disponível com CLI e não está disponível para o System Manager em algumas versões.

Como funciona a aprovação multi-admin

Sempre que uma operação protegida é inserida em um cluster protegido por MAV, uma solicitação de execução de operação é enviada para o grupo de administradores designado MAV.

Você pode configurar:

- Nomes, informações de Contato e número de administradores no grupo MAV.

Um administrador MAV deve ter uma função RBAC com o administrador de cluster Privileges.

- O número de grupos de administradores do MAV.
  - Um grupo MAV é atribuído para cada regra de operação protegida.
  - Para vários grupos MAV, você pode configurar qual grupo MAV aprova uma determinada regra.
- O número de aprovações MAV necessárias para executar uma operação protegida.
- Um período de expiração de *aprovação* dentro do qual um administrador do MAV deve responder a uma solicitação de aprovação.
- Um período de expiração de *execução* dentro do qual o administrador solicitante deve concluir a operação.

Uma vez configurados esses parâmetros, a aprovação MAV é necessária para modificá-los.

Os administradores do MAV não podem aprovar suas próprias solicitações para executar operações protegidas. Por conseguinte:

- O MAV não deve ser ativado em clusters com apenas um administrador.
- Se houver apenas uma pessoa no grupo MAV, o administrador do MAV não poderá iniciar operações protegidas; os administradores regulares devem iniciar operações protegidas e o administrador do MAV só pode aprovar.
- Se você quiser que os administradores do MAV possam executar operações protegidas, o número de administradores do MAV deve ser maior do que o número de aprovações necessárias. Por exemplo, se duas aprovações forem necessárias para uma operação protegida e você quiser que os administradores do MAV as executem, deve haver três pessoas no grupo de administradores do MAV.

Os administradores do MAV podem receber solicitações de aprovação em alertas de e-mail (usando o EMS) ou podem consultar a fila de solicitações. Quando recebem um pedido, podem tomar uma das três ações:

- Aprovar
- Rejeitar (veto)
- Ignorar (sem ação)

As notificações por e-mail são enviadas a todos os aprovadores associados a uma regra MAV quando:

- Uma solicitação é criada.
- Uma solicitação é aprovada ou vetada.
- Uma solicitação aprovada é executada.

Se o solicitante estiver no mesmo grupo de aprovação para a operação, ele receberá um e-mail quando a solicitação for aprovada.

> Um solicitante não pode aprovar suas próprias solicitações, mesmo que esteja no grupo de aprovação (embora possa receber notificações por e-mail para suas próprias solicitações). Os solicitantes que não estão em grupos de aprovação (ou seja, que não são administradores MAV) não recebem notificações por e-mail.

Como funciona a execução da operação protegida

Se a execução for aprovada para uma operação protegida, o usuário solicitante continuará com a operação

quando solicitado. Se a operação for vetada, o usuário solicitante deverá excluir a solicitação antes de prosseguir.

As regras MAV são avaliadas após as permissões RBAC. Como resultado, um usuário sem permissões RBAC suficientes para execução da operação não pode iniciar o processo de solicitação MAV.

Gerenciar grupos de aprovação de administrador

Antes de ativar a verificação multi-admin (MAV), você deve criar um grupo de aprovação de administrador contendo um ou mais administradores para receber autoridade de aprovação ou veto. Depois de ativar a verificação multi-admin, quaisquer modificações na associação ao grupo de aprovação requerem a aprovação de um dos administradores qualificados existentes.

Sobre esta tarefa

Você pode adicionar administradores existentes a um grupo MAV ou criar novos administradores.

A funcionalidade MAV homenageia as configurações de controle de acesso baseado em função (RBAC) existentes. Os potenciais administradores do MAV devem ter privilégios suficientes para executar operações protegidas antes de serem adicionados aos grupos de administradores do MAV. "Saiba mais sobre o RBAC."

Você pode configurar o MAV para alertar os administradores do MAV de que as solicitações de aprovação estão pendentes. Para fazer isso, você deve configurar notificações por e-mail - em particular, os `Mail From` parâmetros e `Mail Server` - ou você pode limpar esses parâmetros para desativar a notificação. Sem alertas de e-mail, os administradores do MAV devem verificar a fila de aprovação manualmente.

Procedimento do System Manager

Se pretender criar um grupo de aprovação MAV pela primeira vez, consulte o procedimento do Gestor do sistema para "ative a verificação de vários administradores."

Para modificar um grupo de aprovação existente ou criar um grupo de aprovação adicional:

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."

2. Criar ou modificar o grupo de aprovação MAV:
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **aprovação Multi-Admin** na seção **Segurança**. (Você verá o ⚙ ícone se o MAV ainda não estiver configurado.)
      - Nome: Introduza um nome de grupo.
      - Aprovadores: Selecione aprovadores de uma lista de usuários.
      - Endereço de e-mail: Insira o(s) endereço(s) de e-mail.
      - Grupo padrão: Selecione um grupo.

A aprovação MAV é necessária para editar uma configuração existente assim que o MAV estiver ativado.

Procedimento CLI

1. Verifique se os valores foram definidos para `Mail From` os parâmetros e. `Mail Server` Introduza:

   `event config show`

   O visor deve ser semelhante ao seguinte:

   ```
   cluster01::> event config show
                              Mail From:  admin@localhost
                            Mail Server:  localhost
                              Proxy URL:  -
                             Proxy User:  -
    Publish/Subscribe Messaging Enabled:  true
   ```

   Para configurar estes parâmetros, introduza:

   `event config modify -mail-from` *`email_address`* `-mail-server` *`server_name`*

2. Identifique os administradores para receber a verificação de vários administradores

Se você quiser…	Introduza este comando
Exibir administradores atuais	`security login show`
Modifique as credenciais dos administradores atuais	`security login modify <parameters>`
Crie novas contas de administrador	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

3. Crie o grupo de aprovação MAV:

   `security multi-admin-verify approval-group create [ -vserver` *`svm_name`*`] -name` *`group_name`* `-approvers` *`approver1`*`[,`*`approver2`*`…] [[-email` *`address1`*`], `*`address1`*`…]`

   - `-vserver` - Somente o administrador SVM é suportado nesta versão.
   - `-name` - O nome do grupo MAV, até 64 carateres.
   - `-approvers` - A lista de um ou mais aprovadores.
   - `-email` - Um ou mais endereços de e-mail que são notificados quando uma solicitação é criada, aprovada, vetada ou executada.

     Exemplo: o comando a seguir cria um grupo MAV com dois membros e endereços de e-mail associados.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Verificar a criação e a associação do grupo:

   `security multi-admin-verify approval-group show`

   Exemplo:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

Use esses comandos para modificar a configuração inicial do grupo MAV.

Nota: todos exigem aprovação do administrador do MAV antes da execução.

Se você quiser…	Introduza este comando
Modifique as caraterísticas do grupo ou modifique as informações de membros existentes	`security multi-admin-verify approval-group modify [`*parameters*`]`
Adicionar ou remover membros	`security multi-admin-verify approval-group replace [-vserver` *svm_name*`] -name` *group_name* `[-approvers-to-add` *approver1*`[,`*approver2*`…]][-approvers-to-remove` *approver1*`[,`*approver2*`…]]`
Eliminar um grupo	`security multi-admin-verify approval-group delete [-vserver` *svm_name*`] -name` *group_name*

Ative e desative a verificação de vários administradores

A verificação multi-admin (MAV) deve ser ativada explicitamente. Depois de ativar a verificação multi-admin, a aprovação por administradores em um grupo de aprovação MAV (administradores MAV) é necessária para excluí-la.

Sobre esta tarefa

Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

Se você precisar desabilitar a funcionalidade de verificação multiadministrador sem a aprovação do administrador do MAV, entre em Contato com o suporte da NetApp e mencione o seguinte artigo da base de dados de Conhecimento: "Como desativar a Verificação Multi-Admin se o administrador do MAV não estiver disponível".

Ao ativar o MAV, você pode especificar os seguintes parâmetros globalmente.

Grupos de aprovação

Uma lista de grupos de aprovação globais. É necessário pelo menos um grupo para ativar a funcionalidade MAV.

Se você estiver usando o MAV com o Autonomous ransomware Protection (ARP), defina um grupo de aprovação novo ou existente que seja responsável por aprovar a pausa ARP, desativar e limpar solicitações suspeitas.

Aprovadores necessários

O número de aprovadores necessários para executar uma operação protegida. O número padrão e mínimo é 1.

O número necessário de aprovadores deve ser menor que o número total de aprovadores exclusivos nos grupos de aprovação padrão.

Validade da aprovação (horas, minutos, segundos)

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Expiração da execução (horas, minutos, segundos)

O período durante o qual o administrador requerente deve concluir a operação::. O valor padrão é de uma hora (1h), o valor mínimo suportado é de um segundo (1s) e o valor máximo suportado é de 14 dias (14d).

Você também pode substituir qualquer um desses parâmetros para específico "regras de operação."

Procedimento do System Manager

1. Identifique os administradores para receber a verificação de vários administradores.
   a. Clique em **Cluster > Settings.**
   b. Clique → ao lado de **usuários e funções.**
   c. Clique + Add em **Users.**
   d. Modifique a lista conforme necessário.

      Para obter mais informações, consulte "Controle o acesso do administrador."

2. Ative a verificação de vários administradores criando pelo menos um grupo de aprovação e adicionando pelo menos uma regra.
   a. Clique em **Cluster > Settings.**
   b. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
   c. Clique + Add para adicionar pelo menos um grupo de aprovação.

- Name (Nome) – Introduza o nome de um grupo.
- Aprovadores – Selecione aprovadores de uma lista de usuários.
- Endereço de e-mail – Digite o(s) endereço(s) de e-mail.
- Grupo padrão – Selecione um grupo.

d. Adicione pelo menos uma regra.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais; deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação
e. Clique em **Configurações avançadas** para exibir ou modificar os padrões.
   - Número necessário de aprovadores (padrão: 1)
   - Expiração da solicitação de execução (padrão: 1 hora)
   - Expiração do pedido de aprovação (predefinição: 1hour)
   - Servidor de correio*
   - A partir do endereço de e-mail*

     *Estes atualizam as definições de e-mail geridas em "Gestão de notificações". Você será solicitado a configurá-los se eles ainda não tiverem sido configurados.
f. Clique em **Enable** para concluir a configuração inicial do MAV.

Após a configuração inicial, o status atual do MAV é exibido no mosaico **aprovação Multi-Admin**.

- Estado (ativado ou não)
- Operações ativas para as quais são necessárias aprovações
- Número de solicitações abertas no estado pendente

Você pode exibir uma configuração existente clicando →em . A aprovação MAV é necessária para editar uma configuração existente.

Para desativar a verificação de vários administradores:

1. Clique em **Cluster > Settings.**
2. Clique ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. Clique no botão de alternância ativado.

   A aprovação MAV é necessária para concluir esta operação.

Procedimento CLI

Antes de ativar a funcionalidade MAV na CLI, pelo menos um "Grupo de administradores do MAV"deve ter sido criado.

Se você quiser…	Introduza este comando

Ativar a funcionalidade MAV	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	Exemplo : o comando a seguir habilita o MAV com 1 grupo de aprovação, 2 aprovadores necessários e períodos de expiração padrão.
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	Conclua a configuração inicial adicionando pelo menos uma "regra de operação."

Modificar uma configuração MAV (requer aprovação MAV)	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

Verifique a funcionalidade MAV	`security multi-admin-verify show`
	
	Exemplo:
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

Desativar a funcionalidade MAV (requer aprovação MAV)	`security multi-admin-verify modify -enabled false`

Gerenciar regras de operação protegidas

Você cria regras de verificação multi-admin (MAV) para designar operações que exigem aprovação. Sempre que uma operação é iniciada, operações protegidas são intercetadas e uma solicitação de aprovação é gerada.

As regras podem ser criadas antes de ativar o MAV por qualquer administrador com recursos RBAC apropriados, mas uma vez que o MAV está habilitado, qualquer modificação no conjunto de regras requer aprovação MAV.

Apenas uma regra MAV pode ser criada por operação; por exemplo, você não pode fazer várias `volume-snapshot-delete` regras. Quaisquer restrições de regra desejadas devem estar contidas em uma regra.

Você pode criar regras para proteger "estes comandos". Você pode proteger cada comando começando com a versão ONTAP na qual a capacidade de proteção para o comando ficou disponível pela primeira vez.

As regras para os comandos padrão do sistema MAV, o `security multi-admin-verify` "comandos", não podem ser alteradas.

Além das operações definidas pelo sistema, os seguintes comandos são protegidos por padrão quando a verificação multi-admin está ativada, mas você pode modificar as regras para remover a proteção desses comandos.

- `security login password`
- `security login unlock`
- `set`

Restrições de regra

Ao criar uma regra, você pode especificar opcionalmente a `-query` opção para limitar a solicitação a um subconjunto da funcionalidade de comando. A `-query` opção também pode ser usada para limitar elementos de configuração, como SVM, volume e nomes de Snapshot.

Por exemplo, no `volume snapshot delete` comando, `-query` pode ser definido como `-snapshot !hourly*,!daily*,!weekly*`, o que significa que instantâneos de volume pré-fixados com atributos de hora em hora, dia ou semanal são excluídos das proteções MAV.

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- --------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

Quaisquer elementos de configuração excluídos não seriam protegidos pelo MAV, e qualquer administrador poderia excluí-los ou renomeá-los.

Por padrão, as regras especificam que um comando correspondente `security multi-admin-verify request create` *"protected_operation"* é gerado automaticamente quando uma operação protegida

é inserida. Você pode modificar esse padrão para exigir que o `request create` comando seja inserido separadamente.

Por padrão, as regras herdam as seguintes configurações globais de MAV, embora você possa especificar exceções específicas de regras:

- Número necessário de Aprovadores
- Grupos de aprovação
- Período de validade da aprovação
- Período de expiração da execução

Procedimento do System Manager

Se pretender adicionar uma regra de operação protegida pela primeira vez, consulte o procedimento do Gestor de sistema a. "ative a verificação de vários administradores."

Para modificar o conjunto de regras existente:

1. Selecione **Cluster > Settings**.
2. Selecione ⚙ ao lado de **aprovação Multi-Admin** na seção **Segurança**.
3. + Add Selecione para adicionar pelo menos uma regra; você também pode modificar ou excluir regras existentes.
   - Operação – Selecione um comando suportado na lista.
   - Consulta – Insira quaisquer opções e valores de comando desejados.
   - Parâmetros opcionais – deixe em branco para aplicar configurações globais ou atribua um valor diferente para regras específicas para substituir as configurações globais.
     - Número necessário de aprovadores
     - Grupos de aprovação

Procedimento CLI

ⓘ Todos `security multi-admin-verify rule` os comandos requerem aprovação do administrador MAV antes da execução, exceto `security multi-admin-verify rule show`.

Se você quiser…	Introduza este comando
Crie uma regra	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

Se você quiser…	Introduza este comando

Modifique as credenciais dos administradores atuais	`security login modify <parameters>`
	
	Exemplo: A regra a seguir requer aprovação para excluir o volume raiz.
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

Modificar uma regra	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
Excluir uma regra	`security multi-admin-verify rule delete -operation "protected_operation"`
Mostrar regras	`security multi-admin-verify rule show`

Para obter detalhes da sintaxe do comando, consulte as `security multi-admin-verify rule` páginas man.

Solicitar a execução de operações protegidas

Quando você inicia uma operação ou comando protegidos em um cluster habilitado para verificação multi-admin (MAV), o ONTAP interceta automaticamente a operação e solicita a geração de uma solicitação, que deve ser aprovada por um ou mais administradores em um grupo de aprovação MAV (administradores MAV). Alternativamente, você pode criar uma solicitação MAV sem a caixa de diálogo.

Se aprovado, você deve responder à consulta para concluir a operação dentro do período de expiração da solicitação. Se vetado, ou se a solicitação ou os períodos de expiração forem excedidos, você deverá excluir a solicitação e reenviar.

A funcionalidade MAV homenageia as configurações RBAC existentes. Ou seja, sua função de administrador deve ter privilégio suficiente para executar uma operação protegida sem considerar as configurações de MAV. "Saiba mais sobre o RBAC".

Se você for um administrador do MAV, suas solicitações para executar operações protegidas também devem ser aprovadas por um administrador do MAV.

Procedimento do System Manager

Quando um usuário clica em um item de menu para iniciar uma operação e a operação é protegida, uma solicitação de aprovação é gerada e o usuário recebe uma notificação semelhante à seguinte:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

A janela **pedidos Multi-Admin** está disponível quando o MAV está ativado, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não). Para cada solicitação pendente, os seguintes campos são exibidos:

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Quando a solicitação for aprovada, o usuário solicitante poderá tentar novamente a operação dentro do período de expiração.

Se o utilizador voltar a tentar a operação sem aprovação, é apresentada uma notificação semelhante à seguinte:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

Procedimento CLI

1. Introduzir diretamente a operação protegida ou através do comando pedido MAV.

   Exemplos – para excluir um volume, digite um dos seguintes comandos:

   - `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create “volume delete”`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. Verifique o status da solicitação e responda ao aviso MAV.
   a. Se a solicitação for aprovada, responda à mensagem CLI para concluir a operação.

      Exemplo:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. Se a solicitação for vetada ou se o período de expiração tiver passado, exclua a solicitação e envie novamente ou entre em Contato com o administrador do MAV.

Exemplo:

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gerenciar solicitações de operação protegidas

Quando os administradores de um grupo de aprovação MAV (administradores MAV) são notificados de uma solicitação de execução de operação pendente, eles devem responder com uma mensagem de aprovação ou veto dentro de um período de tempo fixo (expiração da aprovação). Se um número suficiente de aprovações não for recebido, o solicitante deve excluir a solicitação e fazer outra.

Sobre esta tarefa

As solicitações de aprovação são identificadas com números de índice, que são incluídos em mensagens de e-mail e exibições da fila de solicitações.

As seguintes informações da fila de pedidos podem ser exibidas:

Operação
A operação protegida para a qual a solicitação é criada.

Consulta
O objeto (ou objetos) sobre o qual o usuário deseja aplicar a operação.

Estado

O estado atual da solicitação; pendente, aprovado, rejeitado, expirado, executado. Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

Aprovadores necessários

O número de administradores MAV que são necessários para aprovar a solicitação. Um usuário pode definir o parâmetro de aprovadores necessários para a regra de operação. Se um usuário não definir os aprovadores necessários para a regra, os aprovadores necessários da configuração global serão aplicados.

Aprovadores pendentes

O número de administradores MAV que ainda são obrigados a aprovar a solicitação para que a solicitação seja marcada como aprovada.

Validade da aprovação

O período durante o qual um administrador do MAV deve responder a uma solicitação de aprovação. Qualquer utilizador autorizado pode definir a validade da aprovação para uma regra de operação. Se a expiração da aprovação não for definida para a regra, então a expiração da aprovação do ajuste global é aplicada.

Expiração da execução

O período durante o qual o administrador requerente deve concluir a operação. Qualquer usuário autorizado pode definir a expiração de execução para uma regra de operação. Se a execução-expiração não estiver definida para a regra, então a execução-expiração da configuração global será aplicada.

Usuários aprovados

Os administradores do MAV que aprovaram a solicitação.

Vetado pelo utilizador

Os administradores do MAV que vetaram a solicitação.

VM de storage (vserver)

O SVM com o qual a solicitação está associada. Somente o SVM admin é compatível nesta versão.

Utilizador solicitado

O nome de usuário do usuário que criou a solicitação.

Hora criada

A hora em que a solicitação é criada.

Hora aprovada

A hora em que o estado da solicitação foi alterado para aprovado.

Comentário

Quaisquer comentários associados à solicitação.

Usuários permitidos

A lista de utilizadores autorizados a realizar a operação protegida para a qual a solicitação foi aprovada. Se `users-permitted` estiver vazio, qualquer usuário com permissões apropriadas pode executar a operação.

Todas as solicitações expiradas ou executadas são excluídas quando um limite de 1000 solicitações é atingido

ou quando o tempo expirado é maior que 8hrs para solicitações expiradas. As solicitações vetadas são excluídas depois que forem marcadas como expiradas.

Procedimento do System Manager

Os administradores do MAV recebem mensagens de e-mail com detalhes da solicitação de aprovação, período de expiração da solicitação e um link para aprovar ou rejeitar a solicitação. Eles podem acessar uma caixa de diálogo de aprovação clicando no link no e-mail ou navegar para **Eventos & trabalhos>solicitações** no System Manager.

A janela **Requests** está disponível quando a verificação multi-admin está ativada, mostrando solicitações pendentes com base no ID de login do usuário e na função MAV (aprovador ou não).

- Operação
- Índice (número)
- Estado (pendente, aprovado, rejeitado, executado ou expirado)

  Se uma solicitação for rejeitada por um aprovador, nenhuma outra ação será possível.

- Consulta (quaisquer parâmetros ou valores para a operação solicitada)
- Utilizador a solicitar
- A solicitação expira em
- (Número de) Aprovadores pendentes
- (Número de) potenciais Aprovadores

Os administradores do MAV têm controles adicionais nesta janela; eles podem aprovar, rejeitar ou excluir operações individuais ou grupos selecionados de operações. No entanto, se o administrador MAV for o Usuário solicitante, ele não poderá aprovar, rejeitar ou excluir seus próprios pedidos.

Procedimento CLI

1. Quando notificado de solicitações pendentes por e-mail, observe o número de índice e o período de expiração da aprovação da solicitação. O número do índice também pode ser exibido usando as opções **show** ou **show-pending** mencionadas abaixo.
2. Aprovar ou vetar o pedido.

Se você quiser…	Introduza este comando
Aprovar uma solicitação	`security multi-admin-verify request approve` *nn*
Veto um pedido	`security multi-admin-verify request veto` *nn*
Mostrar todas as solicitações, solicitações pendentes ou uma única solicitação	`security multi-admin-verify request { show

Se você quiser…	Introduza este comando
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  Você pode mostrar todas as solicitações na fila ou apenas solicitações pendentes. Se introduzir o número do índice, apenas são apresentadas informações para esse número. Você pode exibir informações sobre campos específicos (usando o `-fields` parâmetro) ou sobre todos os campos (usando o `-instance` parâmetro).
Eliminar um pedido	`security multi-admin-verify request delete` *nn*

Exemplo:

A sequência a seguir aprova uma solicitação após o administrador do MAV receber o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Exemplo:

A sequência a seguir veta uma solicitação depois que o administrador do MAV recebeu o e-mail da solicitação com o índice número 3, que já tem uma aprovação.

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

Gerenciar autorização dinâmica

Descrição geral da autorização dinâmica

A partir do ONTAP 9.15,1, os administradores podem configurar e habilitar a autorização dinâmica para aumentar a segurança do acesso remoto ao ONTAP, além de mitigar possíveis danos que podem ser causados por um ator mal-intencionado. Com o ONTAP 9.15,1, a autorização dinâmica fornece uma estrutura inicial para atribuir uma pontuação de segurança aos usuários e, se sua atividade parecer suspeita, desafiando-os com verificações de autorização adicionais ou negando uma operação completamente. Os administradores podem criar regras, atribuir pontuações de confiança e restringir comandos para determinar quando determinada atividade é permitida ou negada para um usuário. Os administradores podem habilitar a autorização dinâmica em todo o

cluster ou para VMs de armazenamento individuais.

Como funciona a autorização dinâmica

A autorização dinâmica utiliza um sistema de pontuação de confiança para atribuir aos utilizadores um nível de confiança diferente, dependendo das políticas de autorização. Com base no nível de confiança do usuário, uma atividade que ele executa pode ser permitida ou negada, ou o usuário pode ser solicitado para autenticação adicional.

"Personalizar autorização dinâmica"Consulte para saber mais sobre como configurar pesos de pontuação de critérios e outros atributos de autorização dinâmica.

Dispositivos confiáveis

Quando a autorização dinâmica está em uso, a definição de um dispositivo confiável é um dispositivo usado por um usuário para fazer login no ONTAP usando autenticação de chave pública como um dos métodos de autenticação. O dispositivo é confiável porque somente esse usuário possui a chave privada correspondente.

Exemplo de autorização dinâmica

Veja o exemplo de três usuários diferentes tentando excluir um volume. Quando eles tentam executar a operação, a classificação de risco para cada usuário é examinada:

- O primeiro usuário faz login de um dispositivo confiável com poucas falhas de autenticação anteriores, o que torna sua classificação de risco baixa; a operação é permitida sem autenticação adicional.
- O segundo usuário faz login em um dispositivo confiável com uma porcentagem moderada de falhas de autenticação anteriores, o que torna a classificação de risco moderada; ela é solicitada a autenticação adicional antes que a operação seja permitida.
- O terceiro usuário faz logon de um dispositivo não confiável com uma alta porcentagem de falhas de autenticação anteriores, o que torna a classificação de risco alta; a operação não é permitida.

O que vem a seguir

- "Ativar ou desativar a autorização dinâmica"
- "Personalizar autorização dinâmica"

Ative ou desative a autorização dinâmica no ONTAP

A partir do ONTAP 9.15,1, os administradores podem configurar e ativar a autorização dinâmica no `visibility` modo para testar a configuração, ou no `enforced` modo para ativar a configuração para os usuários CLI que se conetam por SSH. Se você não precisar mais de autorização dinâmica, você pode desativá-la. Quando você desativa a autorização dinâmica, as configurações permanecem disponíveis e você pode usá-las mais tarde se decidir reativá-las.

Saiba mais sobre `security dynamic-authorization modify` o "Referência do comando ONTAP"na .

Ativar autorização dinâmica para testes

Você pode ativar a autorização dinâmica no modo de visibilidade, que permite testar o recurso e garantir que os usuários não serão bloqueados acidentalmente. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas, mas não aplicada. No entanto, qualquer atividade que tenha sido negada ou

sujeita a desafios de autenticação adicionais é registrada. Como prática recomendada, você deve testar as configurações pretendidas neste modo antes de aplicá-las.

> Pode seguir este passo para ativar a autorização dinâmica pela primeira vez, mesmo que ainda não tenha configurado quaisquer outras definições de autorização dinâmica. "Personalizar autorização dinâmica"Consulte para obter instruções sobre como configurar outras definições de autorização dinâmica para personalizá-las para o seu ambiente.

Passos

1. Ative a autorização dinâmica no modo de visibilidade configurando as configurações globais e alterando o estado da função para `visibility`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

Ativar autorização dinâmica no modo imposto

Pode ativar a autorização dinâmica no modo imposto. Normalmente, você usa este modo depois de concluir o teste com o modo de visibilidade. Neste modo, a pontuação de confiança é verificada em todas as atividades restritas e as restrições de atividade são aplicadas se as condições de restrição forem cumpridas. O intervalo de supressão também é aplicado, impedindo desafios de autenticação adicionais dentro do intervalo especificado.

> Esta etapa pressupõe que você configurou e ativou previamente a autorização dinâmica no `visibility` modo, o que é altamente recomendado.

Passos

1. Ative a autorização dinâmica no `enforced` modo alterando seu estado para `enforced`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

Desativar autorização dinâmica

Você pode desativar a autorização dinâmica se não precisar mais da segurança de autenticação adicionada.

Passos

1. Desative a autorização dinâmica alterando seu estado para `disabled`. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Parâmetros em negrito são necessários:

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Verifique o resultado usando o `show` comando para exibir a configuração global:

```
security dynamic-authorization show
```

O que vem a seguir

(Opcional) dependendo do seu ambiente, "Personalizar autorização dinâmica"consulte para configurar outras definições de autorização dinâmica.

Personalizar autorização dinâmica no ONTAP

Como administrador, você pode personalizar diferentes aspetos de sua configuração de autorização dinâmica para aumentar a segurança das conexões SSH do administrador remoto ao cluster do ONTAP.

Pode personalizar as seguintes definições de autorização dinâmica, dependendo das suas necessidades de segurança:

- Configure as definições globais de autorização dinâmica
- Configurar componentes de pontuação de confiança de autorização dinâmica
- Configure um provedor de pontuação de confiança personalizado
- Configurar comandos restritos
- Configurar grupos de autorização dinâmicos

Configure as definições globais de autorização dinâmica

Você pode configurar configurações globais para autorização dinâmica, incluindo a VM de armazenamento para proteger, o intervalo de supressão para desafios de autenticação e as configurações de pontuação de

confiança.

Saiba mais sobre `security login domain-tunnel create` o "Referência do comando ONTAP"na .

Passos

1. Configurar definições globais para autorização dinâmica. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Atualize os valores entre parêntesis> para corresponder ao seu ambiente:

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Veja a configuração resultante:

```
security dynamic-authorization show
```

Configurar comandos restritos

Quando você ativa a autorização dinâmica, o recurso inclui um conjunto padrão de comandos restritos. Você pode modificar esta lista para atender às suas necessidades. Consulte a "Documentação de verificação multi-admin (MAV)"para obter informações sobre a lista padrão de comandos restritos.

Adicionar um comando restrito

Você pode adicionar um comando à lista de comandos restritos com autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-rule-create.html[`security dynamic-authorization rule create` em referência de comando ONTAP.

Passos

1. Adicione o comando. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Veja a lista resultante de comandos restritos:

```
security dynamic-authorization rule show
```

Remover um comando restrito

Você pode remover um comando da lista de comandos que são restritos com autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-rule-delete.html[`security dynamic-authorization rule delete` em referência de comando ONTAP.

Passos

1. Remova o comando. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Veja a lista resultante de comandos restritos:

```
security dynamic-authorization rule show
```

Configurar grupos de autorização dinâmicos

Por padrão, a autorização dinâmica se aplica a todos os usuários e grupos assim que você a ativar. No entanto, você pode criar grupos usando o `security dynamic-authorization group create` comando, para que a autorização dinâmica se aplique apenas a esses usuários específicos.

Adicione um grupo de autorização dinâmica

Pode adicionar um grupo de autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-group-create.html[`security dynamic-authorization group create` em referência de comando ONTAP.

Passos

1. Crie o grupo. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. Veja os grupos de autorização dinâmica resultantes:

```
security dynamic-authorization group show
```

Remova um grupo de autorização dinâmica

Pode remover um grupo de autorização dinâmica.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-group-delete.html[`security dynamic-authorization group delete` em referência de comando ONTAP.

Passos

1. Exclua o grupo. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Veja os grupos de autorização dinâmica resultantes:

```
security dynamic-authorization group show
```

Configurar componentes de pontuação de confiança de autorização dinâmica

Pode configurar o peso máximo da pontuação para alterar a prioridade dos critérios de pontuação ou remover determinados critérios da pontuação de risco.

Como uma prática recomendada, você deve deixar os valores de peso de pontuação padrão no lugar, e apenas ajustá-los se necessário.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-modify.html[`security dynamic-authorization trust-score-component modify` em referência de comando ONTAP.

A seguir estão os componentes que você pode modificar, juntamente com sua pontuação padrão e pesos percentuais:

Critérios	Nome do componente	Peso bruto padrão da pontuação	Peso percentual padrão
Dispositivo confiável	`trusted-device`	20	50
Histórico de autenticação de login do usuário	`authentication-history`	20	50

Passos

1. Modificar componentes da pontuação de confiança. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Veja as configurações de componente de pontuação de confiança resultantes:

```
security dynamic-authorization trust-score-component show
```

Redefina a pontuação de confiança de um utilizador

Se um usuário tiver acesso negado devido a políticas do sistema e puder provar sua identidade, o administrador poderá redefinir a pontuação de confiança do usuário.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-user-trust-score-reset.html[`security dynamic-authorization user-trust-score reset` em referência de comando ONTAP.

Passos

1. Adicione o comando. Consulte a Configurar componentes de pontuação de confiança de autorização dinâmica para obter uma lista de componentes de pontuação de confiança que pode repor. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Exiba sua pontuação de confiança

Um usuário pode exibir sua própria pontuação de confiança para uma sessão de login.

Passos

1. Exiba sua pontuação de confiança:

```
security login whoami
```

Você deve ver saída semelhante ao seguinte:

```
User: admin
Role: admin
Trust Score: 50
```

Configure um provedor de pontuação de confiança personalizado

Se já receber métodos de pontuação de um fornecedor externo de pontuação de confiança, pode adicionar o fornecedor personalizado à configuração de autorização dinâmica.

Antes de começar

- O provedor de pontuação de confiança personalizado deve retornar uma resposta JSON. Os seguintes requisitos de sintaxe devem ser atendidos:
  - O campo que retorna a pontuação de confiança deve ser um campo escalar e não um elemento de um array.
  - O campo que retorna a pontuação de confiança pode ser um campo aninhado, `trust_score.value` como .
  - Deve haver um campo dentro da resposta JSON que retorna uma pontuação de confiança numérica. Se isso não estiver disponível nativamente, você pode escrever um script wrapper para retornar esse valor.
- O valor fornecido pode ser uma pontuação de confiança ou uma pontuação de risco. A diferença é que a pontuação de confiança está em ordem crescente com uma pontuação mais alta denotando um nível de confiança mais alto, enquanto a pontuação de risco está em ordem decrescente. Por exemplo, uma pontuação de confiança de 90 para uma faixa de pontuação de 0 a 100 indica que a pontuação é muito confiável e provavelmente resultará em uma "permissão" sem desafio adicional, enquanto uma pontuação de risco de 90 para uma faixa de pontuação de 0 a 100 indica alto risco e provavelmente resultará em uma "negação" sem um desafio adicional.
- O provedor de pontuação de confiança personalizado deve estar acessível por meio da API REST do ONTAP.
- O provedor de pontuação de confiança personalizado deve ser configurável usando um dos parâmetros suportados. Os provedores de pontuação de confiança personalizados que exigem configuração que não esteja na lista de parâmetros suportados não são suportados.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-create.html[`security dynamic-authorization trust-score-component create` em referência de comando ONTAP.

Passos

1. Adicione um provedor de pontuação de confiança personalizado. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Veja as configurações do provedor de pontuação de confiança resultantes:

```
security dynamic-authorization trust-score-component show
```

Configurar etiquetas de fornecedor de pontuação de confiança personalizadas

Você pode se comunicar com provedores externos de pontuação de confiança usando tags. Isso permite que você envie informações no URL para o provedor de pontuação de confiança sem expor informações confidenciais.

Saiba mais sobre o comando link:https://docs.NetApp.com/US-en/ONTAP-cli/security-dynamic-authorization-trust-score-component-create.html[`security dynamic-authorization trust-score-component create` em referência de comando ONTAP.

Passos

1. Ativar etiquetas de fornecedor de pontuação de confiança. Atualize os valores entre parêntesis> para corresponder ao seu ambiente. Se você não usar o `-vserver` parâmetro, o comando será executado no nível do cluster. Parâmetros em negrito são necessários:

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

   Por exemplo:

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

Autenticação e autorização usando OAuth 2,0

Visão geral da implementação do ONTAP OAuth 2,0

A partir do ONTAP 9.14, você tem a opção de controlar o acesso aos clusters do ONTAP usando a estrutura autorização aberta (OAuth 2,0). Você pode configurar esse recurso usando qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI do ONTAP, o Gerenciador do sistema e a API REST. No entanto, as decisões de autorização e controle de acesso do OAuth 2,0 só podem ser aplicadas quando um cliente acessa o ONTAP usando a API REST.

O suporte do OAuth 2,0 foi introduzido pela primeira vez com o ONTAP 9.14,0 e, portanto, sua disponibilidade depende da versão do ONTAP que você está usando. Consulte "Notas de versão do ONTAP" para obter mais informações.

Caraterísticas e benefícios

Os principais recursos e benefícios do uso do OAuth 2,0 com ONTAP são descritos abaixo.

Suporte para o padrão OAuth 2,0

OAuth 2,0 é o quadro de autorização padrão da indústria. Ele é usado para restringir e controlar o acesso a recursos protegidos usando tokens de acesso assinados. Existem vários benefícios para usar o OAuth 2,0:

- Muitas opções para a configuração de autorização
- Nunca revele as credenciais do cliente, incluindo senhas
- Os tokens podem ser definidos para expirar com base na sua configuração
- Ideal para uso com APIS REST

Testado com servidores de autorização populares

A implementação do ONTAP OAuth 2,0 foi testada com vários servidores ou serviços populares baseados na versão do ONTAP da seguinte forma:

- ONTAP 9.16,1 (suporte para UUUID do grupo para nomear o mapeamento e funções externas):
  - ID do Microsoft Entra
- ONTAP 9.14,1 (suporte para recursos padrão OAuth 2,0)
  - Auth0
  - Serviço de Federação do ative Directory (ADFS)
  - Capa da chave

"Servidores de autorização e tokens de acesso"Consulte para obter mais detalhes sobre os recursos e

recursos disponíveis em cada versão do ONTAP.

Suporte para vários servidores de autorização simultâneos

Você pode definir até oito servidores de autorização para um único cluster ONTAP. Isso oferece a flexibilidade para atender às necessidades de seu ambiente de segurança diversificado.

Integração com as funções REST

As decisões de autorização do ONTAP baseiam-se, em última análise, nas funções REST atribuídas a usuários ou grupos. Essas funções são realizadas no token de acesso como escopos autônomos ou baseadas em definições locais do ONTAP junto com grupos do ative Directory ou LDAP.

Opção para usar tokens de acesso com restrição de remetente

Você pode configurar o ONTAP e os servidores de autorização para usar a segurança de camada de transporte mútuo (MTLS), o que fortalece a autenticação do cliente. Ele garante que os tokens de acesso OAuth 2,0 são usados apenas pelos clientes para os quais foram emitidos originalmente. Esse recurso suporta e se alinha com várias recomendações de segurança populares, incluindo aquelas estabelecidas pela FAPI e MITER.

Implementação e configuração

Em um alto nível, há vários aspetos de uma implementação e configuração do OAuth 2,0 que você deve considerar ao começar.

OAuth 2,0 entidades dentro do ONTAP

A estrutura de autorização do OAuth 2,0 define várias entidades que podem ser mapeadas para elementos reais ou virtuais em seu data center ou rede. As entidades OAuth 2,0 e sua adaptação ao ONTAP são apresentadas na tabela abaixo.

Entidade OAuth 2,0	Descrição
Recurso	Os pontos de extremidade da API REST que fornecem acesso aos recursos do ONTAP por meio de comandos internos do ONTAP.
Proprietário do recurso	O usuário do cluster do ONTAP que criou o recurso protegido ou o possui por padrão.
Servidor de recursos	O host dos recursos protegidos que é o cluster do ONTAP.
Cliente	Um aplicativo solicitando acesso a um endpoint de API REST em nome ou com permissão do proprietário do recurso.
Servidor de autorização	Normalmente, um servidor dedicado responsável pela emissão de tokens de acesso e pela aplicação da política administrativa.

Configuração do Core ONTAP

Você precisa configurar o cluster ONTAP para ativar e usar o OAuth 2,0. Isso inclui estabelecer uma conexão com o servidor de autorização e definir a configuração de autorização ONTAP necessária. Você pode executar essa configuração usando qualquer uma das interfaces administrativas, incluindo:

- Interface de linha de comando ONTAP
- System Manager
- API REST do ONTAP

Ambiente e serviços de apoio

Além das definições do ONTAP, você também precisa configurar os servidores de autorização. Se você estiver usando o mapeamento grupo para função, também será necessário configurar os grupos do ative Directory ou o equivalente LDAP.

Clientes ONTAP suportados

A partir do ONTAP 9.14, um cliente API REST pode acessar o ONTAP usando o OAuth 2,0. Antes de emitir uma chamada de API REST, você precisa obter um token de acesso do servidor de autorização. Em seguida, o cliente passa esse token para o cluster ONTAP como um token *portador* usando o cabeçalho de solicitação de autorização HTTP. Dependendo do nível de segurança necessário, você também pode criar e instalar um certificado no cliente para usar tokens com restrição de remetente baseados no MTLS.

Terminologia selecionada

À medida que você começa a explorar uma implantação do OAuth 2,0 com o ONTAP, é útil se familiarizar com alguma terminologia. "Recursos adicionais"Consulte para obter links para mais informações sobre o OAuth 2,0.

Token de acesso

Um token emitido por um servidor de autorização e usado por um aplicativo cliente OAuth 2,0 para fazer solicitações para acessar os recursos protegidos.

JSON Web Token

O padrão usado para formatar os tokens de acesso. JSON é usado para representar as reivindicações OAuth 2,0 em um formato compacto com as reivindicações organizadas em três seções principais.

Token de acesso restrito ao remetente

Um recurso opcional baseado no protocolo MTLS (Mutual Transport Layer Security). Ao usar uma reivindicação de confirmação adicional no token, isso garante que o token de acesso seja usado apenas pelo cliente para o qual foi emitido originalmente.

Conjunto de chaves Web JSON

Um JWKS é uma coleção de chaves públicas usadas pelo ONTAP para verificar os tokens JWT apresentados pelos clientes. Os conjuntos de chaves estão normalmente disponíveis no servidor de autorização através de um URI dedicado.

Âmbito de aplicação

Os escopos fornecem uma maneira de limitar ou controlar o acesso de um aplicativo a recursos protegidos, como a API REST do ONTAP. Eles são representados como strings no token de acesso.

Função REST do ONTAP

As funções REST foram introduzidas com o ONTAP 9.6 e são uma parte essencial da estrutura RBAC do ONTAP. Essas funções são diferentes das funções tradicionais anteriores que ainda são suportadas pelo ONTAP. A implementação do OAuth 2,0 no ONTAP suporta apenas funções REST.

Cabeçalho de autorização HTTP

Um cabeçalho incluído na solicitação HTTP para identificar o cliente e as permissões associadas como parte de fazer uma chamada de API REST. Existem vários tipos ou implementações disponíveis dependendo de como a autenticação e a autorização são executadas. Ao apresentar um token de acesso OAuth 2,0 ao ONTAP, o token é identificado como um *token de portador*.

Autenticação básica HTTP

Uma técnica de autenticação HTTP inicial ainda suportada pelo ONTAP. As credenciais de texto simples (nome de usuário e senha) são concatenadas com dois pontos e codificadas em base64. A cadeia de

carateres é colocada no cabeçalho da solicitação de autorização e enviada para o servidor.

FAPI

Um grupo de trabalho da OpenID Foundation que fornece protocolos, esquemas de dados e recomendações de segurança para o setor financeiro. A API era originalmente conhecida como API Financial Grade.

MITRE

Uma empresa privada sem fins lucrativos que fornece orientação técnica e de segurança à força Aérea dos Estados Unidos e ao governo dos EUA.

Recursos adicionais

Vários recursos adicionais são fornecidos abaixo. Você deve revisar esses sites para obter mais informações sobre o OAuth 2,0 e os padrões relacionados.

Protocolos e padrões

- "RFC 6749: O OAuth 2,0 Authorization Framework"
- "RFC 7519: JSON Web tokens (JWT)"
- "RFC 7523: Perfil JSON Web Token (JWT) para permissões e autenticação de clientes OAuth 2,0"
- "RFC 7662: Introspeção de tokens OAuth 2,0"
- "RFC 7800: Chave de prova de posse para JWTs"
- "RFC 8705: Autenticação de cliente TLS mútuo OAuth 2,0 e tokens de acesso com certificado"

Organizações

- "Fundação OpenID"
- "Grupo de trabalho FAPI"
- "MITRE"
- "IANA - JWT"

Produtos e serviços

- "Auth0"
- "ID entra"
- "Visão geral da ADFS"
- "Capa da chave"

Ferramentas e utilitários adicionais

- "JWT por Auth0"
- "OpenSSL"

Documentação e recursos do NetApp

- "Documentação de automação do ONTAP"

Conceitos

Servidores de autorização e tokens de acesso

Os servidores de autorização executam várias funções importantes como um componente central dentro da estrutura de autorização do OAuth 2,0.

Servidores de autorização OAuth 2,0

Os servidores de autorização são os principais responsáveis pela criação e assinatura de tokens de acesso. Esses tokens contêm informações de identidade e autorização, permitindo que um aplicativo cliente acesse seletivamente recursos protegidos. Os servidores geralmente são isolados uns dos outros e podem ser implementados de várias maneiras diferentes, incluindo como um servidor dedicado autônomo ou como parte de um produto maior de gerenciamento de identidade e acesso.

> Terminologia diferente às vezes pode ser usada para um servidor de autorização, especialmente quando a funcionalidade OAuth 2,0 é empacotada dentro de um produto ou solução de gerenciamento de identidade e acesso maior. Por exemplo, o termo **provedor de identidade (IDP)** é frequentemente usado de forma intercambiável com **servidor de autorização**.

Administração

Além de emitir tokens de acesso, os servidores de autorização também fornecem serviços administrativos relacionados, normalmente através de uma interface de usuário da Web. Por exemplo, você pode definir e administrar:

- Autenticação de usuários e usuários
- Escopos
- Segregação administrativa através de inquilinos e reinos
- Aplicação da política
- Conexão com vários serviços externos
- Suporte para outros protocolos de identidade (como SAML)

O ONTAP é compatível com servidores de autorização compatíveis com o padrão OAuth 2,0.

Definindo para ONTAP

Você precisa definir um ou mais servidores de autorização para o ONTAP. O ONTAP se comunica com segurança com cada servidor para verificar tokens e executar outras tarefas relacionadas no suporte aos aplicativos cliente.

Os principais aspetos da configuração do ONTAP são apresentados abaixo. Consulte também "Cenários de implantação do OAuth 2,0"para obter mais informações.

Como e onde os tokens de acesso são validados

Existem duas opções para validar tokens de acesso.

- Validação local

  O ONTAP pode validar tokens de acesso localmente com base nas informações fornecidas pelo servidor de autorização que emitiu o token. As informações recuperadas do servidor de autorização são armazenadas em cache pelo ONTAP e atualizadas em intervalos regulares.

- Introspeção remota

  Você também pode usar introspeção remota para validar tokens no servidor de autorização. Introspeção é um protocolo que permite que partes autorizadas consultem um servidor de autorização sobre um token de acesso. Ele fornece ao ONTAP uma maneira de extrair determinados metadados de um token de acesso e validar o token. O ONTAP armazena em cache alguns dos dados por motivos de desempenho.

Localização da rede

O ONTAP pode estar atrás de um firewall. Nesse caso, você precisa identificar um proxy como parte da configuração.

Como os servidores de autorização são definidos

Você pode definir um servidor de autorização para o ONTAP usando qualquer uma das interfaces administrativas, incluindo a CLI, o Gerenciador de sistema ou a API REST. Por exemplo, com a CLI você usa o comando `security oauth2 client create`.

Número de servidores de autorização

Você pode definir até oito servidores de autorização para um único cluster ONTAP. O mesmo servidor de autorização pode ser definido mais de uma vez para o mesmo cluster do ONTAP desde que as reivindicações do emissor ou do emissor/público sejam únicas. Por exemplo, com KeyCloak, esse será sempre o caso ao usar reinos diferentes.

Recursos do OAuth 2,0 suportados no ONTAP

O suporte para OAuth 2,0 estava inicialmente disponível com o ONTAP 9.14,1 e continua sendo aprimorado com versões subsequentes. Os recursos do OAuth 2,0 suportados pelo ONTAP são descritos abaixo.

> Os recursos introduzidos com uma versão específica do ONTAP são levados para versões futuras.

ONTAP 9.16,1

O ONTAP 9.16,1 expande os recursos padrão do OAuth 2,0 para incluir extensões específicas do Entra ID para grupos nativos de ID do Entra. Isso envolve o uso de GUIDs no token de acesso em vez de nomes. Além disso, a versão adiciona suporte para mapeamento de funções externas para mapear as funções nativas do provedor de identidade para as funções do ONTAP usando o campo "funções" no token de acesso.

ONTAP 9.14,1

A partir do ONTAP 9.14,1, os servidores de autorização são suportados através dos seguintes recursos padrão do OAuth 2,0 para aplicativos que usam:

- OAuth 2,0 com os campos padrão, incluindo "iss", "AUD" e "exp", conforme descrito em "RFC6749: O Quadro de autorização OAuth 2,0" e "RFC 7519: JSON Web Token (JWT)". Isso também inclui suporte para identificar exclusivamente usuários através de campos no token de acesso, como "upn", "appid", "sub", "username" ou "Preferred_username".
- Extensões específicas do fornecedor ADFS para nomes de grupos com o campo "grupo".
- Extensões específicas do fornecedor do Azure para UUIDs de grupo com o campo "grupo".
- Extensões ONTAP para suporte de autorização usando funções independentes e nomeadas dentro do escopo do token de acesso OAuth 2,0. Isso inclui os campos "Escopo" e "scp", bem como os nomes de grupos dentro do escopo.

Usando tokens de acesso OAuth 2,0

Os tokens de acesso OAuth 2,0 emitidos pelos servidores de autorização são verificados pelo ONTAP e usados para tomar decisões de acesso baseadas em função para as solicitações de cliente de API REST.

Adquirir um token de acesso

Você precisa adquirir um token de acesso a partir de um servidor de autorização definido para o cluster ONTAP onde você usa a API REST. Para adquirir um token, você deve entrar em Contato diretamente com o servidor de autorização.

O ONTAP não emite tokens de acesso nem redireciona solicitações de clientes para os servidores de autorização.

A forma como você solicita um token depende de vários fatores, incluindo:

- Servidor de autorização e suas opções de configuração
- OAuth 2,0 tipo de concessão
- Ferramenta cliente ou software usada para emitir a solicitação

Tipos de concessão

Um *Grant* é um processo bem definido, incluindo um conjunto de fluxos de rede, usado para solicitar e receber um token de acesso OAuth 2,0. Vários tipos de concessão diferentes podem ser usados dependendo dos requisitos de cliente, ambiente e segurança. Uma lista dos tipos de concessão populares é apresentada na tabela abaixo.

Tipo de concessão	Descrição
Credenciais do cliente	Um tipo de concessão popular baseado no uso apenas de credenciais (como um ID e segredo compartilhado). Presume-se que o cliente tenha uma relação de confiança próxima com o proprietário do recurso.
Palavra-passe	O tipo de concessão de credenciais de senha do proprietário do recurso pode ser usado nos casos em que o proprietário do recurso tenha uma relação de confiança estabelecida com o cliente. Também pode ser útil ao migrar clientes HTTP legados para o OAuth 2,0.
Código de autorização	Este é um tipo de concessão ideal para clientes confidenciais e é baseado em um fluxo baseado em redirecionamento. Ele pode ser usado para obter um token de acesso e atualizar token.

Conteúdo do JWT

Um token de acesso OAuth 2,0 é formatado como JWT. O conteúdo é criado pelo servidor de autorização com base na sua configuração. No entanto, os tokens são opacos para as aplicações cliente. Um cliente não tem razão para inspecionar um token ou estar ciente do conteúdo.

Cada token de acesso JWT contém um conjunto de reivindicações. As reclamações descrevem as caraterísticas do emissor e a autorização com base nas definições administrativas do servidor de autorização. Algumas das reclamações registadas com a norma estão descritas na tabela abaixo. Todas as cordas são sensíveis a maiúsculas e minúsculas.

Pedido de reembolso	Palavra-chave	Descrição
Emissor	iss	Identifica o principal que emitiu o token. O processamento da reclamação é específico da aplicação.
Assunto	sub	O assunto ou usuário do token. O nome é definido para ser global ou localmente único.
Público-alvo	aud	Os destinatários para os quais o token se destina. Implementado como uma matriz de strings.
Expiração	exp	O tempo após o qual o token expira e deve ser rejeitado.

Consulte "RFC 7519: JSON Web tokens" para obter mais informações.

Autorização do cliente

Visão geral e opções para autorização de cliente ONTAP

A implementação do ONTAP OAuth 2,0 foi projetada para ser flexível e robusta, fornecendo os recursos necessários para proteger seu ambiente ONTAP. Existem várias opções de configuração mutuamente exclusivas disponíveis. As decisões de autorização são, em última análise, baseadas nas funções REST do ONTAP contidas ou derivadas dos tokens de acesso OAuth 2,0.

Você só pode usar "Funções REST do ONTAP" ao configurar a autorização para o OAuth 2,0. As funções tradicionais anteriores do ONTAP não são suportadas.

O ONTAP aplica a única opção de autorização mais adequada com base na sua configuração. "Como o ONTAP determina o acesso"Consulte para obter mais informações sobre como o ONTAP toma decisões de acesso ao cliente.

Escopos auto-contidos OAuth 2,0

Esses escopos contêm uma ou mais funções REST personalizadas, cada uma encapsulada em uma única cadeia no token de acesso. Eles são independentes das definições de função do ONTAP. Você precisa configurar as strings de escopo em seu servidor de autorização. Consulte "Escopos OAuth 2,0 independentes" para obter mais informações.

Funções REST do ONTAP local

Uma única função REST nomeada, seja builtin ou personalizado, pode ser usada. A sintaxe do escopo para uma função nomeada é **ONTAP-role-** com codificação URL-ONTAP-role-name>. Por exemplo, se a função ONTAP for `admin` a string Escopo será `ontap-role-admin`.

Usuários

O nome de usuário no token de acesso definido com acesso ao aplicativo "http" pode ser usado. Um usuário é testado na seguinte ordem com base no método de autenticação definido: Senha, domínio (ative Directory), nsswitch (LDAP).

Grupos

Os servidores de autorização podem ser configurados para usar grupos ONTAP para autorização. Se as definições locais do ONTAP forem examinadas, mas não for possível tomar nenhuma decisão de acesso, os grupos do ative Directory ("domínio") ou LDAP ("nsswitch") serão usados. As informações do grupo podem ser

especificadas de duas maneiras:

- OAuth 2,0 string de escopo

  Suporta aplicativos confidenciais usando o fluxo de credenciais de cliente onde não há usuário com uma associação de grupo. O escopo deve ser nomeado **ONTAP-group-** com codificação URL-ONTAP-group-name>. Por exemplo, se o grupo for "desenvolvimento", a string de escopo será "ONTAP-group-development".

- Na reclamação "Group" (grupo)

  Isso é destinado a tokens de acesso emitidos pelo ADFS usando o fluxo proprietário do recurso (concessão de senha).

Consulte "Trabalhar com grupos" para obter mais informações.

Escopos OAuth 2,0 independentes

Escopos auto-contidos são strings transportadas no token de acesso. Cada uma é uma definição completa de função personalizada e inclui tudo o que a ONTAP precisa para tomar uma decisão de acesso. O escopo é separado e distinto de qualquer uma das funções REST definidas no próprio ONTAP.

Formato da cadeia de escopo

Em um nível base, o escopo é representado como uma cadeia contígua e composto por seis valores separados por dois pontos. Os parâmetros usados na cadeia de escopo são descritos abaixo.

ONTAP literal

O escopo deve começar com o valor literal `ontap` em minúsculas. Isso identifica o escopo como específico do ONTAP.

Cluster

Isso define a que cluster ONTAP o escopo se aplica. Os valores podem incluir:

- UUID do cluster

  Identifica um único cluster.

- Asterisco (*)

  Indica que o escopo se aplica a todos os clusters.

Você pode usar o comando ONTAP CLI `cluster identity show` para exibir o UUID do cluster. Se não for especificado, o escopo se aplica a todos os clusters.

Função

O nome do papel RESTANTE contido no escopo auto-contido. Esse valor não é examinado pelo ONTAP nem correspondido a nenhuma função REST existente definida como ONTAP. O nome é utilizado para registar.

Nível de acesso

Esse valor indica o nível de acesso aplicado ao aplicativo cliente ao usar o endpoint da API no escopo. Existem seis valores possíveis, conforme descrito na tabela abaixo.

Nível de acesso	Descrição
nenhum	Nega todo o acesso ao endpoint especificado.
readonly	Permite apenas acesso de leitura utilizando O GET.
read_create	Permite o acesso de leitura, bem como a criação de novas instâncias de recursos usando POST.
read_modify	Permite acesso de leitura, bem como a capacidade de atualizar os recursos existentes USANDO PATCH.
read_create_modify	Permite todo o acesso, exceto apagar. As operações permitidas incluem GET (read), POST (Create) e PATCH (update).
tudo	Permite acesso total.

SVM

O nome da SVM no cluster ao qual o escopo se aplica. Use o valor * (asterisco) para indicar todos os SVMs.

> Esta funcionalidade não é totalmente suportada com o ONTAP 9.14,1. Você pode ignorar o parâmetro SVM e usar um asterisco como um marcador de posição. Revise o "Notas de versão do ONTAP" para verificar se há suporte futuro à SVM.

URI DA API REST

O caminho completo ou parcial para um recurso ou conjunto de recursos relacionados. A string deve começar com `/api`. Se você não especificar um valor, o escopo se aplica a todos os endpoints da API no cluster do ONTAP.

Exemplos de escopo

Alguns exemplos de escopos auto-contidos são apresentados abaixo.

ONTAP:*:joes-role:read_create_modify:*:/api/cluster

Fornece ao usuário atribuído essa função de leitura, criação e modificação do acesso ao `/cluster` endpoint.

Ferramenta administrativa CLI

Para tornar a administração dos escopos auto-contidos mais fácil e menos propensa a erros, o ONTAP fornece o comando CLI `security oauth2 scope` para gerar strings de escopo com base em seus parâmetros de entrada.

O comando `security oauth2 scope` tem dois casos de uso com base na sua entrada:

- Parâmetros CLI para string de escopo

  Você pode usar esta versão do comando para gerar uma string de escopo com base nos parâmetros de entrada.

- String de escopo para parâmetros CLI

  Você pode usar esta versão do comando para gerar os parâmetros do comando com base na cadeia de carateres de escopo de entrada.

Exemplo

O exemplo a seguir gera uma string de escopo com a saída incluída após o exemplo de comando abaixo. A definição se aplica a todos os clusters.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Trabalhar com grupos

O ONTAP fornece várias opções para configurar grupos com base no servidor de autorização. Os grupos podem então ser mapeados para funções que são usadas pelo ONTAP para determinar o acesso.

Como os grupos são identificados

Quando você configura um grupo em um servidor de autorização, ele é identificado e transportado em um token de acesso OAuth 2,0 usando um nome ou UUID. Você precisa estar ciente de como o servidor de autorização lida com grupos antes de configurar o ONTAP.

Se vários grupos forem incluídos em um token de acesso, o ONTAP tentará usar cada um até que haja uma correspondência.

Nomes de grupos

Muitos servidores de autorização identificam e representam grupos usando um nome. Aqui está um fragmento de um token de acesso JSON gerado pelo Serviço de Federação do ative Directory (ADFS) contendo vários grupos. Consulte Gerenciar grupos com nomes para obter mais informações.

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

UUUIDs de grupo

Alguns servidores de autorização identificam e representam grupos usando um UUID. Aqui está um fragmento de um token de acesso JSON gerado pelo Microsoft Entra ID contendo vários grupos. Consulte Gerenciar grupos com UUIDs para obter mais informações.

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

Gerenciar grupos com nomes

Se o servidor de autorização usar nomes para identificar grupos, você precisa garantir que cada grupo esteja definido como ONTAP. Dependendo do seu ambiente de segurança, talvez você já tenha o grupo definido.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo nomeado do token de acesso de amostra. Você precisa estar no nível de privilégio ONTAP **admin** para emitir o comando.

Exemplo

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

Você também pode configurar esse recurso usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Gerenciar grupos com UUIDs

Se o servidor de autorização representar grupos usando valores UUID, você precisará executar uma configuração de duas etapas antes de usar um grupo. A partir do ONTAP 9.16,1, dois recursos de mapeamento estão disponíveis e foram testados com o Microsoft Entra ID. Você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos CLI.

Você também pode configurar esses recursos usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Informações relacionadas

- "Comandos CLI do ONTAP"

Mapear um UUID de grupo para um nome de grupo

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, será necessário mapear os UUIDs do grupo para nomes de grupos. As principais operações da CLI do ONTAP são

descritas abaixo.

Criar

Você pode definir uma nova configuração de mapeamento de grupo com o `security login group create` comando. O UUID e o nome do grupo devem corresponder à configuração no servidor de autorização.

Parâmetros

Os parâmetros usados para criar um mapeamento de grupo são descritos abaixo.

Parâmetro	Descrição
`vserver`	Opcionalmente, especifica o nome do SVM (vserver) ao qual o grupo está associado. Se omitido, o grupo está associado ao cluster ONTAP.
`name`	O nome exclusivo do grupo que o ONTAP usará.
`type`	Este valor indica o provedor de identidade do qual o grupo se origina.
`uuid`	Especifica o identificador universalmente exclusivo do grupo, conforme fornecido pelo servidor de autorização.

Aqui está um exemplo de comando CLI definindo um grupo para ONTAP. Observe que está usando um grupo UUID do token de acesso de amostra.

Exemplo

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

Depois de criar o grupo, um identificador inteiro exclusivo somente leitura é gerado para o grupo.

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Você pode usar a `show` opção para recuperar o ID de grupo exclusivo gerado para um grupo. Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapear um UUID de grupo para uma função

Se você estiver usando um servidor de autorização que representa grupos usando valores UUID, você poderá mapear o grupo para uma função. As principais operações da CLI do ONTAP são descritas abaixo. Além disso, você precisa estar no nível de privilégio ONTAP **admin** para emitir os comandos.

> Você precisa primeiro Mapear um UUID de grupo para um nome de grupo e recuperar o ID inteiro exclusivo gerado para o grupo. Você precisará do ID para mapear o grupo para uma função.

Criar

Você pode definir um novo mapeamento de função com o `security login group role-mapping create` comando.

Parâmetros

Os parâmetros usados para mapear um grupo para uma função são descritos abaixo.

Parâmetro	Descrição
`group-id`	Especifica o ID exclusivo gerado para o grupo usando o comando `security login group create`.
`role`	O nome da função ONTAP para o qual o grupo é mapeado.

Exemplo

```
security login group role-mapping create -group-id 1 -role admin
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos ONTAP para obter mais informações.

Mapeamento de funções externas

Uma função externa é definida em um provedor de identificação configurado para uso pelo ONTAP. Você pode criar e administrar relacionamentos de mapeamento entre essas funções externas e as funções do ONTAP usando a CLI do ONTAP.

Você também pode configurar o recurso de mapeamento de função externa usando a API REST do ONTAP. Saiba mais no "Documentação de automação do ONTAP".

Informações relacionadas

- "Comandos CLI do ONTAP".

Funções externas em um token de acesso

Aqui está um fragmento de um token de acesso JSON contendo dois papéis externos.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configuração

Você pode usar a interface de linha de comando ONTAP para administrar o recurso de mapeamento de função externa.

Criar

Você pode definir uma configuração de mapeamento de função com o `security login external-role-mapping create` comando. Você precisa estar no nível de privilégio ONTAP **admin** para emitir este comando, bem como as opções relacionadas.

Parâmetros

Os parâmetros usados para criar um mapeamento de grupo são descritos abaixo.

Parâmetro	Descrição
`external-role`	O nome da função definida no provedor de identidade externo.
`provider`	O nome do provedor de identidade. Este deve ser o identificador do sistema.
`ontap-role`	Indica a função ONTAP existente para a qual a função externa está mapeada.

Exemplo

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Operações CLI adicionais

O comando suporta várias operações adicionais, incluindo:

- Mostrar
- Modificar
- Eliminar

Consulte a documentação de referência dos comandos do ONTAP ou as páginas man da CLI do ONTAP para obter mais informações.

Como o ONTAP determina o acesso do cliente

Para projetar e implementar adequadamente o OAuth 2,0, você precisa entender como sua configuração de autorização é usada pelo ONTAP para tomar decisões de acesso para os clientes. As principais etapas usadas para determinar o acesso são apresentadas abaixo com base na versão do ONTAP.

Não houve atualizações significativas do OAuth 2,0 com o ONTAP 9.15,1. Se estiver a utilizar a versão 9.15.1, consulte a descrição do ONTAP 9.14,1.

Informações relacionadas

- "Recursos do OAuth 2,0 suportados no ONTAP"

ONTAP 9.16,1

O ONTAP 9.16,1 expande o suporte padrão do OAuth 2,0 para incluir extensões específicas do Microsoft Entra ID para grupos nativos de ID do Entra, bem como mapeamento de funções externas.

Determine o acesso do cliente para o ONTAP 9.16,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, ou como uma reivindicação, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos, o formato será examinado. Se os grupos forem representados como UUIDs, uma tabela de mapeamento de grupo interno será pesquisada. Se houver uma correspondência de grupo e uma função associada, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina. Para obter mais informações, "Trabalhar com grupos"consulte .

Se os grupos forem representados como nomes e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente. Se houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma

decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

ONTAP 9.14,1

O OAuth 2,0 inicial suportado é introduzido com o ONTAP 9.14,1 com base nos recursos padrão do OAuth 2,0.

Determine o acesso do cliente para o ONTAP 9.14,1

Passo 1: Escopos auto-contidos

Se o token de acesso contiver quaisquer escopos auto-contidos, o ONTAP examina esses escopos primeiro. Se não existirem escopos auto-suficientes, avance para o passo 2.

Com um ou mais escopos independentes presentes, o ONTAP aplica cada escopo até que uma decisão explícita de **PERMITIR** ou **NEGAR** possa ser tomada. Se uma decisão explícita for tomada, o processamento termina.

Se o ONTAP não conseguir tomar uma decisão de acesso explícito, avance para o passo 2.

Passo 2: Verifique o sinalizador de funções locais

ONTAP examina o parâmetro booleano `use-local-roles-if-present` . O valor deste sinalizador é definido separadamente para cada servidor de autorização definido como ONTAP.

- Se o valor for `true`, avance para o passo 3.
- Se o valor estiver `false` a processar termina e o acesso for negado.

Passo 3: Nomeado ONTAP REST role

Se o token de acesso contiver uma FUNÇÃO REST nomeada `scope` no campo ou `scp`, o ONTAP usará a função para tomar a decisão de acesso. Isso sempre resulta em uma decisão **ALLOW** ou **DENY** e o processamento termina.

Se não houver nenhuma função REST nomeada ou a função não for encontrada, continue para a etapa 4.

Passo 4: Usuários

Extraia o nome de usuário do token de acesso e tente combiná-lo com os usuários que têm acesso ao aplicativo "http". Os usuários são examinados com base no método de autenticação na seguinte ordem:

- palavra-passe
- Domínio (ative Directory)
- Nsswitch (LDAP)

Se um usuário correspondente for encontrado, o ONTAP usará a função definida para que o usuário tome uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se um usuário não for correspondido ou se não houver nome de usuário no token de acesso, continue para a etapa 5.

Passo 5: Grupos

Se um ou mais grupos forem incluídos e configurados com autorização de domínio ou nsswitch, o ONTAP tentará combiná-los com um grupo do ative Directory ou LDAP, respetivamente.

Se houver uma correspondência de grupo, o ONTAP usará a função definida para o grupo tomar uma decisão de acesso. Isso sempre resulta em uma decisão e processamento **ALLOW** ou **DENY** termina.

Se não houver correspondência de grupo ou se não houver nenhum grupo no token de acesso, o acesso será negado e o processamento será concluído.

Cenários de implantação do OAuth 2,0

Há várias opções de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Com base nessas opções, você pode definir um servidor de autorização apropriado para o seu ambiente usando um dos vários cenários de implantação.

Resumo dos parâmetros de configuração

Existem vários parâmetros de configuração disponíveis ao definir um servidor de autorização para o ONTAP. Estes parâmetros são geralmente suportados em todas as interfaces administrativas.

> O nome usado para um parâmetro ou campo individual pode variar dependendo da interface administrativa do ONTAP. Para acomodar as diferenças nas interfaces administrativas, um único nome genérico é usado para cada parâmetro na tabela. O nome exato usado com uma interface específica deve ser óbvio com base no contexto.

Parâmetro	Descrição
Nome	O nome do servidor de autorização como é conhecido pelo ONTAP.
Aplicação	A aplicação interna do ONTAP à qual a definição se aplica. Este deve ser **http**.
URI do emissor	O FQDN com o caminho que identifica o site ou a organização que emite os tokens.
URI do provedor JWKS	O FQDN com caminho e nome de arquivo onde o ONTAP obtém os conjuntos de chaves da Web JSON usados para validar os tokens de acesso.
Intervalo de atualização do JWKS	O intervalo de tempo que determina com que frequência o ONTAP atualiza informações de certificado do URI JWKS do provedor. O valor é especificado no formato ISO-8601.
Endpoint de introspeção	O FQDN com caminho que o ONTAP usa para executar a validação remota de token por meio de introspeção.
ID do cliente	O nome do cliente, conforme definido no servidor de autorização. Quando esse valor é incluído, você também precisa fornecer o segredo do cliente associado com base na interface.
Proxy de saída	Isso é para fornecer acesso ao servidor de autorização quando o ONTAP está atrás de um firewall. O URI deve estar no formato curl.
Use funções locais, se presentes	Um sinalizador booleano que determina se as definições ONTAP locais são usadas, incluindo uma FUNÇÃO REST nomeada e usuários locais.
Reclamação do utilizador remoto	Um nome alternativo que o ONTAP usa para corresponder aos usuários locais. Use o `sub` campo no token de acesso para corresponder ao nome de usuário local.
Público-alvo	Este campo define os endpoints onde o token de acesso pode ser usado.

Cenários de implantação

Vários cenários comuns de implantação são apresentados abaixo. Eles são organizados com base se a validação de token é realizada localmente pelo ONTAP ou remotamente pelo servidor de autorização. Cada cenário inclui uma lista das opções de configuração necessárias. "Implantar o OAuth 2,0 no ONTAP"Consulte para obter exemplos dos comandos de configuração.

Depois de definir um servidor de autorização, você pode exibir sua configuração por meio da interface administrativa do ONTAP. Por exemplo, use o comando `security oauth2 client show` com a CLI do ONTAP.

Validação local

Os cenários de implantação a seguir são baseados no ONTAP executando a validação de token localmente.

Use escopos autônomos sem um proxy

Esta é a implantação mais simples usando apenas escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- URI do emissor

Você também precisa adicionar os escopos no servidor de autorização.

Use escopos autônomos com um proxy

Esse cenário de implantação usa os escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade ONTAP local é usada. Mas o servidor de autorização está atrás de um firewall e, portanto, você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Proxy de saída
- URI do emissor
- Público-alvo

Você também precisa adicionar os escopos no servidor de autorização.

Use funções de usuário local e mapeamento de nome de usuário padrão com um proxy

Esse cenário de implantação usa funções de usuário local com mapeamento de nomes padrão. A reivindicação de usuário remoto usa o valor padrão de `sub` e, portanto, esse campo no token de acesso é usado para corresponder ao nome de usuário local. O nome de usuário deve ter 40 carateres ou menos. O servidor de autorização está atrás de um firewall, então você também precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Proxy de saída
- Emissor

Tem de se certificar de que o utilizador local está definido como ONTAP.

Use funções de usuário local e mapeamento de nome de usuário alternativo com um proxy

Esse cenário de implantação usa funções de usuário local com um nome de usuário alternativo que é usado para corresponder a um usuário local do ONTAP. O servidor de autorização está atrás de um firewall, então você precisa configurar um proxy. Você precisa incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- URI do provedor JWKS
- Usar funções locais, se presentes (`true`)
- Reclamação do utilizador remoto
- Proxy de saída
- URI do emissor
- Público-alvo

Tem de se certificar de que o utilizador local está definido como ONTAP.

Introspeção remota

As configurações de implantação a seguir são baseadas no ONTAP executando a validação de token remotamente por meio de introspeção.

Use escopos autônomos sem proxy

Esta é uma implantação simples baseada no uso dos escopos auto-contidos do OAuth 2,0. Nenhuma das definições de identidade do ONTAP é usada. Você deve incluir os seguintes parâmetros:

- Nome
- Aplicação (http)
- Endpoint de introspeção
- ID do cliente
- URI do emissor

Você precisa definir os escopos, bem como o segredo do cliente e do cliente no servidor de autorização.

Autenticação de cliente usando TLS mútuo

Dependendo de suas necessidades de segurança, você pode configurar opcionalmente o TLS mútuo (MTLS) para implementar uma autenticação de cliente forte. Quando usado com o ONTAP como parte de uma implantação do OAuth 2,0, o MTLS garante que os tokens de acesso são usados apenas pelos clientes aos quais foram emitidos originalmente.

TLS mútuo com OAuth 2,0

O Transport Layer Security (TLS) é usado para estabelecer um canal de comunicação seguro entre dois aplicativos, normalmente um navegador cliente e um servidor da Web. O TLS mútuo estende isso fornecendo uma forte identificação do cliente através de um certificado de cliente. Quando usado em um cluster ONTAP

com OAuth 2,0, a funcionalidade base MTLS é estendida criando e usando tokens de acesso restritos ao remetente.

Um token de acesso restrito ao remetente só pode ser usado pelo cliente para o qual foi emitido originalmente. Para suportar esse recurso, uma nova solicitação de confirmação (`cnf`) é inserida no token. O campo contém uma propriedade `x5t#S256` que contém um resumo do certificado de cliente usado ao solicitar o token de acesso. Esse valor é verificado pela ONTAP como parte da validação do token. Os tokens de acesso emitidos por servidores de autorização que não estão restritos ao remetente não incluem a reivindicação de confirmação adicional.

Você precisa configurar o ONTAP para usar o MTLS separadamente para cada servidor de autorização. Por exemplo, o comando CLI `security oauth2 client` inclui o parâmetro `use-mutual-tls` para controlar o processamento MTLS com base em três valores, como mostrado na tabela abaixo.

Em cada configuração, o resultado e a ação tomadas pelo ONTAP dependem do valor do parâmetro de configuração, bem como do conteúdo do token de acesso e do certificado do cliente. Os parâmetros na tabela são organizados do mínimo ao mais restritivo.

Parâmetro	Descrição
nenhum	A autenticação TLS mútua OAuth 2,0 está completamente desativada para o servidor de autorização. A ONTAP não executará a autenticação de certificado de cliente MTLS, mesmo que a reclamação de confirmação esteja presente no token ou um certificado de cliente seja fornecido com a conexão TLS.
pedido	A autenticação TLS mútua do OAuth 2,0 é aplicada se um token de acesso restrito ao remetente for apresentado pelo cliente. Ou seja, o MTLS é aplicado somente se a reivindicação de confirmação (com propriedade `x5t#S256`) estiver presente no token de acesso. Esta é a configuração padrão.
obrigatório	A autenticação TLS mútua OAuth 2,0 é aplicada para todos os tokens de acesso emitidos pelo servidor de autorização. Portanto, todos os tokens de acesso devem ser restritos ao remetente. A autenticação e a solicitação de API REST falharão se a solicitação de confirmação não estiver presente no token de acesso ou se houver um certificado de cliente inválido.

Fluxo de implementação de alto nível

As etapas típicas envolvidas ao usar o MTLS com o OAuth 2,0 em um ambiente ONTAP são apresentadas abaixo. "RFC 8705: Autenticação de cliente TLS mútuo OAuth 2,0 e tokens de acesso com certificado"Consulte para obter mais detalhes.

Passo 1: Criar e instalar um certificado de cliente

O estabelecimento da identidade do cliente é baseado na comprovação do conhecimento de uma chave privada do cliente. A chave pública correspondente é colocada em um certificado X,509 assinado apresentado pelo cliente. Em alto nível, as etapas envolvidas na criação do certificado de cliente incluem:

1. Gere um par de chaves públicas e privadas
2. Crie uma solicitação de assinatura de certificado
3. Envie o arquivo CSR para uma CA conhecida
4. A CA verifica a solicitação e emite o certificado assinado

Normalmente, você pode instalar o certificado de cliente em seu sistema operacional local ou usá-lo

diretamente com um utilitário comum, como curl.

Passo 2: Configure o ONTAP para usar o MTLS

Você precisa configurar o ONTAP para usar o MTLS. Esta configuração é feita separadamente para cada servidor de autorização. Por exemplo, com a CLI o comando `security oauth2 client` é usado com o parâmetro opcional `use-mutual-tls` . Consulte "Implantar o OAuth 2,0 no ONTAP" para obter mais informações.

Passo 3: O cliente solicita um token de acesso

O cliente precisa solicitar um token de acesso do servidor de autorização configurado para ONTAP. O aplicativo cliente deve usar o MTLS com o certificado criado e instalado na etapa 1.

Passo 4: O servidor de autorização gera o token de acesso

O servidor de autorização verifica a solicitação do cliente e gera um token de acesso. Como parte disso, ele cria um resumo de mensagem do certificado do cliente que é incluído no token como uma reivindicação de confirmação (campo `cnf`).

Passo 5: O aplicativo cliente apresenta o token de acesso ao ONTAP

O aplicativo cliente faz uma chamada de API REST para o cluster ONTAP e inclui o token de acesso no cabeçalho da solicitação de autorização como um **token de portador**. O cliente deve usar o MTLS com o mesmo certificado usado para solicitar o token de acesso.

Passo 6: O ONTAP verifica o cliente e o token.

O ONTAP recebe o token de acesso em uma solicitação HTTP, bem como o certificado de cliente usado como parte do processamento do MTLS. O ONTAP primeiro valida a assinatura no token de acesso. Com base na configuração, o ONTAP gera um resumo de mensagem do certificado do cliente e compara-o com a reclamação de confirmação **cnf** no token. Se os dois valores corresponderem, o ONTAP confirmou que o cliente que faz a solicitação de API é o mesmo cliente para o qual o token de acesso foi originalmente emitido.

Configurar e implantar

Prepare-se para implantar o OAuth 2,0 com o ONTAP

Antes de configurar o OAuth 2,0 em um ambiente ONTAP, você deve se preparar para a implantação. Um resumo das principais tarefas e decisões está incluído abaixo. O arranjo das seções é geralmente alinhado com a ordem que você deve seguir. Mas, embora seja aplicável à maioria das implantações, você deve adaptá-lo ao seu ambiente conforme necessário. Você também deve considerar a criação de um plano de implantação formal.

Com base no seu ambiente, pode selecionar a configuração para os servidores de autorização definidos para o ONTAP. Isso inclui os valores de parâmetro que você precisa especificar para cada tipo de implantação. Consulte "Cenários de implantação do OAuth 2,0" para obter mais informações.

Recursos protegidos e aplicativos de clientes

O OAuth 2,0 é uma estrutura de autorização para controlar o acesso a recursos protegidos. Diante disso, um primeiro passo importante com qualquer implantação é determinar quais são os recursos disponíveis e quais clientes precisam acessar.

Identificar aplicativos clientes

Você precisa decidir quais clientes usarão o OAuth 2,0 ao emitir chamadas de API REST e quais endpoints de API eles precisam acessar.

Analise as funções REST do ONTAP e os usuários locais existentes

Você deve rever as definições de identidade do ONTAP existentes, incluindo as funções REST e os usuários locais. Dependendo de como você configura o OAuth 2,0, essas definições podem ser usadas para tomar decisões de acesso.

Transição global para o OAuth 2,0

Embora você possa implementar a autorização do OAuth 2,0 gradualmente, você também pode mover todos os clientes de API REST para o OAuth 2,0 imediatamente definindo um sinalizador global para cada servidor de autorização. Isso permite que as decisões de acesso sejam tomadas com base na configuração existente do ONTAP sem a necessidade de criar escopos autônomos.

Servidores de autorização

Os servidores de autorização desempenham um papel importante na implantação do OAuth 2,0, emitindo tokens de acesso e impondo a política administrativa.

Selecione e instale o servidor de autorização

Você precisa selecionar e instalar um ou mais servidores de autorização. É importante familiarizar-se com as opções de configuração e procedimentos dos seus provedores de identidade, incluindo como definir escopos. Observe que alguns servidores de autorização, incluindo o Microsoft Entra ID, representam grupos usando UUIDs em vez de nomes.

Determine se o certificado de CA raiz de autorização precisa ser instalado

O ONTAP usa o certificado do servidor de autorização para validar os tokens de acesso assinados apresentados pelos clientes. Para fazer isso, o ONTAP precisa do certificado de CA raiz e de quaisquer certificados intermediários. Estes podem ser pré-instalados com o ONTAP. Se não, você precisa instalá-los.

Avaliar a localização e a configuração da rede

Se o servidor de autorização estiver atrás de um firewall, o ONTAP precisa ser configurado para usar um servidor proxy.

Autenticação e autorização do cliente

Existem vários aspetos da autenticação e autorização do cliente que você precisa considerar.

Escopos auto-contidos ou definições de identidade ONTAP local

Em um alto nível, você pode definir escopos autônomos definidos no servidor de autorização ou confiar nas definições de identidade ONTAP locais existentes, incluindo funções e usuários.

Opções com processamento ONTAP local

Se você usar as definições de identidade do ONTAP, você deve decidir qual aplicar, incluindo:

- Função REST nomeada
- Corresponder a utilizadores locais
- Grupos do ative Directory ou LDAP

Validação local ou introspeção remota

Você precisa decidir se os tokens de acesso serão validados localmente pelo ONTAP ou no servidor de

autorização por meio de introspeção. Há também vários valores relacionados a serem considerados, como o intervalo de atualização.

Tokens de acesso restrito ao remetente

Para ambientes que exigem um alto nível de segurança, você pode usar tokens de acesso com restrição de envio baseados em MTLS. Isso requer um certificado para cada cliente.

Grupos como UUIDs e mapeamento de identidade

Se você estiver usando um servidor de autorização que representa grupos usando UUIDs, você precisará Planejar como mapeá-los para nomes de grupos e, possivelmente, para funções associadas.

Interface administrativa

Você pode executar a administração do OAuth 2,0 por meio de qualquer uma das interfaces do ONTAP, incluindo:

- Interface de linha de comando
- System Manager
- API REST

Como os clientes solicitam tokens de acesso

Os aplicativos cliente devem solicitar tokens de acesso diretamente do servidor de autorização. Você precisa decidir como isso será feito, incluindo o tipo de concessão.

Configurar o ONTAP

Há várias tarefas de configuração do ONTAP que você precisa executar.

Defina funções REST e usuários locais

Com base na sua configuração de autorização, pode ser utilizado o processamento de identificação local do ONTAP. Nesse caso, você precisa revisar e definir as funções REST e as definições de usuário. E, dependendo do seu servidor de autorização, isso também pode incluir a administração de grupos com base nos valores UUID.

Configuração central

Há três etapas principais necessárias para executar a configuração principal do ONTAP, incluindo:

- Opcionalmente, instale o certificado raiz (e quaisquer certificados intermediários) para a CA que assinou o certificado do servidor de autorização.
- Defina o servidor de autorização.
- Ative o processamento OAuth 2,0 para o cluster.

Implantar o OAuth 2,0 no ONTAP

A implantação da funcionalidade principal do OAuth 2,0 envolve três etapas principais.

Antes de começar

Você deve se preparar para a implantação do OAuth 2,0 antes de configurar o ONTAP. Por exemplo, você precisa avaliar o servidor de autorização, incluindo como seu certificado foi assinado e se está atrás de um firewall. Consulte "Prepare-se para implantar o OAuth 2,0 com o ONTAP" para obter mais informações.

Etapa 1: Instale os certificados de CA raiz do servidor de autorização

O ONTAP inclui um grande número de certificados de CA raiz pré-instalados. Assim, em muitos casos, o certificado para o seu servidor de autorização será imediatamente reconhecido pelo ONTAP sem configuração adicional. Mas dependendo de como o certificado do servidor de autorização foi assinado, talvez seja necessário instalar um certificado de CA raiz e quaisquer certificados intermediários.

Siga as instruções fornecidas abaixo para instalar o certificado, se necessário. Você deve instalar todos os certificados necessários no nível do cluster.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 1. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **certificados**.
4. Na guia **autoridades de certificação confiáveis**, clique em **Adicionar**.
5. Clique em **Importar** e selecione o arquivo de certificado.
6. Complete os parâmetros de configuração para o seu ambiente.
7. Clique em **Add**.

CLI

1. Inicie a instalação:

   ```
   security certificate install -type server-ca
   ```

2. Procure a seguinte mensagem do console:

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. Abra o arquivo de certificado com um editor de texto.
4. Copie o certificado inteiro, incluindo as seguintes linhas:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Cole o certificado no terminal após o prompt de comando.
6. Pressione **Enter** para concluir a instalação.
7. Confirme se o certificado está instalado usando uma das seguintes opções:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Etapa 2: Configurar o servidor de autorização

Você precisa definir pelo menos um servidor de autorização para o ONTAP. Você deve escolher os valores de parâmetro com base em sua configuração e plano de implantação. Reveja "Cenários de implantação do OAuth2" para determinar os parâmetros exatos necessários para a sua configuração.

Para modificar uma definição de servidor de autorização, você pode excluir a definição existente e criar uma nova.

O exemplo fornecido abaixo é baseado no primeiro cenário de implantação simples em "Validação local". Escopos auto-contidos são usados sem um proxy.

Escolha o procedimento correto com base em como você acessa o ONTAP. O procedimento CLI usa variáveis simbólicas que você precisa substituir antes de emitir o comando.

Exemplo 2. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em *** ao lado de *autorização OAuth 2,0**.
4. Selecione **mais opções**.
5. Forneça os valores necessários para sua implantação, como:
   - Nome
   - Aplicação (http)
   - URI do provedor JWKS
   - URI do emissor
6. Clique em **Add**.

CLI

1. Crie a definição novamente:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Por exemplo:

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Passo 3: Ative o OAuth 2,0

O passo final é habilitar o OAuth 2,0. Esta é uma configuração global para o cluster ONTAP.

> Não ative o processamento do OAuth 2,0 até confirmar que o ONTAP, os servidores de autorização e quaisquer serviços de suporte foram configurados corretamente.

Escolha o procedimento correto com base em como você acessa o ONTAP.

Exemplo 3. Passos

System Manager

1. No System Manager, selecione **Cluster** > **Settings**.
2. Role para baixo até a seção **Segurança**.
3. Clique em → ao lado de **autorização OAuth 2,0**.
4. Ativar **autorização OAuth 2,0**.

CLI

1. Ativar OAuth 2,0:

   ```
   security oauth2 modify -enabled true
   ```

2. Confirmar que o OAuth 2,0 está ativado:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Emita uma chamada de API REST usando o OAuth 2,0

A implementação do OAuth 2,0 no ONTAP suporta aplicações cliente API REST. Você pode emitir uma simples chamada de API REST usando curl para começar a usar o OAuth 2,0. O exemplo apresentado abaixo recupera a versão do cluster do ONTAP.

Antes de começar

Você deve configurar e ativar o recurso OAuth 2,0 para seu cluster ONTAP. Isso inclui a definição de um servidor de autorização.

Passo 1: Adquira um token de acesso

Você precisa adquirir um token de acesso para usar com a chamada API REST. A solicitação de token é realizada fora do ONTAP e o procedimento exato depende do servidor de autorização e de sua configuração. Você pode solicitar o token através de um navegador da Web, com um comando curl ou usando uma linguagem de programação.

Para fins de ilustração, um exemplo de como um token de acesso pode ser solicitado ao Keycloak usando curl é apresentado abaixo.

Exemplo de capa-chave

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Você deve copiar e salvar o token retornado.

Etapa 2: Emita a chamada da API REST

Depois de ter um token de acesso válido, você pode usar um comando curl com o token de acesso para emitir uma chamada de API REST.

Parâmetros e variáveis

As duas variáveis no exemplo curl são descritas na tabela abaixo.

Variável	Descrição
FQDN_IP	O nome de domínio totalmente qualificado ou o endereço IP do LIF de gerenciamento do ONTAP.
ACCESS_TOKEN	O token de acesso OAuth 2,0 emitido pelo servidor de autorização.

Você deve primeiro definir essas variáveis no ambiente de shell Bash antes de emitir o exemplo curl. Por exemplo, na CLI do Linux digite o seguinte comando para definir e exibir a variável FQDN:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Depois que ambas as variáveis são definidas no seu shell Bash local, você pode copiar o comando curl e colá-lo na CLI. Pressione **Enter** para substituir as variáveis e emitir o comando.

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

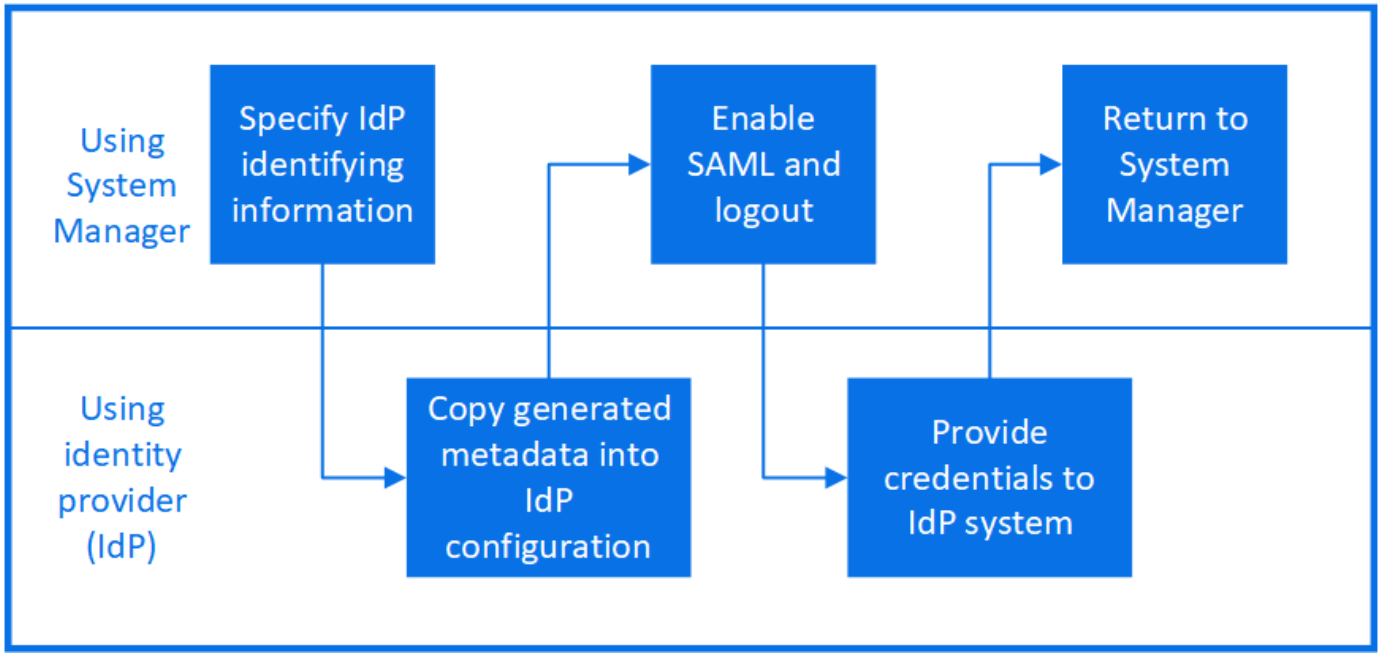
Configurar a autenticação SAML

A partir do ONTAP 9.3, você pode configurar a autenticação de linguagem de marcação de asserção de Segurança (SAML) para serviços da Web. Quando a autenticação SAML é configurada e ativada, os usuários são autenticados por um Provedor de identidade (IDP) externo em vez dos provedores de serviços de diretório, como o ative Directory e o LDAP.

Ativar a autenticação SAML

Para ativar a autenticação SAML com o System Manager ou com a CLI, execute as seguintes etapas. Se o cluster estiver executando o ONTAP 9.7 ou anterior, as etapas do Gerenciador de sistema que você precisa seguir serão diferentes. Consulte a ajuda online do System Manager disponível no seu sistema.

> Depois de ativar a autenticação SAML, somente usuários remotos podem acessar a GUI do System Manager. Os usuários locais não podem acessar a GUI do System Manager depois que a autenticação SAML estiver ativada.



Antes de começar

- O IDP que pretende utilizar para autenticação remota tem de ser configurado.

  > Consulte a documentação fornecida pelo IDP que você configurou.

- Você deve ter o URI do IDP.

Sobre esta tarefa

- A autenticação SAML aplica-se apenas `http` aos aplicativos e `ontapi`.

`http`Os aplicativos e `ontapi` são usados pelos seguintes serviços da Web: Infraestrutura do processador de serviço, APIs do ONTAP ou Gerenciador de sistema.

- A autenticação SAML é aplicável apenas para acessar o SVM admin.

Os seguintes IDPs foram validados com o System Manager:

- Serviços de Federação do ative Directory
- Cisco Duo (validado com as seguintes versões do ONTAP:)
  - 9.7P21 e versões posteriores do 9,7 (consulte a "Documentação do System Manager Classic")
  - 9.8P17 e versões posteriores do 9,8
  - 9,9.1P13 e versões posteriores do 9,9
  - 9.10.1P9 e versões posteriores do 9,10
  - 9.11.1P4 e versões posteriores do 9,11
  - 9.12.1 e versões posteriores
- Shibboleth

Execute as seguintes etapas, dependendo do ambiente:

Exemplo 4. Passos

System Manager

1. Clique em **Cluster > Settings**.
2. Ao lado de **Autenticação SAML**, clique em .
3. Verifique se há uma verificação na caixa de seleção **Ativar autenticação SAML**.
4. Insira o URL do URI de IDP (incluindo "https://").
5. Modifique o endereço do sistema host, se necessário.
6. Certifique-se de que está a ser utilizado o certificado correto:
   - Se o seu sistema foi mapeado com apenas um certificado com o tipo "servidor", esse certificado é considerado o padrão e não é exibido.
   - Se o seu sistema foi mapeado com vários certificados como tipo "servidor", um dos certificados será exibido. Para selecionar um certificado diferente, clique em **alterar**.
7. Clique em **Salvar**. Uma janela de confirmação exibe as informações de metadados, que foram copiadas automaticamente para a área de transferência.
8. Vá para o sistema IDP que você especificou e copie os metadados da área de transferência para atualizar os metadados do sistema.
9. Retorne à janela de confirmação (no System Manager) e marque a caixa de seleção **Eu configurei o IDP com o URI do host ou metadados**.
10. Clique em **Logout** para ativar a autenticação baseada em SAML. O sistema IDP exibirá uma tela de autenticação.
11. No sistema IDP, insira suas credenciais baseadas em SAML. Depois que suas credenciais forem verificadas, você será direcionado para a página inicial do System Manager.

CLI

1. Crie uma configuração SAML para que o ONTAP possa acessar os metadados do IDP:

   `security saml-sp create -idp-uri` *`idp_uri`* `-sp-host` *`ontap_host_name`*

   `idp_uri` É o endereço FTP ou HTTP do host IDP de onde os metadados IDP podem ser baixados.

   `ontap_host_name` É o nome do host ou endereço IP do host do provedor de serviços SAML, que neste caso é o sistema ONTAP. Por padrão, o endereço IP do LIF de gerenciamento de cluster é usado.

   Opcionalmente, você pode fornecer as informações do certificado do servidor ONTAP. Por padrão, as informações de certificado do servidor Web do ONTAP são usadas.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the Data ONTAP user configuration.
```

O URL para acessar os metadados do host do ONTAP é exibido.

2. No host IDP, configure o IDP com os metadados do host ONTAP.

   Para obter mais informações sobre como configurar o IDP, consulte a documentação do IDP.

3. Ativar configuração SAML:

   security saml-sp modify -is-enabled true

   Qualquer usuário existente que acesse o `http` aplicativo ou `ontapi` é configurado automaticamente para autenticação SAML.

4. Se você quiser criar usuários para o `http` aplicativo ou `ontapi` depois que o SAML for configurado, especifique SAML como o método de autenticação para os novos usuários.

   a. Criar um método de login para novos usuários com autenticação SAML
   security login create -user-or-group-name *user_name* -application [http | ontapi] -authentication-method saml -vserver *svm_name*

   ```
   cluster_12::> security login create -user-or-group-name admin1
   -application http -authentication-method saml -vserver
   cluster_12
   ```

   b. Verifique se a entrada do usuário foi criada:

   security login show

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                 Authentication                 Acct
Authentication
Name           Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin          console     password      admin            no
none
admin          http        password      admin            no
none
admin          http        saml          admin            -
none
admin          ontapi      password      admin            no
none
admin          ontapi      saml          admin            -
none
admin          service-processor
                           password      admin            no
none
admin          ssh         password      admin            no
none
admin1         http        password      backup           no
none
**admin1       http        saml          backup           -
none**
```

Desativar a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários da Web usando um provedor de identidade externo (IDP). Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ative Directory e o LDAP, são usados para autenticação.

Execute as seguintes etapas, dependendo do ambiente:

Exemplo 5. Passos

System Manager

1. Clique em **Cluster > Settings**.
2. Em **Autenticação SAML**, clique no botão de alternância **Enabled**.
3. *Opcional*: Você também pode clicar ⚙ ao lado de **Autenticação SAML** e, em seguida, desmarcar a caixa de seleção **Ativar autenticação SAML**.

CLI

1. Desativar autenticação SAML:

   ```
   security saml-sp modify -is-enabled false
   ```

2. Se você não quiser mais usar a autenticação SAML ou se quiser modificar o IDP, exclua a configuração SAML:

   ```
   security saml-sp delete
   ```

Solucionar problemas com a configuração SAML

Se a configuração da autenticação SAML (Security Assertion Markup Language) falhar, você poderá reparar manualmente cada nó em que a configuração SAML falhou e recuperar da falha. Durante o processo de reparo, o servidor da Web é reiniciado e todas as conexões HTTP ou HTTPS ativas são interrompidas.

Sobre esta tarefa

Quando você configura a autenticação SAML, o ONTAP aplica a configuração SAML por nó. Quando você ativa a autenticação SAML, o ONTAP tenta reparar automaticamente cada nó se houver problemas de configuração. Se houver problemas com a configuração SAML em qualquer nó, você poderá desabilitar a autenticação SAML e rehabilitar a autenticação SAML. Pode haver situações em que a configuração SAML não se aplica em um ou mais nós, mesmo após a reativação da autenticação SAML. Você pode identificar o nó no qual a configuração SAML falhou e, em seguida, reparar manualmente esse nó.

Passos

1. Inicie sessão no nível de privilégio avançado:

   ```
   set -privilege advanced
   ```

2. Identificar o nó no qual a configuração SAML falhou:

   ```
   security saml-sp status show -instance
   ```

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. Repare a configuração SAML no nó com falha:

   security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   O servidor web é reiniciado e quaisquer conexões HTTP ou HTTPS ativas são interrompidas.

4. Verifique se o SAML está configurado com êxito em todos os nós:

   security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: **config-success**
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

Informações relacionadas

"Referência do comando ONTAP"

Autenticação e autorização usando WebAuthn MFA

Visão geral da autenticação multifator WebAuthn

A partir do ONTAP 9.16,1, os administradores podem ativar a autenticação multifator WebAuthn (MFA) para usuários que fazem login no Gerenciador de sistema. Isso permite logins do System Manager usando uma chave FIDO2 (como uma YubiKey) como uma segunda forma de autenticação. Por padrão, o WebAuthn MFA está desativado para usuários novos e existentes do ONTAP.

O WebAuthn MFA é compatível com usuários e grupos que usam os seguintes tipos de autenticação para o primeiro método de autenticação:

- Usuários: Senha, domínio ou nsswitch
- Grupos: Domínio ou nsswitch

Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário, o usuário é solicitado a Registrar um autenticador de hardware ao fazer login no System Manager. Após o Registro, a chave privada é armazenada no autenticador e a chave pública é armazenada no ONTAP.

O ONTAP suporta uma credencial WebAuthn por usuário. Se um usuário perder um autenticador e precisar substituí-lo, o administrador do ONTAP precisará excluir a credencial WebAuthn do usuário para que o usuário possa Registrar um novo autenticador no próximo login.

Os usuários que têm o WebAuthn MFA habilitado como um segundo método de autenticação precisam usar o FQDN (por exemplo, "https://myontap.example.com") em vez do endereço IP (por exemplo, "https://192.168.100.200") para acessar o System Manager. Para usuários com WebAuthn MFA habilitado, as tentativas de fazer login no System Manager usando o endereço IP são rejeitadas.

Habilite o MFA WebAuthn para usuários ou grupos do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode ativar o WebAuthn MFA para um usuário ou grupo do Gerenciador de sistema adicionando um novo usuário ou grupo com a opção de WebAuthn MFA ativada ou habilitando a opção para um usuário ou grupo existente.

Depois de ativar o WebAuthn MFA como o segundo método de autenticação para um usuário ou grupo, o usuário (ou todos os usuários desse grupo) será solicitado a Registrar um dispositivo FIDO2 de hardware no próximo login no System Manager. Esse Registro é gerenciado pelo sistema operacional local do usuário e geralmente consiste em inserir a chave de segurança, criar uma chave de acesso e tocar na chave de segurança (se suportada).

Ative o WebAuthn MFA ao criar um novo usuário ou grupo

Você pode criar um novo usuário ou grupo com o WebAuthn MFA habilitado usando o Gerenciador de sistema ou a CLI do ONTAP.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Selecione **Adicionar** em **usuários**.
4. Especifique um nome de usuário ou grupo e selecione uma função no menu suspenso para **função**.
5. Especifique um método de login e uma senha para o usuário ou grupo.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.

6. Na coluna **MFA para HTTP**, selecione **Enabled**.
7. Selecione **Guardar**.

CLI

1. Crie um novo usuário ou grupo com o WebAuthn MFA habilitado.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Ative o WebAuthn MFA para um usuário ou grupo existente

Você pode ativar o WebAuthn MFA para um usuário ou grupo existente.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o menu de opções para o utilizador ou grupo que pretende editar.

   WebAuthn MFA suporta métodos de login de "senha", "domínio" ou "nsswitch" para usuários e "domínio" ou "nsswitch" para grupos.
4. Na coluna **MFA para HTTP** para esse usuário, selecione **Enabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para ativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é habilitado escolhendo "publikey" para o segundo método de autenticação:

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "login de segurança criar"
- "modificação de início de sessão de segurança"

Desative o WebAuthn MFA para usuários do Gerenciador de sistema do ONTAP

Como administrador do ONTAP, você pode desativar o WebAuthn MFA para um usuário ou grupo editando o usuário ou grupo com o Gerenciador do sistema ou a CLI do ONTAP.

Desative o WebAuthn MFA para um usuário ou grupo existente

Você pode desativar o WebAuthn MFA para um usuário ou grupo existente a qualquer momento.

> Se desativar as credenciais registadas, as credenciais são retidas. Se você ativar as credenciais novamente no futuro, as mesmas credenciais serão usadas, para que o usuário não precise se Registrar novamente ao fazer login.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de utilizadores e grupos, selecione o utilizador ou grupo que pretende editar.
4. Na coluna **MFA para HTTP** para esse usuário, selecione **Disabled**.
5. Selecione **Guardar**.

CLI

1. Modifique um usuário ou grupo existente para desativar o WebAuthn MFA para esse usuário ou grupo.

   No exemplo a seguir, o WebAuthn MFA é desativado escolhendo "nenhum" para o segundo método de autenticação.

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

Saiba mais

Visite as páginas do manual do ONTAP para este comando:

- "modificação de início de sessão de segurança"

Veja as configurações de MFA do ONTAP WebAuthn e gerencie credenciais

Como administrador do ONTAP, você pode exibir configurações de MFA WebAuthn em todo o cluster e gerenciar credenciais de usuário e grupo para o MFA WebAuthn.

Exibir configurações de cluster para WebAuthn MFA

Você pode exibir as configurações de cluster para WebAuthn MFA usando a CLI do ONTAP.

Passos

1. Veja as configurações do cluster para WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

```
security webauthn show -vserver <storage_vm_name>
```

Veja algoritmos de chave pública suportados do WebAuthn MFA

Você pode exibir os algoritmos de chave pública compatíveis para WebAuthn MFA para uma VM de

armazenamento ou para um cluster.

Passos

1. Liste os algoritmos de chave pública suportados do WebAuthn MFA. Opcionalmente, você pode especificar uma VM de armazenamento usando o `vserver` argumento:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Veja as credenciais do WebAuthn MFA registradas

Como administrador do ONTAP, você pode exibir as credenciais de WebAuthn registradas para todos os usuários. Os utilizadores não administradores que utilizam este procedimento só podem ver as suas próprias credenciais WebAuthn registadas.

Passos

1. Veja as credenciais do WebAuthn MFA registradas:

```
security webauthn credentials show
```

Remova uma credencial WebAuthn MFA registrada

Você pode remover uma credencial WebAuthn MFA registrada. Isso é útil quando a chave de hardware de um usuário foi perdida, roubada ou não está mais em uso. Você também pode remover uma credencial registrada quando o usuário ainda tem o autenticador de hardware original, mas deseja substituí-la por uma nova. Depois de remover a credencial, o usuário será solicitado a Registrar o autenticador de substituição.

> ⓘ A remoção de uma credencial registrada para um usuário não desativa o WebAuthn MFA para o usuário. Se um usuário perder um autenticador de hardware e precisar fazer login antes de substituí-lo, você precisará remover a credencial usando estas etapas e também "Desative o WebAuthn MFA" para o usuário.

System Manager

1. Selecione **Cluster > Settings**.
2. Selecione o ícone de seta ao lado de **usuários e funções**.
3. Na lista de usuários e grupos, selecione o menu de opções para o usuário ou grupo cujas credenciais deseja remover.
4. Selecione **Remover MFA para credenciais HTTP**.
5. Selecione **Remover**.

CLI

1. Elimine as credenciais registadas. Observe o seguinte:
   - Opcionalmente, você pode especificar uma VM de storage do usuário. Se omitida, a credencial é removida no nível do cluster.
   - Opcionalmente, você pode especificar um nome de usuário do usuário para o qual você está excluindo a credencial. Se omitida, a credencial é removida para o usuário atual.

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

Saiba mais

Visite as páginas do manual do ONTAP para estes comandos:

- "segurança webauthn show"
- "os algoritmos suportados por webauthn de segurança são mostrados"
- "credenciais webauthn de segurança são exibidas"
- "credenciais de segurança webauthn excluídas"

Gerenciar serviços da Web

Gerencie a visão geral dos serviços da Web

Você pode ativar ou desativar um serviço da Web para o cluster ou uma máquina virtual de armazenamento (SVM), exibir as configurações de serviços da Web e controlar se os usuários de uma função podem acessar um serviço da Web.

Você pode gerenciar os serviços da Web para o cluster ou uma SVM das seguintes maneiras:

- Ativar ou desativar um serviço Web específico
- Especificar se o acesso a um serviço da Web é restrito apenas a HTTP encriptado (SSL)
- Exibindo a disponibilidade de serviços da Web
- Permitir ou não permitir que usuários de uma função acessem um serviço da Web
- Exibindo as funções que têm permissão para acessar um serviço da Web

Para que um usuário acesse um serviço da Web, todas as seguintes condições devem ser atendidas:

- O usuário deve ser autenticado.

  Por exemplo, um serviço da Web pode solicitar um nome de usuário e uma senha. A resposta do usuário deve corresponder a uma conta válida.

- O utilizador tem de ser configurado com o método de acesso correto.

  A autenticação só é bem-sucedida para os usuários com o método de acesso correto para o serviço web fornecido. Para o serviço Web da API ONTAP `ontapi`), os usuários devem ter o `ontapi` método de acesso. Para todos os outros serviços da Web, os usuários devem ter o `http` método de acesso.

  > Você usa os `security login` comandos para gerenciar os métodos de acesso e os métodos de autenticação dos usuários.

- O serviço Web deve ser configurado para permitir a função de controle de acesso do usuário.

  > Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se um firewall estiver ativado, a política de firewall para o LIF a ser usado para serviços da Web deve ser configurada para permitir HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou SVM que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Gerencie o acesso a serviços da Web

Um serviço da Web é um aplicativo que os usuários podem acessar usando HTTP ou HTTPS. O administrador do cluster pode configurar o mecanismo de protocolo da Web, configurar SSL, ativar um serviço da Web e permitir que os utilizadores de uma função acedam a um serviço da Web.

A partir do ONTAP 9.6, são suportados os seguintes serviços Web:

- Infraestrutura do processador de serviço (`spi`)

  Esse serviço torna os arquivos de log, despejo de núcleo e MIB de um nó disponíveis para acesso HTTP ou HTTPS por meio do LIF de gerenciamento de cluster ou de um LIF de gerenciamento de nó. A predefinição é `enabled`.

  Após uma solicitação para acessar os arquivos de log de um nó ou arquivos de despejo de núcleo, o `spi` serviço da Web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó onde os arquivos residem. Não é necessário criar manualmente o ponto de montagem. "

- APIs do ONTAP (`ontapi`)

  Este serviço permite executar APIs do ONTAP para executar funções administrativas com um programa remoto. A predefinição é `enabled`.

  Este serviço pode ser necessário para algumas ferramentas de gerenciamento externas. Por exemplo, se

você usar o System Manager, você deve deixar esse serviço habilitado.

- Descoberta do Data ONTAP (`disco`)

  Este serviço permite que os aplicativos de gerenciamento off-box descubram o cluster na rede. A predefinição é `enabled`.

- Diagnóstico de suporte (`supdiag`)

  Este serviço controla o acesso a um ambiente privilegiado no sistema para auxiliar na análise e resolução de problemas. A predefinição é `disabled`. Você deve habilitar este serviço somente quando direcionado pelo suporte técnico.

- System (`sysmgr`Manager)

  Esse serviço controla a disponibilidade do Gerenciador de sistema, que está incluído no ONTAP. A predefinição é `enabled`. Este serviço é suportado apenas no cluster.

- Atualização do controlador de gerenciamento de placa base (BMC) de firmware (`FW_BMC`)

  Este serviço permite-lhe transferir ficheiros de firmware do BMC. A predefinição é `enabled`.

- Documentação do ONTAP (`docs`)

  Este serviço fornece acesso à documentação do ONTAP. A predefinição é `enabled`.

- APIs RESTful do ONTAP (`docs_api`)

  Este serviço fornece acesso à documentação da API RESTful do ONTAP. A predefinição é `enabled`.

- Carregar e transferir ficheiros (`fud`)

  Este serviço oferece upload e download de arquivos. A predefinição é `enabled`.

- Mensagens do ONTAP (`ontapmsg`)

  Este serviço suporta uma interface de publicação e assinatura, permitindo que você se inscreva em eventos. A predefinição é `enabled`.

- Portal do ONTAP (`portal`)

  Este serviço implementa o gateway em um servidor virtual. A predefinição é `enabled`.

- Interface ONTAP RESTful (`rest`)

  Esse serviço dá suporte a uma interface RESTful que é usada para gerenciar remotamente todos os elementos da infraestrutura do cluster. A predefinição é `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  Este serviço fornece recursos para dar suporte ao provedor de serviços SAML. A predefinição é `enabled`.

- Fornecedor de serviços SAML (`saml-sp`)

Esse serviço oferece serviços como metadados SP e o serviço de asserção ao consumidor para o provedor de serviços. A predefinição é `enabled`.

A partir do ONTAP 9.7, são suportados os seguintes serviços adicionais:

- Arquivos de backup de (`backups`configuração)

  Este serviço permite-lhe transferir ficheiros de cópia de segurança de configuração. A predefinição é `enabled`.

- Segurança do ONTAP (`security`)

  Este serviço suporta o gerenciamento de token CSRF para autenticação aprimorada. A predefinição é `enabled`.

Gerencie o mecanismo de protocolo da Web

Você pode configurar o mecanismo de protocolo da Web no cluster para controlar se o acesso à Web é permitido e quais versões SSL podem ser usadas. Também pode apresentar as definições de configuração do motor de protocolo Web.

Você pode gerenciar o mecanismo de protocolo da Web no nível do cluster das seguintes maneiras:

- Você pode especificar se os clientes remotos podem usar HTTP ou HTTPS para acessar o conteúdo do serviço da Web usando o `system services web modify` comando com o `-external` parâmetro.
- Você pode especificar se SSLv3 deve ser usado para acesso seguro à Web usando o `security config modify` comando com o `-supported-protocol` parâmetro. Por padrão, o SSLv3 está desativado. Transport Layer Security 1,0 (TLSv1,0) está ativado e pode ser desativado se necessário.
- Você pode ativar o modo de conformidade FIPS (Federal Information Processing Standard) 140-2 para interfaces de serviço da Web do plano de controle em todo o cluster.

  Por padrão, o modo de conformidade com o FIPS 140-2 está desativado.

  - **Quando o modo de conformidade com o FIPS 140-2 estiver desativado**, é possível ativar o modo de conformidade com o FIPS 140-2 definindo o `is-fips-enabled` parâmetro como `true` para `security config modify` o comando e, em seguida, usando o `security config show` comando para confirmar o status on-line.
  - **Quando o modo de conformidade com o FIPS 140-2 estiver ativado**
    - A partir do ONTAP 9.11,1, TLSv1, TLSv1,1 e SSLv3 estão desativados e apenas TSLv1,2 e TSLv1,3 permanecem ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
    - Para versões do ONTAP anteriores a 9.11.1, tanto o TLSv1 como o SSLv3 estão desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.

- Você pode exibir a configuração de segurança em todo o cluster usando o `system security config show` comando.

Se o firewall estiver ativado, a política de firewall para a interface lógica (LIF) a ser usada para serviços da Web deve ser configurada para permitir o acesso HTTP ou HTTPS.

Se você usar HTTPS para acesso ao serviço da Web, o SSL para o cluster ou a máquina virtual de armazenamento (SVM) que ofereça o serviço da Web também deverá estar habilitado e fornecer um certificado digital para o cluster ou SVM.

Nas configurações do MetroCluster, as alterações de configuração feitas para o mecanismo de protocolo da Web em um cluster não são replicadas no cluster de parceiros.

Comandos para gerenciar o mecanismo de protocolo da Web

Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web. Use os `system services firewall policy create` comandos e `network interface modify` para permitir que as solicitações de acesso à Web passem pelo firewall.

Se você quiser…	Use este comando…
Configure o mecanismo de protocolo da Web no nível do cluster: • Ative ou desative o mecanismo de protocolo da Web para o cluster • Ative ou desative o SSLv3 para o cluster • Ativar ou desativar a conformidade com o FIPS 140-2 para serviços Web seguros (HTTPS)	`system services web modify`
Exibir a configuração do mecanismo de protocolo da Web no nível do cluster, determinar se os protocolos da Web estão funcionais em todo o cluster e exibir se a conformidade com o FIPS 140-2 está ativada e on-line	`system services web show`
Exibir a configuração do mecanismo de protocolo da Web no nível do nó e a atividade de manipulação de serviços da Web para os nós no cluster	`system services web node show`
Crie uma política de firewall ou adicione um serviço de protocolo HTTP ou HTTPS a uma política de firewall existente para permitir que as solicitações de acesso à Web passem pelo firewall	`system services firewall policy create` Definir o `-service` parâmetro para `http` ou `https` permite que as solicitações de acesso à Web passem pelo firewall.

Se você quiser…	Use este comando…
Associar uma política de firewall a um LIF	`network interface modify` Você pode usar o `-firewall-policy` parâmetro para modificar a política de firewall de um LIF.

Configurar o acesso aos serviços da Web

A configuração do acesso a serviços da Web permite que usuários autorizados usem HTTP ou HTTPS para acessar o conteúdo do serviço no cluster ou em uma máquina virtual de armazenamento (SVM).

Passos

1. Se um firewall estiver ativado, verifique se o acesso HTTP ou HTTPS está configurado na política de firewall para o LIF que será usado para serviços da Web:

   Você pode verificar se um firewall está habilitado usando o `system services firewall show` comando.

   a. Para verificar se HTTP ou HTTPS está configurado na política de firewall, use o `system services firewall policy show` comando.

      Você define o `-service` parâmetro `system services firewall policy create` do comando para `http` ou `https` para ativar a diretiva para oferecer suporte ao acesso à Web.

   b. Para verificar se a política de firewall que suporta HTTP ou HTTPS está associada ao LIF que fornece serviços da Web, use o `network interface show` comando com o `-firewall-policy` parâmetro.

      Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para colocar a política de firewall em vigor para um LIF.

2. Para configurar o mecanismo de protocolo da Web em nível de cluster e tornar o conteúdo do serviço da Web acessível, use o `system services web modify` comando.
3. Se você planeja usar serviços da Web seguros (HTTPS), ative o SSL e forneça informações de certificado digital para o cluster ou SVM usando o `security ssl modify` comando.
4. Para ativar um serviço da Web para o cluster ou SVM, use o `vserver services web modify` comando.

   Repita essa etapa para cada serviço que você deseja habilitar para o cluster ou SVM.

5. Para autorizar uma função a acessar serviços da Web no cluster ou SVM, use o `vserver services web access create` comando.

   A função que você concede acesso já deve existir. Você pode exibir funções existentes usando o `security login role show` comando ou criar novas funções usando o `security login role create` comando.

6. Para uma função que tenha sido autorizada a acessar um serviço da Web, verifique se seus usuários

também estão configurados com o método de acesso correto, verificando a saída do `security login show` comando.

Para acessar o serviço Web da API ONTAP `ontapi`), um usuário deve ser configurado com o `ontapi` método de acesso. Para acessar todos os outros serviços da Web, um usuário deve ser configurado com o `http` método de acesso.

Use o `security login create` comando para adicionar um método de acesso a um usuário.

Comandos para gerenciar serviços da Web

Use os `vserver services web` comandos para gerenciar a disponibilidade de serviços da Web para o cluster ou uma máquina virtual de storage (SVM). Você usa os `vserver services web access` comandos para controlar o acesso de uma função a um serviço da Web.

Se você quiser…	Use este comando…
Configurar um serviço da Web para o cluster ou anSVM: • Ativar ou desativar um serviço Web • Especifique se apenas o HTTPS pode ser usado para acessar um serviço da Web	`vserver services web modify`
Exibir a configuração e a disponibilidade dos serviços da Web para o cluster ou anSVM	`vserver services web show`
Autorizar uma função a acessar um serviço da Web no cluster ou na anSVM	`vserver services web access create`
Exibir as funções autorizadas a acessar serviços da Web no cluster ou no anSVM	`vserver services web access show`
Impedir que uma função acesse um serviço da Web no cluster ou na anSVM	`vserver services web access delete`

Informações relacionadas

"Referência do comando ONTAP"

Comandos para gerenciar pontos de montagem nos nós

O `spi` serviço da Web cria automaticamente um ponto de montagem de um nó para o volume raiz de outro nó, mediante uma solicitação para acessar os arquivos de log ou arquivos centrais do nó. Embora você não precise gerenciar manualmente pontos de montagem, você pode fazê-lo usando os `system node root-mount` comandos.

Se você quiser…	Use este comando…
Crie manualmente um ponto de montagem de um nó para o volume raiz de outro nó	`system node root-mount create` Apenas um único ponto de montagem pode existir de um nó para outro.
Exiba pontos de montagem existentes nos nós do cluster, incluindo o tempo em que um ponto de montagem foi criado e seu estado atual	`system node root-mount show`
Exclua um ponto de montagem de um nó para o volume raiz de outro nó e force as conexões ao ponto de montagem para fechar	`system node root-mount delete`

Informações relacionadas

"Referência do comando ONTAP"

Gerenciar SSL

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM). O protocolo SSL melhora a segurança do acesso à Web usando um certificado digital para estabelecer uma conexão criptografada entre um servidor da Web e um navegador.

Você pode gerenciar SSL para o cluster ou uma máquina virtual de armazenamento (SVM) das seguintes maneiras:

- Ativar SSL
- Gerar e instalar um certificado digital e associá-lo ao cluster ou SVM
- Exibindo a configuração SSL para ver se o SSL foi ativado e, se disponível, o nome do certificado SSL
- Configuração de políticas de firewall para o cluster ou SVM, para que as solicitações de acesso à Web possam passar
- Definir quais versões SSL podem ser usadas
- Restringindo o acesso apenas a solicitações HTTPS para um serviço da Web

Comandos para gerenciar SSL

Use os `security ssl` comandos para gerenciar o protocolo SSL para o cluster ou uma máquina virtual de armazenamento (SVM).

Se você quiser…	Use este comando…
Ative o SSL para o cluster ou um SVM e associe um certificado digital a ele	`security ssl modify`
Exiba a configuração SSL e o nome do certificado para o cluster ou um SVM	`security ssl show`

Solucionar problemas de acesso ao serviço da Web

Os erros de configuração causam problemas de acesso ao serviço da Web. Você pode resolver os erros garantindo que o LIF, a política de firewall, o mecanismo de protocolo da Web, os serviços da Web, os certificados digitais e a autorização de acesso do usuário estejam configurados corretamente.

A tabela a seguir ajuda a identificar e tratar erros de configuração do serviço da Web:

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
O navegador da Web retorna um `unable to connect` erro ou `failure to establish a connection` quando você tenta acessar um serviço da Web.	Seu LIF pode estar configurado incorretamente.	Certifique-se de que você pode fazer ping no LIF que fornece o serviço da Web. Você usa o `network ping` comando para fazer ping em um LIF. Para obter informações sobre a configuração de rede, consulte o *Network Management Guide*.
O firewall pode estar configurado incorretamente.	Certifique-se de que uma política de firewall esteja configurada para suportar HTTP ou HTTPS e que a política esteja atribuída ao LIF que fornece o serviço da Web. Você usa os `system services firewall policy` comandos para gerenciar políticas de firewall. Você usa o `network interface modify` comando com o `-firewall-policy` parâmetro para associar uma política a um LIF.	Seu mecanismo de protocolo da Web pode estar desativado.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o mecanismo de protocolo da Web está ativado para que os serviços da Web estejam acessíveis. Você usa os `system services web` comandos para gerenciar o mecanismo de protocolo da Web para o cluster.	Seu navegador retorna um `not found` erro quando você tenta acessar um serviço da Web.	O serviço da Web pode estar desativado.
Certifique-se de que cada serviço Web ao qual você deseja permitir acesso esteja ativado individualmente. Você usa o `vserver services web modify` comando para habilitar um serviço da Web para acesso.	O navegador da Web não consegue fazer login em um serviço da Web com o nome de conta e a senha de um usuário.	O utilizador não pode ser autenticado, o método de acesso não está correto ou o utilizador não está autorizado a aceder ao serviço Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que a conta de utilizador existe e está configurada com o método de acesso e o método de autenticação corretos. Além disso, certifique-se de que a função do utilizador está autorizada a aceder ao serviço Web. Você usa os `security login` comandos para gerenciar contas de usuário e seus métodos de acesso e métodos de autenticação. Acessar o serviço da Web da API do ONTAP requer o `ontapi` método de acesso. O acesso a todos os outros serviços da Web requer o `http` método de acesso. Você usa os `vserver services web access` comandos para gerenciar o acesso de uma função a um serviço da Web.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que sua conexão foi interrompida.	Talvez você não tenha o SSL ativado no cluster ou na máquina virtual de armazenamento (SVM) que fornece o serviço da Web.

Este problema de acesso…	Ocorre devido a este erro de configuração…	Para resolver o erro…
Certifique-se de que o cluster ou SVM tenha SSL habilitado e que o certificado digital seja válido. Você usa os `security ssl` comandos para gerenciar a configuração SSL para servidores HTTP e o `security certificate show` comando para exibir informações de certificado digital.	Você se coneta ao serviço da Web com HTTPS e o navegador da Web indica que a conexão não é confiável.	Você pode estar usando um certificado digital autoassinado.

Verifique a identidade de servidores remotos usando certificados

Verifique a identidade de servidores remotos usando a visão geral de certificados

O ONTAP suporta recursos de certificado de segurança para verificar a identidade de servidores remotos.

O software ONTAP permite conexões seguras usando esses recursos e protocolos de certificado digital:

- O OCSP (Online Certificate Status Protocol) valida o status de solicitações de certificados digitais de serviços ONTAP usando conexões SSL e TLS (Transport Layer Security). Esta funcionalidade está desativada por predefinição.
- Um conjunto padrão de certificados raiz confiáveis é incluído no software ONTAP.
- Os certificados KMIP (Key Management Interoperability Protocol) permitem a autenticação mútua de um cluster e de um servidor KMIP.

Verifique se os certificados digitais são válidos usando OCSP

A partir do ONTAP 9.2, o protocolo OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS (Transport Layer Security) recebam status de certificado digital quando o OCSP está ativado. Você pode ativar ou desativar verificações de status do certificado OCSP para aplicativos específicos a qualquer momento. Por padrão, a verificação do status do certificado OCSP está desativada.

O que você vai precisar

Você precisa de acesso avançado ao nível de privilégio para executar esta tarefa.

Sobre esta tarefa

O OCSP suporta as seguintes aplicações:

- AutoSupport
- Sistema de Gestão de Eventos (EMS)
- LDAP em TLS
- Key Management Interoperability Protocol (KMIP)
- Registo de auditoria
- FabricPool
- SSH (começando com ONTAP 9.13,1)

Passos

1. Defina o nível de privilégio como avançado: `set -privilege advanced`.
2. Para ativar ou desativar as verificações de status do certificado OCSP para aplicativos ONTAP específicos, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para alguns aplicativos sejam…	Use o comando…
Ativado	`security config ocsp enable -app app name`
Desativado	`security config ocsp disable -app app name`

O seguinte comando permite o suporte OCSP para AutoSupport e EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Quando o OCSP está ativado, o aplicativo recebe uma das seguintes respostas:

- Bom - o certificado é válido e a comunicação prossegue.
- Revogado - o certificado é considerado permanentemente como não fidedigno pela Autoridade de Certificação de emissão e a comunicação não procede.
- Desconhecido - o servidor não tem nenhuma informação de estado sobre o certificado e a comunicação não consegue prosseguir.
- As informações do servidor OCSP estão ausentes no certificado - o servidor funciona como se o OCSP estivesse desativado e continua com a comunicação TLS, mas nenhuma verificação de status ocorre.
- Sem resposta do servidor OCSP - o aplicativo não consegue prosseguir.

3. Para ativar ou desativar as verificações de status do certificado OCSP para todos os aplicativos que usam comunicações TLS, use o comando apropriado.

Se você quiser que as verificações de status do certificado OCSP para todos os aplicativos sejam…	Use o comando…
Ativado	`security config ocsp enable -app all`
Desativado	`security config ocsp disable -app all`

Quando ativado, todos os aplicativos recebem uma resposta assinada, significando que o certificado especificado é bom, revogado ou desconhecido. No caso de um certificado revogado, o pedido não irá prosseguir. Se o aplicativo não receber uma resposta do servidor OCSP ou se o servidor estiver inacessível, o aplicativo não conseguirá prosseguir.

4. Use o `security config ocsp show` comando para exibir todos os aplicativos que suportam OCSP e seu status de suporte.

```
cluster::*> security config ocsp show
         Application                     OCSP Enabled?
         --------------------            ---------------------
         autosupport                     false
         audit_log                       false
         fabricpool                      false
         ems                             false
         kmip                            false
         ldap_ad                         true
         ldap_nis_namemap                true
         ssh                             true

         8 entries were displayed.
```

Exibir certificados padrão para aplicativos baseados em TLS

A partir do ONTAP 9.2, o ONTAP fornece um conjunto padrão de certificados raiz confiáveis para aplicativos ONTAP usando a Segurança da camada de Transporte (TLS).

O que você vai precisar

Os certificados padrão são instalados somente no SVM do administrador durante sua criação ou durante uma atualização para o ONTAP 9.2.

Sobre esta tarefa

Os aplicativos atuais que atuam como cliente e exigem validação de certificado são AutoSupport, EMS, LDAP, Registro de auditoria, FabricPool e KMIP.

Quando os certificados expiram, é invocada uma mensagem EMS que solicita ao utilizador que elimine os certificados. Os certificados padrão só podem ser excluídos no nível avançado de privilégio.

> A exclusão dos certificados padrão pode resultar em alguns aplicativos do ONTAP não funcionarem como esperado (por exemplo, AutoSupport e Registro de auditoria).

Passo

1. Você pode exibir os certificados padrão instalados no SVM do administrador usando o comando show do certificado de segurança:

   `security certificate show -vserver –type server-ca`

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

Autentique mutuamente o cluster e um servidor KMIP

Autenticando mutuamente o cluster e uma visão geral do servidor KMIP

Autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP (Key Management Interoperability Protocol), permite que o gerenciador de chaves se comunique com o cluster usando KMIP em SSL. Você o faz quando um aplicativo ou uma determinada funcionalidade (por exemplo, a funcionalidade criptografia de armazenamento) exige chaves seguras para fornecer acesso seguro aos dados.

Gerar uma solicitação de assinatura de certificado para o cluster

Você pode usar o comando certificado de segurança `generate-csr` para gerar uma solicitação de assinatura de certificado (CSR). Depois de processar sua solicitação, a autoridade de certificação (CA) envia o certificado digital assinado.

O que você vai precisar

Você deve ser um administrador de cluster ou um administrador de SVM para executar essa tarefa.

Passos

1. Gerar um CSR:

   `security certificate generate-csr -common-name *FQDN_or_common_name* -size`

512|1024|1536|2048 -country *country* -state *state* -locality *locality* -organization *organization* -unit *unit* -email-addr *email_of_contact* -hash -function SHA1|SHA256|MD5

Para obter a sintaxe completa do comando, consulte as páginas man.

O comando a seguir cria uma CSR com uma chave privada de 2.048 bits gerada pela função de hash SHA256 para uso pelo grupo Software no departamento DE TI de uma empresa cujo nome comum personalizado é server1.companyname.com, localizada em Sunnyvale, Califórnia, EUA. O endereço de e-mail do administrador de Contatos do SVM é web@example.com. O sistema apresenta a CSR e a chave privada na saída.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Copie a solicitação de certificado da saída CSR e, em seguida, envie-a em formato eletrônico (como e-mail) para uma CA de terceiros confiável para assinatura.

   Após processar sua solicitação, a CA envia o certificado digital assinado. Você deve manter uma cópia da chave privada e do certificado digital assinado pela CA.

Instale um certificado de servidor assinado pela CA para o cluster

Para permitir que um servidor SSL autentique o cluster ou a máquina virtual de armazenamento (SVM) como um cliente SSL, instale um certificado digital com o tipo de cliente no cluster ou SVM. Em seguida, você fornece o certificado cliente-CA ao administrador do servidor SSL para instalação no servidor.

O que você vai precisar

Você já deve ter instalado o certificado raiz do servidor SSL no cluster ou SVM com o `server-ca` tipo de certificado.

Passos

1. Para usar um certificado digital autoassinado para autenticação de cliente, use o `security certificate create` comando com o `type client` parâmetro.
2. Para usar um certificado digital assinado pela CA para autenticação de cliente, execute as seguintes etapas:

   a. Gere uma solicitação de assinatura de certificado digital (CSR) usando o comando de certificado de segurança `generate-csr`.

      O ONTAP exibe a saída CSR, que inclui uma solicitação de certificado e uma chave privada, e lembra que você deve copiar a saída para um arquivo para referência futura.

   b. Envie a solicitação de certificado da saída CSR em um formulário eletrônico (como e-mail) para uma CA confiável para assinatura.

      Você deve manter uma cópia da chave privada e do certificado assinado pela CA para referência futura.

   Após processar sua solicitação, a CA envia o certificado digital assinado.

   a. Instale o certificado assinado pela CA usando o `security certificate install` comando com o `-type client` parâmetro.
   b. Digite o certificado e a chave privada quando você for solicitado e pressione **Enter**.
   c. Insira quaisquer certificados raiz ou intermediários adicionais quando for solicitado e pressione **Enter**.

      Você instala um certificado intermediário no cluster ou SVM se uma cadeia de certificados que começa na CA raiz confiável e termina com o certificado SSL emitido para você estiver faltando os certificados intermediários. Um certificado intermediário é um certificado subordinado emitido pela raiz confiável especificamente para emitir certificados de servidor de entidade final. O resultado é uma cadeia de certificados que começa na CA raiz confiável, passa pelo certificado intermediário e termina com o certificado SSL emitido para você.

3. Forneça o `client-ca` certificado do cluster ou SVM ao administrador do servidor SSL para instalação no servidor.

   O comando show do certificado de segurança com os `-instance` parâmetros e `-type client-ca` exibe as `client-ca` informações do certificado.

Instale um certificado de cliente assinado pela CA para o servidor KMIP

O subtipo de certificado do Key Management Interoperability Protocol (KMIP) (o parâmetro -subtype kmip-cert), juntamente com os tipos cliente e servidor-CA, especifica que o certificado é usado para autenticar mutuamente o cluster e um gerenciador de chaves externo, como um servidor KMIP.

Sobre esta tarefa

Instale um certificado KMIP para autenticar um servidor KMIP como um servidor SSL no cluster.

Passos

1. Use o `security certificate install` comando com os `-type server-ca` parâmetros e `-subtype kmip-cert` para instalar um certificado KMIP para o servidor KMIP.
2. Quando lhe for solicitado, introduza o certificado e, em seguida, prima Enter.

   O ONTAP lembra que você deve manter uma cópia do certificado para referência futura.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Controle de acesso baseado em atributos

Controle de acesso baseado em atributos com ONTAP

É possível implementar RBAC aprimorado com atributos e controle de acesso baseado em atributos (ABAC) usando o ONTAP. O ONTAP fornece várias abordagens que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFS 4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

O controle de acesso baseado em atributos (ABAC) é um método sofisticado para gerenciar direitos de acesso que considera atributos do usuário, atributos de recursos e condições ambientais. O Instituto Nacional

de padrões e tecnologia (NIST) estabeleceu um padrão para a ABAC, fornecendo uma estrutura para sua implementação segura e consistente.

A partir do ONTAP 9.12,1, você pode configurar o ONTAP com rótulos de segurança NFSv4,2 e atributos estendidos (XATTRS) para que ele possa ser integrado a uma identidade de controle de acesso baseado em função (RBAC) e controle de acesso baseado em atributos (ABAC). Essa integração permite que o ONTAP acesse softwares de controle que são categorizados como uma solução de gerenciamento de dados compatível com ABAC NIST, oferecendo uma abordagem robusta e avançada para gerenciar direitos de acesso em ambientes complexos, incluindo ponto de aplicação de políticas (PEP), ponto de Decisão de políticas (PDP) e políticas que consideram atributos associados ao usuário, ao recurso e ao ambiente.

A integração do software NetApp ONTAP com atributos estendidos (XATTRS) e Controle de Acesso baseado em Atributo (ABAC) está alinhada com as diretrizes estabelecidas na publicação especial do NIST 800-162, garantindo o cumprimento das normas NIST para implementação da ABAC. O uso de rótulos de segurança NFS 4,2 e XATTRS permite a associação de atributos definidos pelo usuário com arquivos, atendendo aos requisitos do padrão NIST ABAC para considerar atributos de recursos nas decisões de controle de acesso. O PEP e PDP do software ABAC estão alinhados com o requisito do padrão NIST ABAC para esses componentes no processo de controle de acesso. A capacidade de definir políticas complexas que considerem vários atributos e condições alinha-se ao requisito do padrão NIST ABAC para controle de acesso baseado em políticas.

Informações relacionadas

- "Abordagens para ABAC com ONTAP"
- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Abordagens para ABAC com ONTAP

O ONTAP fornece abordagens variadas que um cliente pode usar para obter ABAC no nível do arquivo, incluindo NFSv4,2 e XATTRS rotulados usando NFS e SMB/CIFS.

Identificada como NFSv4,2

A partir do ONTAP 9.9,1, o recurso NFSv4,2 chamado NFS é suportado.

O NFS rotulado é uma maneira de gerenciar o acesso granular a arquivos e pastas usando rótulos SELinux e Controle de Acesso obrigatório (MAC). Esses rótulos MAC são armazenados com arquivos e pastas e funcionam em conjunto com permissões UNIX e ACLs NFSv4.x.

O suporte para NFS rotulado significa que a ONTAP agora reconhece e compreende as configurações de rótulo SELinux do cliente NFS. O NFS rotulado é coberto pela RFC-7204.

Os casos de uso do rotulado NFSv4,2 incluem o seguinte:

- MAC rotulagem de imagens de máquina virtual (VM)
- Classificação de segurança de dados para o setor público (segredo, segredo principal e outras classificações)
- Conformidade de segurança
- Linux sem disco

Ative o rótulo NFSv4,2

Você pode ativar ou desativar o NFS rotulado com a seguinte opção de privilégio avançado:

```
[-v4.2-seclabel {enabled|disabled}] - NFSV4.2 Security Label Support
(privilege: advanced)
```

Este parâmetro é opcional e a predefinição é `disabled`.

Modos de aplicação para o rótulo NFSv4,2

A partir do ONTAP 9.9,1, o ONTAP suporta os seguintes modos de aplicação:

- **Modo de servidor limitado**: O ONTAP não pode impor as etiquetas, mas pode armazená-las e transmiti-las.

  A capacidade de alterar rótulos MAC também depende do cliente para impor.

- **Modo convidado**: Se o cliente não estiver identificado como NFS-Aware (v4,1 ou inferior), os rótulos MAC não serão transmitidos.

Atualmente, o ONTAP não suporta o modo completo (armazenamento e aplicação de etiquetas MAC).

Exemplo de configuração do rotulado NFSv4,2

A configuração de exemplo a seguir demonstra conceitos usando o Red Hat Enterprise Linux versão 9,3 (Plow).

O usuário `jrsmith`, criado com base nas credenciais de John R. Smith, tem o seguinte Privileges de conta:

- Nome de utilizador `jrsmith`
- Privileges `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

Há duas funções: A conta de administrador que é um usuário privilegiado e usuário `jrsmith`, conforme descrito na seguinte tabela MLS Privileges:

Usuários	Função	Tipo	Níveis
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

Neste ambiente de exemplo, o usuário `jrsmith` tem acesso a arquivos nos níveis `s0 s3` de . Podemos aprimorar as classificações de segurança existentes, conforme descrito abaixo, para garantir que os administradores não tenham acesso a dados específicos do usuário.

- s0: dados de usuário do administrador de privilégios
- s0: dados não classificados

- s1: confidencial
- s2: dados secretos
- s3: dados secretos principais

Siga as políticas de segurança da sua organização

Exemplo de etiqueta de segurança NFSv4,2 com MCS

Além do MLS (Multi-Level Security), outro recurso chamado MCS (Multi-Category Security) permite definir categorias como projetos.

Etiqueta de segurança NFS	Valor
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Atributos estendidos (XATTRS)

A partir do ONTAP 9.12,1, o ONTAP suporta xattrs. Os xattrs permitem que os metadados sejam associados a arquivos e diretórios além do que é fornecido pelo sistema, como listas de controle de acesso (ACLs) ou atributos definidos pelo usuário.

Para implementar o xattrs, você pode usar `setfattr` e `getfattr` utilitários de linha de comando no Linux para gerenciar xattrs de objetos de sistema de arquivos. Essas ferramentas fornecem uma maneira poderosa de gerenciar metadados adicionais para arquivos e diretórios. Eles devem ser usados com cuidado, pois o uso inadequado pode levar a comportamentos inesperados ou problemas de segurança. Consulte sempre as `setfattr` páginas de manual e `getfattr` ou outra documentação fiável para obter instruções de utilização detalhadas.

Quando o xattrs está habilitado em um sistema de arquivos ONTAP, os usuários podem definir, modificar e recuperar atributos arbitrários em arquivos. Esses atributos podem ser usados para armazenar informações adicionais sobre o arquivo que não é capturado pelo conjunto padrão de atributos de arquivo, como informações de controle de acesso.

Requisitos para usar xattrs em ONTAP

- Red Hat Enterprise Linux 8,4 ou posterior
- Ubuntu 22,04 ou posterior
- Cada arquivo pode ter até 128 xattrs
- as chaves xattr estão limitadas a 255 bytes
- O tamanho combinado da chave ou do valor é de 1.729 bytes por xattr
- Diretórios e arquivos podem ter xattrs
- Para definir e recuperar xattrs `w`, ou bits de modo de gravação devem estar ativados para o usuário e grupo

Casos de uso para xattrs

Os xattrs são utilizados dentro do namespace do usuário e não carregam nenhum significado intrínseco para o próprio ONTAP. Em vez disso, suas aplicações práticas são determinadas e gerenciadas exclusivamente pelo aplicativo do lado do cliente que interage com o sistema de arquivos.

exemplos de casos de uso do xattr:

- Gravando o nome do aplicativo responsável pela criação de um arquivo.
- Manter uma referência à mensagem de e-mail a partir da qual um arquivo foi obtido.
- Estabelecendo uma estrutura de categorização para organizar objetos de arquivo.
- Rotular arquivos com o URL de sua fonte de download original.

Comandos para gerenciar xattrs

- `setfattr`: Define um atributo estendido de um arquivo ou diretório:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Exemplo de comando:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr`: Recupera o valor de um atributo estendido específico ou lista todos os atributos estendidos de um arquivo ou diretório:

  Atributo específico:
  `getfattr -n <attribute_name> <file or directory name>`

  Todos os atributos:
  `getfattr <file or directory name>`

  Exemplo de comando:

  ```
  getfattr -n user.comment example.txt
  ```

xattr	Valor
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

Permissões de usuário com ACE para atributos estendidos

Uma entrada de controle de acesso (ACE) é um componente dentro de uma lista de controle de acesso (ACL) que define os direitos de acesso ou permissões concedidos a um usuário individual ou a um grupo de usuários para um recurso específico, como um arquivo ou diretório. Cada ACE especifica o tipo de acesso permitido ou negado e está associado a um responsável de segurança específico (identidade de usuário ou grupo).

Tipo de ficheiro	Recuperar xattr	Definir xattrs
Ficheiro	R	A, W, T
Diretório	R	T

Explicação das permissões necessárias para o xattrs:

Retrieve xattr: As permissões necessárias para um usuário ler os atributos estendidos de um arquivo ou diretório. O "R" significa que a permissão de leitura é necessária. * Definir xattrs*: As permissões necessárias para modificar ou definir os atributos estendidos. "A", "W" e "T" representam diferentes exemplos de permissões, como anexar, escrever e uma permissão específica relacionada ao xattrs. **Files**: Os usuários precisam anexar, escrever e potencialmente uma permissão especial relacionada ao xattrs para definir atributos estendidos. **Diretórios**: Uma permissão específica "T" é necessária para definir atributos estendidos.

Suporte ao protocolo SMB/CIFS para xattrs

O suporte da ONTAP para o protocolo SMB/CIFS se estende ao tratamento abrangente de xattrs, que são parte integrante dos metadados de arquivos em ambientes Windows. Os atributos estendidos permitem que usuários e aplicativos armazenem informações adicionais além do conjunto padrão de atributos de arquivo, como detalhes do autor, descritores de segurança personalizados ou dados específicos do aplicativo. A implementação SMB/CIFS da ONTAP garante que esses xatrs sejam totalmente suportados, permitindo uma integração perfeita com serviços e aplicativos do Windows que dependem desses metadados para a funcionalidade e aplicação de políticas.

Quando os arquivos são acessados ou transferidos por compartilhamentos SMB/CIFS gerenciados pelo ONTAP, o sistema preserva a integridade dos xatrs, garantindo que todos os metadados sejam mantidos e permaneçam consistentes. Isso é particularmente importante para manter as configurações de segurança e para aplicativos que dependem do xattrs para configuração ou operação. O manuseio robusto de xatrs da ONTAP no contexto SMB/CIFS garante que o compartilhamento de arquivos entre diferentes plataformas e ambientes seja confiável e seguro, proporcionando aos usuários uma experiência perfeita e aos administradores a garantia de que as políticas de governança de dados são mantidas. Seja para colaboração, arquivamento de dados ou conformidade, a atenção da ONTAP aos xatrs em compartilhamentos SMB/CIFS representa seu compromisso com a excelência no gerenciamento de dados e interoperabilidade em ambientes de sistemas operacionais mistos.

Ponto de aplicação da política (PEP) e ponto de decisão da política (PDP) na ABAC

Em um sistema de controle de acesso baseado em atributos (ABAC), o ponto de aplicação de políticas (PEP) e o PDP (Policy Decision Point) desempenham papéis cruciais. O PEP é responsável pela aplicação de políticas de controle de acesso, enquanto o PDP toma a decisão de conceder ou negar acesso com base nas políticas.

No contexto do snippet de código Python fornecido, o próprio script atua como um PEP. Ele impõe a decisão de controle de acesso, quer concedendo acesso ao arquivo abrindo-o e lendo seu conteúdo ou negando acesso através da criação de um `PermissionError`.

O PDP, por outro lado, faria parte do sistema SELinux subjacente. Quando o script tenta abrir o arquivo com um contexto específico do SELinux, o sistema SELinux verifica suas políticas para decidir se deseja conceder ou negar acesso. Esta decisão é então aplicada pelo script.

Abaixo está um exemplo detalhado de como esse código funciona em um ambiente ABAC:

1. O script define o contexto SELinux para `jrsmith` contexto usando a `selinux.setcon()` função. Isso é equivalente a `jrsmith` tentar acessar o arquivo.
2. O script tenta abrir o arquivo. É aqui que o PEP entra em jogo.
3. O sistema SELinux verifica suas políticas para ver se `jrsmith` (ou mais especificamente, um usuário com `jrsmith` contexto SELinux) tem permissão para acessar o arquivo. Esta é a função do PDP.
4. Se `jrsmith` for permitido acessar o arquivo, o sistema SELinux permite que o script abra o arquivo e o

script leia e imprima o conteúdo do arquivo.

5. Se `jrsmith` não for permitido acessar o arquivo, o sistema SELinux impede que o script abra o arquivo e o script gera um `PermissionError`.
6. O script restaura o contexto original do SELinux para garantir que a alteração temporária do contexto não afete outras operações.

Usando Python, o código para obter o contexto é mostrado abaixo onde o caminho do arquivo variável é o documento que deve ser verificado:

```
#Get the current context

context = selinux.getfilecon(file_path)[1]
```

Clonagem de ONTAP e SnapMirror

As tecnologias de clonagem e SnapMirror da ONTAP foram projetadas para fornecer recursos de replicação e clonagem de dados eficientes e confiáveis, garantindo que todos os aspetos dos dados de arquivos, incluindo atributos estendidos (xattrs), sejam preservados e transferidos junto com o arquivo. Os xattrs são críticos, pois armazenam metadados adicionais associados a um arquivo, como rótulos de segurança, informações de controle de acesso e dados definidos pelo usuário, essenciais para manter o contexto e integridade do arquivo.

Quando um volume é clonado usando a tecnologia FlexClone da ONTAP, uma réplica gravável exata do volume é criada. Esse processo de clonagem é instantâneo e eficiente em espaço, e inclui todos os dados e metadados de arquivos, garantindo que os xatrs sejam totalmente replicados. Da mesma forma, o SnapMirror garante que os dados sejam espelhados para um sistema secundário com fidelidade total. Isso inclui xattrs, que são cruciais para aplicativos que dependem desses metadados para funcionar corretamente.

Ao incluir xatrs nas operações de clonagem e replicação, o NetApp ONTAP garante que todo o conjunto de dados, com todas as suas características, esteja disponível e consistente em sistemas de storage primário e secundário. Essa abordagem abrangente ao gerenciamento de dados é vital para organizações que exigem proteção de dados consistente, recuperação rápida e adesão a padrões regulatórios e de conformidade. Ele também simplifica o gerenciamento de dados em diferentes ambientes, seja no local ou na nuvem, fornecendo aos usuários a confiança de que seus dados estão completos e inalterados durante esses processos.

NFSv4,2 as etiquetas de segurança têm as ressalvas definidas no 2.

Exemplos de controle do acesso aos dados

A seguinte entrada de exemplo para dados armazenados no cert PKI de John R Smith mostra como a abordagem do NetApp pode ser aplicada a um arquivo e fornecer controle de acesso refinado.

Esses exemplos são para fins ilustrativos, e é responsabilidade do governo definir quais metadados são rótulos de segurança NFSv4,2 e xattrs. Detalhes sobre a atualização e retenção de rótulos são omitidos para simplificar.

Chave	Valor
EntitySecurityMark	t:S01 NÃO CLASSIFICADO

Chave	Valor

Informações	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

especificação	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

Chave	Valor

briefings	[
	{
	"value": "ABC1000"
	},
	{
	"value": "DEF1001"
	},
	{
	"value": "EFG2000"
	}
	]

CitizensaStatus	{
	"value": "US"
	}

folgas	[
	{
	"value": "TS"
	},
	{
	"value": "S"
	},
	{
	"value": "C"
	},
	{
	"value": "U"
	}
	]

CountryOfAffiliations	[
	{
	"value": "USA"
	}
	]

Chave	Valor

DigitalIdentifier	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

It is always	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

Tipo de entidade	{
	"value": "GOV"
	}

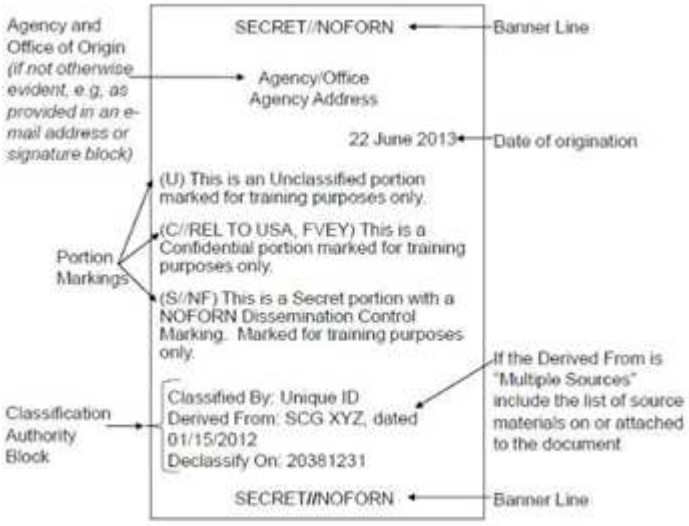
FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

Esses direitos PKI mostram os detalhes de acesso de John R. Smith, incluindo acesso por tipo de dados e atribuição.

Se John R. Smith criou e salvou um documento chamado *"sample_analysis.doc"*, de acordo com as questões relevantes de orientação política, o usuário adicionaria as marcas apropriadas de banner e porção, agência e escritório de origem e bloco de autoridade de classificação adequado com base na classificação do documento, conforme mostrado na imagem a seguir. Estes metadados ricos só são compreensíveis depois de

terem sido digitalizados pelo processamento de linguagem Natural (PNL) e terem regras aplicadas para fazer sentido a partir das marcações. Ferramentas como a classificação NetApp BlueXP podem fazer isso, mas são menos eficientes para decisões de controle de acesso, porque exigem permissão para olhar dentro do documento.

Marcação da parte do documento CAPCO não classificada



Em cenários em que os metadados IC-TDF são armazenados separadamente do arquivo, o NetApp defende uma camada adicional de controle de acesso refinado. Isso envolve o armazenamento de informações de controle de acesso tanto no nível de diretório quanto em associação com cada arquivo. Como exemplo, considere as seguintes tags vinculadas a um arquivo:

- NFSv4,2 rótulos de segurança: Utilizados para tomar decisões de segurança
- Xattrs: Fornecer informações complementares pertinentes ao arquivo e aos requisitos do programa organizacional

Os pares chave-valor a seguir são exemplos de metadados que podem ser armazenados como xattrs e oferecer informações detalhadas sobre o criador do arquivo e classificações de segurança associadas. Esses metadados podem ser aproveitados por aplicativos clientes para tomar decisões de acesso informado e organizar arquivos de acordo com os padrões e requisitos organizacionais.

Chave	Valor
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Chave	Valor

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Chave	Valor
user.geo_point	[-78.7941, 35.7956]

```
    }
}
```

Auditoria de alterações em rótulos

A auditoria de alterações em rótulos de segurança xattrs ou NFS é um aspeto crítico do gerenciamento e da segurança do sistema de arquivos. As ferramentas padrão de auditoria do sistema de arquivos permitem o monitoramento e o Registro de todas as alterações em um sistema de arquivos, incluindo modificações em atributos estendidos e rótulos de segurança.

Em ambientes Linux, o `auditd` daemon é comumente usado para estabelecer auditoria para eventos de sistema de arquivos. Ele permite que os administradores configurem regras para observar chamadas específicas do sistema relacionadas a alterações xattr, como `setxattr`, `lsetxattr` e `fsetxattr` para definir atributos e, `lremovexattr` e `fremovexattr` para `removexattr` remover atributos.

O ONTAP FPolicy amplia esses recursos fornecendo uma estrutura robusta para monitoramento e controle em tempo real de operações de arquivos. O FPolicy pode ser configurado para oferecer suporte a vários eventos xattr, oferecendo controle granular sobre as operações de arquivos e a capacidade de aplicar políticas abrangentes de gerenciamento de dados.

Para usuários que utilizam xattrs, especialmente em ambientes NFSv3 e NFSv4, apenas determinadas combinações de operações de arquivos e filtros são suportadas para monitoramento. A lista de combinações de filtros e operação de arquivos compatíveis para monitoramento FPolicy de eventos de acesso a arquivos NFSv3 e NFSv4 é detalhada abaixo:

Operações de arquivos compatíveis	Filtros suportados
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

Exemplo de um snippet de log auditd para uma operação setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Ativar o ONTAP FPolicy para usuários que trabalham com o xattrs fornece uma camada de visibilidade e controle essencial para manter a integridade e a segurança do sistema de arquivos. Ao aproveitar os recursos avançados de monitoramento da FPolicy, as organizações podem garantir que todas as alterações aos xattrs

sejam rastreadas, auditadas e alinhadas com seus padrões de segurança e conformidade. Essa abordagem proativa para o gerenciamento do sistema de arquivos é por isso que habilitar o ONTAP FPolicy é altamente recomendado para qualquer organização que queira aprimorar suas estratégias de governança e proteção de dados.

Integração com software de controle de acesso e identidade ABAC

Para aproveitar totalmente os recursos do controle de acesso baseado em atributos (ABAC), o ONTAP pode se integrar com um software de gerenciamento de identidade e acesso orientado para ABAC.

> Em paralelo a este conteúdo, o NetApp tem uma implementação de referência usando GreyBox. Uma suposição para este conteúdo é que os serviços de identidade, autenticação e acesso do governo incluem, no mínimo, um ponto de aplicação da Política (PEP) e um ponto de Decisão da Política (PDP) que atuam como intermediários para o acesso ao sistema de arquivos.

Em um ambiente prático, uma organização empregaria uma mistura de rótulos de segurança NFS e xattrs. Eles são usados para representar uma variedade de metadados, incluindo classificação, segurança, aplicativo e conteúdo, que são todos fundamentais para tomar decisões ABAC. O XATTR, por exemplo, pode ser usado para armazenar os atributos de recursos que o PDP usa para seu processo de tomada de decisão. Um atributo pode ser definido para representar o nível de classificação de um arquivo (por exemplo, "não classificado", "confidencial", "segredo" ou "segredo superior"). O PDP poderia então utilizar este atributo para impor uma política que restringe os utilizadores a aceder apenas a ficheiros que tenham um nível de classificação igual ou inferior ao nível de autorização.

Exemplo de fluxo de processo para ABAC

1. O usuário apresenta credenciais (por exemplo, PKI, OAuth, SAML) para acesso ao sistema ao PEP e obtém resultados do PDP.

   A função do PEP é intercetar a solicitação de acesso do usuário e encaminhá-la para o PDP.

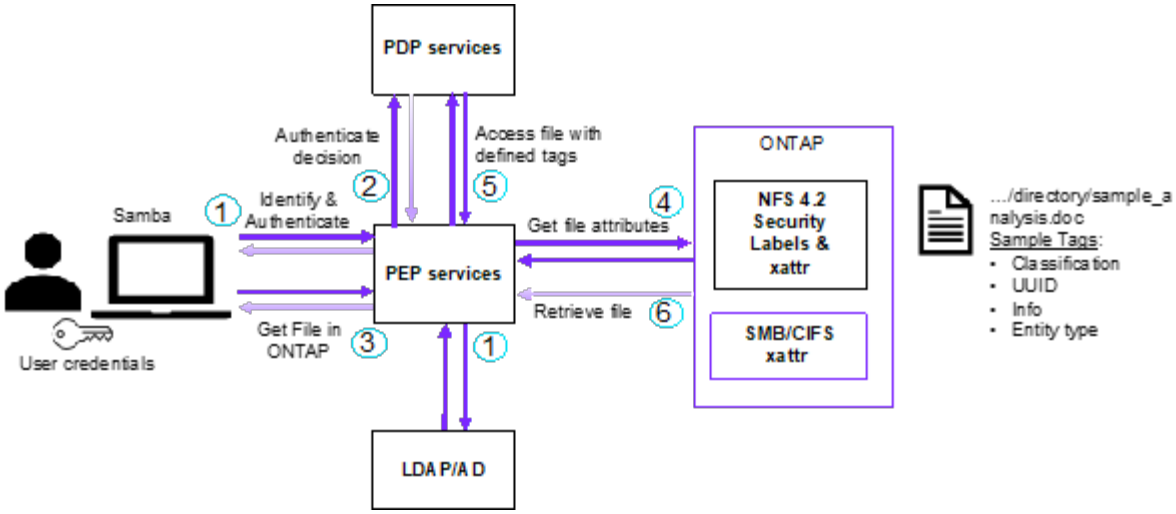
2. Em seguida, o PDP avalia essa solicitação em relação às políticas estabelecidas da ABAC.

   Essas políticas consideram vários atributos relacionados ao usuário, ao recurso em questão e ao ambiente circundante. Com base nessas políticas, o PDP toma uma decisão de acesso para permitir ou negar e, em seguida, comunica essa decisão de volta ao PEP.

   PDP fornece política para PEP para fazer cumprir. O PEP então impõe essa decisão, concedendo ou negando o pedido de acesso do usuário conforme decisão do PDP.

3. Após uma solicitação bem-sucedida, o usuário solicita um arquivo armazenado no ONTAP (AFF, AFF-C, por exemplo).
4. Se a solicitação for bem-sucedida, o PEP obtém tags de controle de acesso de grãos finos do documento.
5. PEP solicita política para o utilizador com base nos certificados desse utilizador.
6. O PEP toma uma decisão com base na política e nas tags se o usuário tiver acesso ao arquivo e permitir que o usuário recupere o arquivo.

> O acesso real pode ser feito usando tokens que não são protegidos.



Informações relacionadas

- "NFS no NetApp ONTAP: Guia de práticas recomendadas e implementação"
- Pedido de comentários (RFC)
  - RFC 2203: Especificação do protocolo RPCSEC_GSS
  - RFC 3530: Protocolo NFS (Network File System) versão 4

Informações sobre direitos autorais

Informações sobre marcas comerciais