Gerenciar a autenticação do administrador e o RBAC

ONTAP 9

NetApp
January 17, 2025

Índice

Gerenciar a autenticação do administrador e o RBAC

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

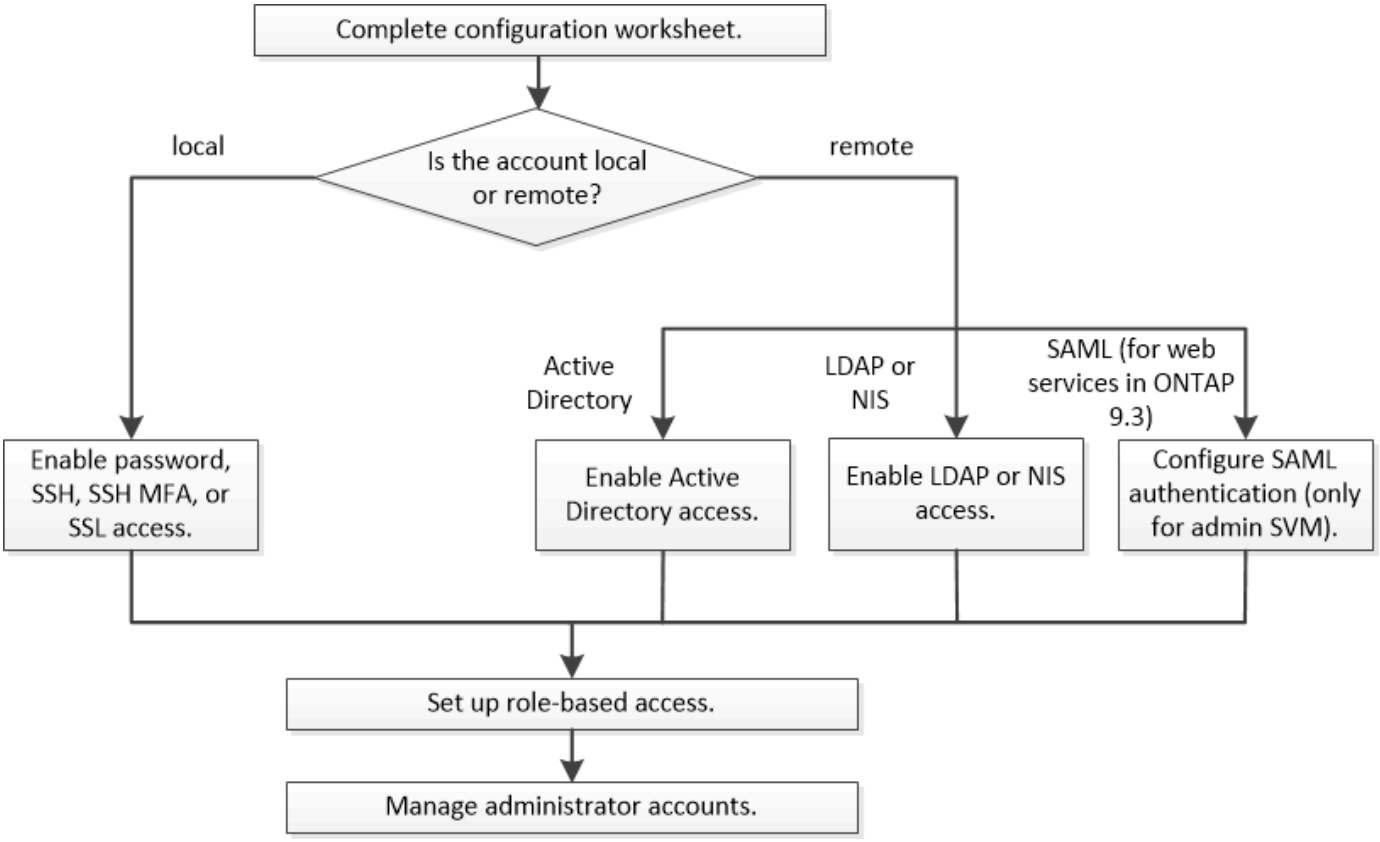
Você pode habilitar contas de login para administradores de cluster do ONTAP e administradores de máquina virtual de storage (SVM). Você também pode usar o controle de acesso baseado em função (RBAC) para definir as funcionalidades dos administradores.

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)

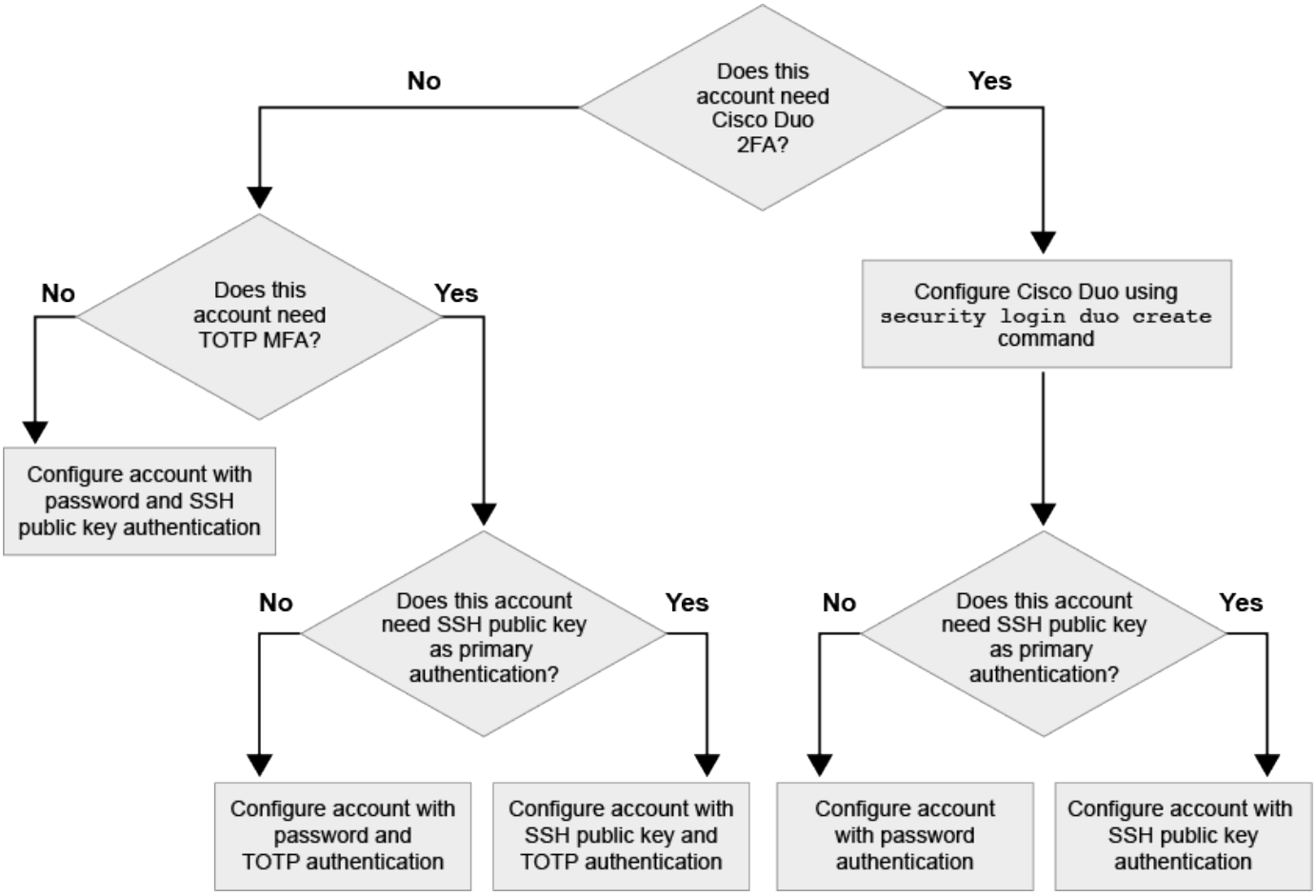
Visão geral da autenticação multifator

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"
```

Informações sobre direitos autorais

Informações sobre marcas comerciais