



Segurança RBAC

ONTAP automation

NetApp

January 12, 2026

This PDF was generated from https://docs.netapp.com/pt-br/ontap-automation/rest/rbac_overview.html on January 12, 2026. Always check docs.netapp.com for the latest.

Índice

- Segurança RBAC 1
 - Visão geral da segurança RBAC com a API REST do ONTAP 1
 - Funções do ONTAP 1
 - Mapeamento de funções e processamento de ONTAP 2
 - Resumo da evolução da RBAC 2
 - Trabalhe com funções e usuários na API REST do ONTAP 3
 - Acesso administrativo 3
 - Definições de função 4
 - Privileges 4
 - Resumo das funções incorporadas 5
 - Comparando os tipos de função 6

Segurança RBAC

Visão geral da segurança RBAC com a API REST do ONTAP

O ONTAP inclui uma funcionalidade robusta e extensível de controle de acesso baseado em funções (RBAC). Você pode atribuir a cada conta uma função diferente para controlar o acesso do usuário aos recursos expostos por meio da API REST e da CLI. As funções definem diferentes níveis de acesso administrativo para os vários usuários do ONTAP.



O recurso RBAC do ONTAP continuou a se expandir e foi significativamente aprimorado com o ONTAP 9.11.1 (e versões subsequentes). ["Resumo da evolução da RBAC"](#) Consulte e ["Novidades da API REST do ONTAP"](#) para obter mais informações.

Funções do ONTAP

Uma função é um conjunto de Privileges que definem coletivamente quais ações o usuário pode realizar. Cada privilégio identifica um caminho de acesso específico e o nível de acesso associado. As funções são atribuídas a contas de usuário e aplicadas pelo ONTAP ao tomar decisões de controle de acesso.

Tipos de papéis

Existem dois tipos de funções. Eles foram introduzidos e adaptados a diferentes ambientes à medida que o ONTAP evoluiu.



Há vantagens e desvantagens ao usar cada tipo de função. Consulte ["Comparando os tipos de função"](#) para obter mais informações.

Tipo	Descrição
DESCANSO	As funções REST foram introduzidas com o ONTAP 9.6 e geralmente são aplicadas aos usuários que acessam o ONTAP por meio da API REST. Criar uma FUNÇÃO REST cria automaticamente uma função <i>mapping</i> tradicional.
Tradicional	Estas são as funções herdadas incluídas antes do ONTAP 9.6. Eles foram introduzidos no ambiente de CLI do ONTAP e continuam sendo fundamentais para a segurança do RBAC.

Âmbito de aplicação

Cada função tem um escopo ou contexto dentro do qual é definida e aplicada. O escopo determina onde e como uma função específica é usada.



As contas de usuário do ONTAP também têm um escopo semelhante que determina como um usuário é definido e usado.

Âmbito de aplicação	Descrição
Cluster	As funções com um escopo de cluster são definidas no nível do cluster do ONTAP. Eles estão associados a contas de usuário no nível do cluster.

Âmbito de aplicação	Descrição
SVM	As funções com um escopo da SVM são definidas para um data SVM específico. Elas são atribuídas a contas de usuário no mesmo SVM.

Fonte das definições de função

Há duas maneiras de definir uma função ONTAP.

Fonte da função	Descrição
Personalizado	O administrador do ONTAP pode criar funções personalizadas. Essas funções podem ser adaptadas a um ambiente específico e requisitos de segurança.
Incorporado	Embora as funções personalizadas forneçam mais flexibilidade, também há um conjunto de funções incorporadas disponível no nível do cluster e do SVM. Essas funções são pré-definidas e podem ser usadas para muitas tarefas administrativas comuns.

Mapeamento de funções e processamento de ONTAP

Dependendo da versão do ONTAP que você está usando, todas ou quase todas as chamadas de API REST mapeiam para um ou mais comandos CLI. Quando você cria uma FUNÇÃO REST, uma função tradicional ou legada também é criada. Esta função tradicional **mapeada** é baseada nos comandos CLI correspondentes e não pode ser manipulada ou alterada.



O mapeamento de função reversa não é suportado. Ou seja, criar uma função tradicional não cria uma FUNÇÃO REST correspondente.

Resumo da evolução da RBAC

As funções tradicionais estão incluídas em todas as versões do ONTAP 9. Os papéis RESTANTES foram introduzidos mais tarde e evoluíram como descrito abaixo.

ONTAP 9,6

A API REST foi introduzida com o ONTAP 9.6. Os papéis RESTANTES também foram incluídos nesta versão. Além disso, quando você cria uma FUNÇÃO REST, uma função tradicional correspondente também é criada.

ONTAP 9 9.10.1

Cada versão do ONTAP de 9,7 a 9.10.1 inclui melhorias na API REST. Por exemplo, terminais REST adicionais foram adicionados a cada versão. No entanto, a criação e o gerenciamento dos dois tipos de papéis permaneceram separados. Além disso, o ONTAP 9.10,1 adicionou suporte a RBAC REST para o endpoint REST de snapshots `/api/storage/volumes/{vol.uuid}/snapshots`, que é um endpoint qualificado por recursos.

ONTAP 9.11,1

A capacidade de configurar e gerenciar funções tradicionais usando a API REST foi adicionada com esta versão. Níveis de acesso adicionais para as funções REST também foram adicionados.

Trabalhe com funções e usuários na API REST do ONTAP

Depois de entender os recursos básicos do RBAC, você pode começar a trabalhar com as funções e os usuários do ONTAP.



"[Workflows de RBAC](#)" Consulte para obter exemplos de como criar e usar funções com a API REST do ONTAP.

Acesso administrativo

Você pode criar e gerenciar as funções do ONTAP por meio da API REST ou da interface de linha de comando. Os detalhes de acesso são descritos abaixo.

API REST

Existem vários endpoints que podem ser usados ao trabalhar com funções RBAC e contas de usuário. Os quatro primeiros na tabela são usados para criar e gerenciar as funções. Os dois últimos são usados para criar e gerenciar contas de usuário.



Você pode acessar a documentação on-line do ONTAP "[Referência da API](#)" para obter mais informações, incluindo exemplos de como usar a API.

Endpoint	Descrição
/security/roles	Esse endpoint permite que você crie uma nova função REST. E começando com ONTAP 9.11,1 você também pode criar um papel tradicional. Neste caso, o ONTAP determina o tipo de função com base nos parâmetros de entrada. Você também pode recuperar uma lista das funções definidas.
/security/roles/{owner.UUID}/{name}	Você pode recuperar ou excluir um cluster específico ou função de escopo SVM. O valor UUID identifica o SVM onde a função é definida (cluster ou data SVM). O valor do nome é o nome da função.
/security/roles/{owner.UUID}/{name}/privileges	Este endpoint permite configurar o Privileges para uma função específica. As funções incorporadas podem ser recuperadas, mas não atualizadas. Consulte a documentação de referência da API para sua versão do ONTAP para obter mais informações.
/security/roles/{owner.UUID}/{name}/privileges/[path]	Você pode recuperar, modificar e excluir o nível de acesso e o valor de consulta opcional para um privilégio específico. Consulte a documentação de referência da API para sua versão do ONTAP para obter mais informações.
/security/accounts	Esse endpoint permite que você crie uma nova conta de usuário com escopo de cluster ou SVM. Vários tipos de informações devem ser incluídos ou posteriormente adicionados antes que a conta esteja operacional. Você também pode recuperar uma lista das contas de usuário definidas.
/security/accounts/{owner.UUID}/{name}	Você pode recuperar, modificar e excluir uma conta de usuário com escopo específico de cluster ou SVM. O valor UUID identifica o SVM onde o usuário está definido (cluster ou data SVM). O valor do nome é o nome da conta.

Interface de linha de comando

Os comandos ONTAP CLI relevantes são descritos abaixo. Todos os comandos são acessados no nível do cluster por meio de uma conta de administrador.

Comando	Descrição
<code>security login</code>	Este é o diretório que contém os comandos necessários para criar e gerenciar um login de usuário.
<code>security login rest-role</code>	Este é o diretório que contém os comandos necessários para criar e gerenciar uma FUNÇÃO REST associada a um login de usuário.
<code>security login role</code>	Este é o diretório que contém os comandos necessários para criar e gerenciar uma função tradicional associada a um login de usuário.

Definições de função

Os papéis REST e tradicionais são definidos através de um conjunto de atributos.

Proprietário e escopo

Uma função pode pertencer ao cluster do ONTAP ou a um data SVM específico no cluster. O proprietário também determina implicitamente o escopo da função.

Nome único

Cada função deve ter um nome único dentro de seu escopo. O nome de uma função de cluster deve ser exclusivo no nível de cluster do ONTAP, enquanto as funções do SVM precisam ser exclusivas no SVM específico.



O nome de uma nova função REST deve ser único entre os papéis REST, bem como os papéis tradicionais. Isso ocorre porque a criação de uma FUNÇÃO REST também resulta em uma nova função *mapping* tradicional com o mesmo nome.

Conjunto de Privileges

Cada função contém um conjunto de um ou mais Privileges. Cada privilégio identifica um recurso ou comando específico e o nível de acesso associado.

Privileges

Uma função pode conter um ou mais Privileges. Cada definição de privilégio é uma tupla e estabelece o nível de acesso a um recurso ou operação específico.

Caminho do recurso

O caminho do recurso é identificado como um endpoint REST ou caminho do diretório de comando/comando CLI.

Endpoint da REST

Um endpoint de API identificou o recurso de destino para uma FUNÇÃO REST.

Comando CLI

Um comando CLI identifica o destino para uma função tradicional. Um diretório de comando também pode ser especificado, que incluirá todos os comandos downstream na hierarquia da CLI do ONTAP.

Nível de acesso

O nível de acesso define o tipo de acesso que a função tem ao caminho ou comando específico do recurso. Os níveis de acesso são identificados através de um conjunto de palavras-chave predefinidas. Três níveis de acesso foram introduzidos com o ONTAP 9.6. Eles podem ser usados para papéis tradicionais e REST. Além disso, três novos níveis de acesso foram adicionados com o ONTAP 9.11.1. Esses novos níveis de acesso só podem ser usados com funções REST.



Os níveis de acesso seguem o modelo CRUD. Com REST, isso é baseado nos métodos HTTP primários (POST, GET, PATCH, DELETE). As operações CLI correspondentes geralmente mapeiam para as OPERAÇÕES REST (criar, mostrar, modificar, excluir).

Nível de acesso	Primitivas de REPOUSO	Adicionado	Apenas função REST
nenhum	n/a.	9,6	Não
readonly	OBTER	9,6	Não
tudo	OBTER, POSTAR, PATCH, EXCLUIR	9,6	Não
read_create	GET, POST	9.11.1	Sim
read_modify	OBTER, PATCH	9.11.1	Sim
read_create_modify	OBTER, POSTAR, PATCH	9.11.1	Sim

Consulta opcional

Ao criar uma função tradicional, você pode opcionalmente incluir um valor **query** para identificar o subconjunto de objetos aplicáveis para o diretório de comando ou comando.

Resumo das funções incorporadas

Há várias funções predefinidas incluídas no ONTAP que podem ser usadas no cluster ou no nível da SVM.

Funções de escopo do cluster

Há várias funções incorporadas disponíveis no escopo do cluster.

Consulte "[Funções predefinidas para administradores de cluster](#)" para obter mais informações.

Função	Descrição
administrador	Os administradores com essa função têm direitos irrestritos e podem fazer qualquer coisa no sistema ONTAP. Eles podem configurar todos os recursos no nível do cluster e do SVM.
AutoSupport	Esta é uma função especial adaptada para a conta AutoSupport.
backup	Esta função especial para software de backup que precisa fazer backup do sistema.
SnapLock	Esta é uma função especial adaptada para a conta SnapLock.
readonly	Os administradores com essa função podem visualizar tudo no nível do cluster, mas não podem fazer alterações.
nenhum	Não são fornecidos recursos administrativos.

Funções com escopo do SVM

Há várias funções incorporadas disponíveis no escopo da SVM. O **vsadmin** fornece acesso aos recursos mais gerais e poderosos. Existem várias funções adicionais adaptadas a tarefas administrativas específicas, incluindo:

- vsadmin-volume
- protocolo vsadmin
- vsadmin-backup
- vsadmin-SnapLock
- vsadmin-readonly

Consulte "[Funções predefinidas para administradores de SVM](#)" para obter mais informações.

Comparando os tipos de função

Antes de selecionar uma função **REST** ou **tradicional**, você deve estar ciente das diferenças. Algumas das maneiras como os dois tipos de função podem ser comparados são descritas abaixo.



Para casos de uso de RBAC mais avançados ou complexos, você normalmente deve usar uma função tradicional.

Como o usuário acessa o ONTAP

Antes de criar uma função, é importante saber como o usuário acessará o sistema ONTAP. Com base nisso, um tipo de função pode ser determinado.

Acesso	Tipo sugerido
Somente API REST	A função REST foi projetada para ser usada com a API REST.
API REST E CLI	Você pode definir uma FUNÇÃO REST que também cria uma função tradicional correspondente.
Apenas CLI	Você pode criar uma função tradicional.

Precisão do caminho de acesso

O caminho de acesso definido para uma FUNÇÃO REST é baseado em um endpoint REST. O caminho de acesso para uma função tradicional é baseado em um comando CLI ou diretório de comando. Além disso, você pode incluir um parâmetro de consulta opcional com uma função tradicional para restringir ainda mais o acesso com base nos valores de parâmetro do comando.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.