# Gerenciar autorização dinâmica

ONTAP 9

NetApp
January 17, 2025

# Índice

# 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