# Manage dynamic authorization

ONTAP 9

NetApp
May 18, 2024

# Table of Contents

# Manage dynamic authorization

## Dynamic authorization overview

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization to increase security of remote access to ONTAP while also mitigating potential damage that could be caused by a malicious actor. With ONTAP 9.15.1, dynamic authorization provides an initial framework for assigning a security score to users and, if their activity looks suspicious, challenging them with additional authorization checks or denying an operation completely. Administrators can create rules, assign trust scores, and restrict commands to determine when certain activity is allowed or denied for a user. Administrators can enable dynamic authorization cluster-wide or for individual storage VMs.

### How dynamic authorization works

Dynamic authorization uses a trust scoring system to assign users a different level of trust depending on the authorization policies. Based on the user's trust level, an activity they perform can be allowed or denied, or the user can be prompted for further authentication.

Take the example of three different users attempting to delete a volume. At the time they try to perform the operation, the risk rating for each user is examined:

- The first user logs in from a trusted device at regular office hours, which makes her risk rating low; the operation is allowed without additional authentication.
- The second user logs in from a trusted device in her home outside of office hours, which makes the risk rating moderate; she is prompted for additional authentication before the operation is allowed.
- The third user logs in from an untrusted device in a new location outside of office hours, which makes the risk rating high; the operation is not allowed.

**What's next**

- Customize dynamic authorization
- Enable or disable dynamic authorization

## Enable or disable dynamic authorization

Beginning with ONTAP 9.15.1, administrators can configure and enable dynamic authorization either in `visibility` mode to test the configuration, or in `enforced` mode to activate the configuration for CLI users connecting over SSH. If you no longer need dynamic authorization, you can disable it. When you disable dynamic authorization, the configuration settings remain available and you can use them later if you decide to re-enable it.

For more information about the parameters for the `security dynamic-authorization modify` command, refer to the ONTAP manual pages.

## Enable dynamic authorization for testing

You can enable dynamic authorization in visibility mode, which enables you to test the feature and ensure that users will not be accidentally locked out. In this mode, the trust score is checked with every restricted activity, but not enforced. However, any activity that would have been denied or subject to additional authentication challenges is logged. As a best practice, you should test your intended settings in this mode before enforcing them.

You can follow this step to enable dynamic authorization for the first time even if you haven't yet configured any other dynamic authorization settings. Refer to Customize dynamic authorization for steps to configure other dynamic authorization settings to customize it to your environment.

**Steps**

1. Enable dynamic authorization in visibility mode by configuring global settings and changing the feature state to `visibility`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

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

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

## Enable dynamic authorization in enforced mode

You can enable dynamic authorization in enforced mode. Typically, you use this mode after you have completed testing with visibility mode. In this mode, the trust score is checked with every restricted activity, and activity restrictions are enforced if the restriction conditions are met. The suppression interval is also enforced, preventing additional authentication challenges within the specified interval.

This step assumes that you have previously configured and enabled dynamic authorization in `visibility` mode, which is strongly recommended.

**Steps**

1. Enable dynamic authorization in `enforced` mode by changing its state to `enforced`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

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

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

### Disable dynamic authorization

You can disable dynamic authorization if you no longer need the added authentication security.

**Steps**

1. Disable dynamic authorization by changing its state to `disabled`. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment. Parameters in bold are required:

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

2. Check the result by using the `show` command to display the global configuration:

```
security dynamic-authorization show
```

### What's next

(Optional) Depending on your environment, refer to Customize dynamic authorization to configure other dynamic authorization settings.

# Customize dynamic authorization

As an administrator, you can customize different aspects of your dynamic authorization configuration to increase the security of remote administrator SSH connections to your ONTAP cluster.

You can customize the following dynamic authorization settings depending on your security needs:

- Configure dynamic authorization global settings
- Configure dynamic authorization trust score components
- Configure a custom trust score provider
- Configure restricted commands

- Configure dynamic authorization groups

## Configure dynamic authorization global settings

You can configure global settings for dynamic authorization, including the storage VM to secure, the suppression interval for authentication challenges, and the trust score settings.

For more information about the parameters and default values for the `security dynamic-authorization modify` command, refer to the ONTAP manual pages.

### Steps

1. Configure global settings for dynamic authorization. If you don't use the `-vserver` parameter, the command is run at the cluster level. Update the values in brackets <> to match your environment:

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

2. View the resulting configuration:

```
security dynamic-authorization show
```

## Configure restricted commands

When you enable dynamic authorization, the feature includes a default set of restricted commands. You can modify this list to suit your needs. Refer to the multi-admin verification (MAV) documentation for information on the default list of restricted commands.

### Add a restricted command

You can add a command to the list of commands that are restricted with dynamic authorization.

For more information about the parameters and default values for the `security dynamic-authorization rule create` command, refer to the ONTAP manual pages.

### Steps

1. Add the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

2. View the resulting list of restricted commands:

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

#### Remove a restricted command

You can remove a command from the list of commands that are restricted with dynamic authorization.

For more information about the parameters and default values for the `security dynamic-authorization rule delete` command, refer to the ONTAP manual pages.

**Steps**

1. Remove the command. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

2. View the resulting list of restricted commands:

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

## Configure dynamic authorization groups

By default, dynamic authorization applies to all users and groups as soon as you enable it. However, you can create groups using the `security dynamic-authorization group create` command, so that dynamic authorization only applies to those specific users.

#### Add a dynamic authorization group

You can add a dynamic authorization group.

For more information about the parameters and default values for the `security dynamic-authorization group create` command, refer to the ONTAP manual pages.

**Steps**

1. Create the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

2. View the resulting dynamic authorization groups:

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

### Remove a dynamic authorization group

You can remove a dynamic authorization group.

**Steps**

1. Delete the group. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

2. View the resulting dynamic authorization groups:

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

## Configure dynamic authorization trust score components

You can configure the maximum score weight to change priority of scoring criteria or to remove certain criteria from risk scoring.

As a best practice, you should leave the default score weight values in place, and only adjust them if needed.

For more information about the parameters and default values for the `security dynamic-authorization trust-score-component modify` command, refer to the ONTAP manual pages.

The following are the components that you can modify, along with their default score and percentage weights:

| Criteria | Component name | Default raw score weight | Default percentage weight |
|---|---|---|---|
| Trusted device | `trusted-device` | 20 | 50 |
| User login authentication history | `authentication-history` | 20 | 50 |

**Steps**

1. Modify trust score components. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

2. View the resulting trust score component settings:

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

### Reset the trust score for a user

If a user is denied access due to system policies and is able to prove their identity, the administrator can reset the user's trust score.

For more information about the parameters and default values for the `security dynamic-authorization user-trust-score reset` command, refer to the ONTAP manual pages.

#### Steps

1. Add the command. Refer to Configure dynamic authorization trust score components for a list of trust score components that you can reset. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

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

### Display your trust score

A user can display their own trust score for a login session.

#### Steps

1. Display your trust score:

```
security login whoami
```

You should see output similar to the following:

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

## Configure a custom trust score provider

If you already receive scoring methods from an external trust score provider, you can add the custom provider to the dynamic authorization configuration.

**Before you begin**

- The custom trust score provider must return a JSON response. The following syntax requirements must be met:
  - The field that returns the trust score must be a scalar field and not an element of an array.
  - The field that returns the trust score can be a nested field, such as `trust_score.value`.
  - There must be a field within the JSON response that returns a numeric trust score. If this is not natively available, you can write a wrapper script to return this value.
- The value provided can be either a trust score or a risk score. The difference is that the trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. For example, a trust score of 90 for a score range of 0 to 100 indicates that the score is very trustworthy and likely to result in an "allow" without additional challenge, while a risk score of 90 for a score range of 0 to 100 indicates high risk and likely to result in a "deny" without an additional challenge.
- The custom trust score provider must be accessible via the ONTAP REST API.
- The custom trust score provider must be configurable using one of the supported parameters. Custom trust score providers that require configuration that is not in the supported parameter list are not supported.

For more information about the parameters and default values for the `security dynamic-authorization trust-score-component create` command, refer to the ONTAP manual pages.

**Steps**

1. Add a custom trust score provider. Update the values in brackets <> to match your environment. If you don’t use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
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. View the resulting trust score provider settings:

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

### Configure custom trust score provider tags

You can communicate with external trust score providers using tags. This enables you to send information in the URL to the trust score provider without exposing sensitive information.

For more information about the parameters and default values for the `security dynamic-authorization trust-score-component create` command, refer to the ONTAP manual pages.

#### Steps

1. Enable trust score provider tags. Update the values in brackets <> to match your environment. If you don't use the `-vserver` parameter, the command is run at the cluster level. Parameters in bold are required:

```
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>
```

For example:

```
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"
```

## Copyright information



## Trademark information