security dynamic-authorization commands

ONTAP 9.15.1 commands

NetApp
December 18, 2024

Table of Contents

security dynamic-authorization commands

security dynamic-authorization modify

Modify dynamic-authorization global settings

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization modify` command modifies one or more dynamic authorization settings.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the setting. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver is used.

`[-state {disabled|visibility|enforced}]` - Dynamic Authorization State

This parameter sets the state of the dynamic authorization feature. Valid values are *`disabled`*, *`visibility`* and *`enforced`*.

- disabled: Dynamic Authorization is disabled. This is the default factory setting.
- visibility: Dynamic Authorization is enabled in visibility mode. Customers will typically use this mode during a trial run to test the feature and ensure that users are not being inadvertently locked out. In this mode, the trust score is checked every time the user attempts to execute a restricted command, but not enforced. That is, the user will be allowed to execute all restricted commands as long as his RBAC privileges allow it. However, all commands that will either be denied or subject to additional MFA challenge will be logged.
- enforced: Dynamic Authorization is enabled in enforcement mode. Customers will typically use this mode after they have completed their trial run using visibility mode and verified that their configuration settings are correct, i.e. no users are being inadvertently locked out as a result of incorrect configuration. In this mode, the trust score is checked every time the user attempts to execute a restricted command and use to enforce dynamic authorization. That is, the user will be allowed to execute all restricted commands without additional MFA challenge only if the trust score exceeds the upper MFA challenge boundary. If the trust score falls within the lower and upper MFA challenge boundary, the user will be subject to an additional MFA challenge before being allowed to execute the command. If the trust score falls below the lower MFA challenge boundary, the user will be denied access. All additional MFA challenges and denials will be logged. The suppression interval is also enforced so no additional authentication challenges will be required if repeated authorization requests are made within the suppression interval.

`[-suppression-interval {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W | disabled}]` - Dynamic Authorization Suppression Interval

The dynamic authorization challenge suppression interval in ISO-8601 format. When a series of restricted commands are executed within a short interval, multiple authentication prompts are suppressed to create a good user experience. The default suppression interval is 10 minutes, or *`PT10M`* in ISO-8601 format.

[-lower-challenge-boundary <percent>] - Lower MFA Challenge Boundary

The lower MFA challenge percentage boundary. Supported values are from *0* to *99* . Default value is *0* .

[-upper-challenge-boundary <percent>] - Upper MFA Challenge Boundary

The upper MFA challenge percentage boundary. Supported values are from *0* to *100* . This must be equal to or greater than the value of the lower boundary. A value of 100 means that every request will either be denied or subject to an additional authentication challenge; there are no requests that are allowed without a challenge. Default value is *90* .

Examples

The following command modifies the lower challenge boundary to 10.

```
cluster1::> security dynamic-authorization modify -lower-challenge
-boundary 10

cluster1::> security dynamic-authorization show
Vserver: cluster1
                          Dynamic Authorization State: disabled
           Dynamic Authorization Suppression Interval: 10m
                        Lower MFA Challenge Boundary: 10%
                        Upper MFA Challenge Boundary: 90%
```

security dynamic-authorization show

Show dynamic-authorization global settings

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization show` displays information on dynamic authorization settings.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the dynamic authorization settings.

[-vserver <vserver name>] - Vserver

Selects the dynamic authorization settings that match this parameter value. If not specified, all cluster-level and Vserver-level settings are displayed.

[-state {disabled|visibility|enforced}] - Dynamic Authorization State

Selects the dynamic authorization settings that match this parameter value.

[-suppression-interval {P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W | disabled}] - Dynamic Authorization Suppression Interval

Selects the dynamic authorization settings that match this parameter value.

[-lower-challenge-boundary <percent>] - Lower MFA Challenge Boundary

Selects the dynamic authorization settings that match this parameter value.

[-upper-challenge-boundary <percent>] - Upper MFA Challenge Boundary

Selects the dynamic authorization settings that match this parameter value.

Examples

The example below displays information on dynamic authorization settings:

```
cluster1::> security dynamic-authorization show
Vserver: cluster1
                          Dynamic Authorization State: disabled
           Dynamic Authorization Suppression Interval: 10m
                        Lower MFA Challenge Boundary: 0%
                        Upper MFA Challenge Boundary: 90%
```

security dynamic-authorization authentication-history-policy modify

Modify authentication history policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization authentication-history-policy modify` command updates the authentication history policy settings for dynamic authorization.

Parameters

-vserver <vserver name> - Vserver

This parameter optionally specifies the Vserver associated with the authentication history policy setting. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

[-use-last-num-days <integer>] - Last Number of Days

This parameter optionally specifies the last number of days of authentication history statistics to use in calculating the trust score for the authentication history component. By default, this is set to -1, which means the trust score for authentication history component is calculated from all successful and failed authentications since the user's first successful login.

[-lower-boundary <percent>] - Lower Boundary of Authentication Failures

This parameter optionally specifies the lower boundary of authentication failures. The value is a percentage from 0 to 99, and must be less than or equal to the upper boundary. When used in conjunction with the *upper-boundary* , if the authentication failures are less than the *lower-boundary* percentage, the authentication history component gets a full trust score, while if the authentication failures are higher than the *upper-boundary* percentage, the authentication history component gets a zero trust score. Authentication failures falling between the *lower-boundary* and *upper-boundary* gets a 50% trust score for the authentication history component.

[-upper-boundary <percent>] - Upper Boundary of Authentication Failures

This parameter optionally specifies upper boundary of authentication failures. The value is a percentage from 0 to 100, and must be greater than or equal to the lower boundary. Refer to the description in the *lower-boundary* parameter on how this setting is used.

Examples

The following command modifies the upper boundary of authentication failures for the Administrative Vserver to 90%.

```
cluster1::*> security dynamic-authorization authentication-history-policy
modify -upper-boundary 90

cluster1::*> security dynamic-authorization authentication-history-policy
show
Vserver: cluster1
                                  Last Number of Days: 90
            Lower Boundary of Authentication Failures: 10%
            Upper Boundary of Authentication Failures: 90%
Vserver: svm0
                                  Last Number of Days: -1
            Lower Boundary of Authentication Failures: 10%
            Upper Boundary of Authentication Failures: 100%
2 entries were displayed.
```

security dynamic-authorization authentication-history-policy show

Show authentication history policy

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization authentication-history-policy show` displays information about the dynamic authorization authentication history policy settings.

Parameters

{ [-fields <fieldname>,…]
Selects the fields that you specify.

| [-instance] }
Displays all the fields for the dynamic authorization authentication history policy.

[-vserver <vserver name>] - Vserver
Selects the dynamic authorization authentication history policy fields that match this parameter value.

[-use-last-num-days <integer>] - Last Number of Days
Selects the dynamic authorization authentication history policy fields that match this parameter value.

[-lower-boundary <percent>] - Lower Boundary of Authentication Failures
Selects the dynamic authorization authentication history policy fields that match this parameter value.

[-upper-boundary <percent>] - Upper Boundary of Authentication Failures
Selects the dynamic authorization authentication history policy fields that match this parameter value.

Examples

The example below displays information about all dynamic authorization authentication history policy settings:

```
cluster1::> security dynamic-authorization authentication-history-policy
show
Vserver: cluster1
                           Last Number of Days: 90
    Lower Boundary of Authentication Failures: 10%
    Upper Boundary of Authentication Failures: 100%
Vserver: svm0
                           Last Number of Days: -1
    Lower Boundary of Authentication Failures: 10%
    Upper Boundary of Authentication Failures: 100%
2 entries were displayed.
```

security dynamic-authorization executed-commands show

Display executed commands

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization executed-commands show` command displays information about the executed commands according to the dynamic authorization rules.

Parameters

{ [-fields <fieldname>,…]
Selects the fields that you specify.

| [-instance] }
Displays all the fields for the dynamic authorization executed commands.

[-vserver <vserver name>] - Vserver
Selects the dynamic authorization executed command fields that match this Vserver.

[-date <MM/DD/YYYY HH:MM:SS>] - Date
Selects the dynamic authorization executed command fields that match this date.

[-username <text>] - Username
Selects the dynamic authorization executed command fields that match this username.

[-operation <text>] - Operation
Selects the dynamic authorization executed command fields that match this operation.

[-count <integer>] - Count
Selects the dynamic authorization executed command fields that match this count.

[-score <integer>] - Trust Score
Selects the dynamic authorization executed command fields that match this score.

[-result {permit|deny|challenge}] - Result
Selects the dynamic authorization executed command fields that match this result.

Examples

The example below displays information about all dynamic authorization executed commands:

```
cluster1::> security dynamic-authorization executed-commands show

Vserver: usernamecluster-1

Date                  Operation   Username   Count   Trust Score   Result
-------------------   ---------   --------   -----   -----------   ------
12/7/2023 08:25:57    security login create
                                  admin      1       100           permit
12/7/2023 08:26:04    security login unlock
                                  admin      1       100           permit
12/7/2023 08:26:09    security multi-admin-verify approval-group create
                                  admin      1       100           permit
3 entries were displayed.
```

security dynamic-authorization group create

Add a Dynamic Authorization group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization group create` command creates the groups to include in dynamic authorization.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver of the dynamic authorization group that is being created. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

`-name <text>` - Group Name

This parameter specifies the name of the group that will be part of dynamic authorization.

`[-excluded-usernames <text>,…]` - List of Excluded Users

This parameter optionally specifies the list of users that will be excluded from dynamic authorization.

`[-comment <text>]` - Comment

This parameter optionally specifies the comments.

Examples

The following command creates a group *`test`* on vserver *`vs1`* and excludes the user *`tsmith`* from dynamic authorization.

```
cluster1::> security dynamic-authorization group create -vserver vs1 -name
test -excluded-usernames tsmith
```

security dynamic-authorization group delete

Delete a Dynamic Authorization group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization group delete` command deletes the specified group.

Parameters

-vserver <vserver name> - Vserver

This parameter optionally specifies the Vserver of the dynamic authorization group that is being deleted. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

-name <text> - Group Name

This parameter specifies the group name that is being deleted.

Examples

The following command deletes the group *test* from the Vserver *vs1* .

```
cluster1::> dynamic authorization group delete -vserver vs1 -name test
```

security dynamic-authorization group modify

Modify a Dynamic Authorization group

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization group modify` command modifies the dynamic authorization groups.

Parameters

-vserver <vserver name> - Vserver

This parameter optionally specifies the Vserver of the group for which the `-excluded-usernames` or `-comment` is being modified. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

-name <text> - Group Name

This parameter specifies the name of the group for which the `-excluded-usernames` or `-comment` is being modified.

[-excluded-usernames <text>,…] - List of Excluded Users

This parameter specifies the list of users to be excluded from dynamic authorization.

[-comment <text>] - Comment

This parameter optionally specifies the comments.

Examples

The following command modifies the excluded users for the group *test* who is part of Vserver *vs1* .

```
cluster1::> security dynamic-authorization group modify -vserver vs1
-group-name test -excluded-usernames Jsmith
```

security dynamic-authorization group show

Display Dynamic Authorization groups

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization group show` command displays information about the dynamic authorization groups.

Parameters

{ [-fields <fieldname>,…]

If you specify the `-fields <fieldname>, …` parameter, the command output also includes the specified field or fields. You can use '-fields ?' to display the fields to specify.

| [-instance] }

If you specify the `-instance` parameter, the command displays detailed information about all fields.

[-vserver <vserver name>] - Vserver

Selects dynamic-authorization groups for this Vserver.

[-name <text>] - Group Name

Selects dynamic-authorization groups that match this group name.

[-excluded-usernames <text>,…] - List of Excluded Users

Selects the dynamic-authorization groups that match the specified excluded username.

[-comment <text>] - Comment

Selects the dynamic-authorization groups that match this comment.

Examples

The example below displays dynamic authorization group information for the Vserver *vs1* .

```
cluster1::> security dynamic-authorization group show -vserver vs1
               Vserver: vs1
            Group Name: NETAPP_ENG
List of Excluded Users: user1, user2, user12
               Comment: -
```

security dynamic-authorization rule create

Add a dynamic authorization rule

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization rule create` command creates a custom dynamic authorization rule for an operation. By default, the set of operations subject to dynamic authorization is the same as the default Multi-Admin-Verify (MAV) set of commands. Additional operations can be configured using the `security dynamic-authorization rule create` command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom dynamic authorization rule.

`-operation <Command or Command Directory>` - Command or Command Directory

This parameter specifies the operation for the custom dynamic authorization rule to be created. The operation can be a command or command directory.

`-query <query>` - Query

This parameter optionally specifies the object (or objects) upon which to apply the operation. Any field or query supported by the operation can be supplied. If a query is not specified for the rule, the rule applies to all objects of the specified operation. The query object must be enclosed in double quotation marks ("").

Examples

The following command creates a custom dynamic authorization rule for the job delete operation for the Administrative Vserver. This rule is applicable only to job objects whose job ID is greater than 50.

```
cluster1::> security dynamic-authorization rule create -operation "job
delete" -query "-id >50"
```

The following command creates a custom dynamic authorization rule for the snapmirror policy create operation for the data Vserver *vs1.example.com*. This rule is applicable only to snapmirror policies of type other than *async-mirror*.

```
cluster1::> security dynamic-authorization rule create -vserver
vs1.example.com -operation "snapmirror policy create" -query "-type
!async-mirror"
```

Related Links

- job delete
- snapmirror policy create

security dynamic-authorization rule delete

Delete a dynamic authorization rule

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization rule delete` command deletes a custom dynamic authorization rule for an operation. It can be used to delete a custom dynamic authorization rule that was configured using the security dynamic-authorization rule create command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom dynamic authorization rule.

`-operation <Command or Command Directory>` - Command or Command Directory

This parameter specifies the operation for the custom dynamic authorization rule to be deleted.

Examples

The following command deletes a custom dynamic authorization rule for the `network port ifgrp` operation for the Administrative Vserver.

```
cluster1::> security dynamic-authorization rule delete -vserver cluster1
-operation "network port ifgrp"
```

The following command deletes a custom dynamic authorization rule for the `vserver services nis-domain create` operation for the data Vserver *`vs1.example.com`*.

```
cluster1::> security dynamic-authorization rule delete -vserver
vs1.example.com -operation "vserver services nis-domain create"
```

Related Links

- security dynamic-authorization rule create

security dynamic-authorization rule modify

Modify a dynamic authorization rule

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization rule modify` command modifies a custom dynamic authorization rule for an operation. It can be used to modify a custom dynamic authorization rule that was configured using the security dynamic-authorization rule create command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom dynamic authorization rule.

`-operation <Command or Command Directory>` - Command or Command Directory

This parameter specifies the operation for the custom dynamic authorization rule to be modified. The operation can be a command or command directory.

`[-query <query>]` - Query

This parameter optionally specifies the object (or objects) upon which to apply the operation. Any field or query supported by the operation can be supplied. If the query is specified as "" i.e., empty, the rule applies to all objects of the specified operation. The query object must be enclosed in double quotation marks ("").

Examples

The following command modifies the query of a custom dynamic authorization rule for the storage encryption disk destroy operation in the Administrative Vserver. The new query disallows destroying of storage encryption disks starting with the name `xxxxx_` .

```
cluster1::> security dynamic-authorization rule modify -operation "storage
encryption disk destroy" -query "-disk !xxxxx_*"
```

The following command resets the query of a custom dynamic authorization rule for the vserver active-directory create operation for the data Vserver *`vs1.example.com`* .

```
cluster1::> security dynamic-authorization rule modify -vserver
vs1.example.com -operation "vserver active-directory create" -query ""
```

Related Links

- security dynamic-authorization rule create
- storage encryption disk destroy
- vserver active-directory create

security dynamic-authorization rule show

Show dynamic authorization rules

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization rule show` displays information about dynamic authorization rules, which includes both pre-defined as well as custom dynamic authorization rules.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the specified dynamic authorization rules.

[-vserver <vserver name>] - Vserver

Selects the dynamic authorization rules that match this parameter value.

[-operation <Command or Command Directory>] - Command or Command Directory

Selects the dynamic authorization rules that match this parameter value.

[-query <query>] - Query

Selects the dynamic authorization rules that match this parameter value.

Examples

The example below displays information about all dynamic authorization rules whose operation matches the prefix *`security multi-admin-verify`*.

```
cluster1::*> security dynamic-authorization rule show -operation "security
multi-admin-verify"*

Vserver: cluster1

Operation
Query
---------------------------------------
----------------------------------
security multi-admin-verify
security multi-admin-verify approval-group
security multi-admin-verify approval-group replace
security multi-admin-verify rule

Vserver: vs1

Operation
Query
---------------------------------------
----------------------------------
security multi-admin-verify
security multi-admin-verify approval-group
security multi-admin-verify approval-group replace
security multi-admin-verify rule
8 entries were displayed.
```

security dynamic-authorization trust-score-component create

Create a trust score component

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization trust-score-component create` command creates and registers a custom trust score component. Administrators can use this command to configure trust score components in addition to or as an alternative to built-in components.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom trust score component. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

-component <text> - Component Name

The name of the custom component used to obtain the trust score. This must be unique within the Vserver.

[-weight <integer>] - Score Weight

An integer giving the raw weight of the component, indicating the importance of the component relative to other components for calculating the trust score. Built-in components have a default weightage of *20* .

[-provider-uri {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Trust Score Provider URI of Component

The trust score provider URI to obtain the trust score for the component. The response from the URI must be in JSON.

[-max-score <integer>] - Max Trust Score of Component

The maximum score for the component. The default value is *20* .

[-min-score <integer>] - Min Trust Score of Component

The minimum score for the component. The default value is *0* .

[-score-field <text>] - Score field to check in JSON response

The field within the JSON response to obtain the trust score.

[-score-type {trust-score|risk-score}] - Score Type

This parameter specifies if the score returned from the component is trust score or risk score. The trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. The default value is *trust-score* .

[-secret-access-key <text>] - Access key for trust score provider

An optional field giving the access key for the trust score provider. This is used to authenticate to the provider.

[-provider-http-headers <text>,…] - Provider HTTP headers

An optional list of HTTP headers required by the trust score provider.

Examples

The following command creates a dynamic authorization custom component for the Administrative Vserver. The username is a parameter that will be replaced with the actual username at run-time:

```
cluster1::> security dynamic-authorization trust-score-component create
-component comp1 -weight 20 -max-score 500 -provider-uri
https://provider.example.com/trust-scores/users/${username}/component
-score-field score
```

security dynamic-authorization trust-score-component delete

Delete a trust score component

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization trust-score-component delete` command deletes a custom trust score component. It can be used to delete a custom trust score component that was configured using the security dynamic-authorization trust-score-component create command.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom trust score component. If not specified, this defaults to the cluster Vserver.

`-component <text>` - Component Name

Name of the custom trust score component to be deleted.

Examples

The following command deletes a custom trust score component named comp1 for the Administrative Vserver.

```
cluster1::> security dynamic-authorization trust-score-component delete
-component comp1
```

Related Links

- security dynamic-authorization trust-score-component create

security dynamic-authorization trust-score-component modify

Modify a trust score component

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization trust-score-component modify` command updates an existing custom trust score component.

Parameters

`-vserver <vserver name>` - Vserver

This parameter optionally specifies the Vserver associated with the custom trust score provider component. If this parameter is specified, the setting applies to that Vserver only. If not specified, the cluster Vserver setting is used.

-component <text> - Component Name

The component name.

[-weight <integer>] - Score Weight

An integer giving the raw weight of the component, indicating the importance of the component relative to other components for calculating the trust score. Built-in components have a default weightage of 20.

[-provider-uri {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Trust Score Provider URI of Component

The trust score provider URI to obtain the trust score for the component. The response from the URI must be in JSON.

[-max-score <integer>] - Max Trust Score of Component

The maximum score for the component.

[-min-score <integer>] - Min Trust Score of Component

The minimum score for the component.

[-score-field <text>] - Score field to check in JSON response

The field within the JSON response to obtain the trust score.

[-score-type {trust-score|risk-score}] - Score Type

This parameter specifies if the score returned from the component is trust score or risk score. The trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. The default value is *trust-score* .

[-secret-access-key <text>] - Access key for trust score provider

An optional field giving the access key for the trust score provider. This is used to authenticate to the provider.

[-provider-http-headers <text>,…] - Provider HTTP headers

An optional list of HTTP headers required by the trust score provider.

Examples

The following command modifies a dynamic authorization custom component for the Administrative Vserver to change the weightage of the component to 100.

```
cluster1::> security dynamic-authorization trust-score-component modify
-component comp1 -weight 100
```

security dynamic-authorization trust-score-component show

Display trust score components

Availability: This command is available to *cluster* and *Vserver* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization trust-score-component show` displays information about the components that comprise the trust score.

Parameters

{ [-fields <fieldname>,…]

Selects the fields that you specify.

| [-instance] }

Displays all the fields for the specified dynamic authorization trust score components.

[-vserver <vserver name>] - Vserver

Selects the dynamic authorization trust score components that match this parameter value.

[-component <text>] - Component Name

Selects the dynamic authorization trust score components that match this parameter value.

[-weight <integer>] - Score Weight

Selects the dynamic authorization trust score components that match this parameter value.

[-max-percent-score-weight <double hundredths>] - Max Percentage Score Weight

Selects the dynamic authorization trust score components that match this parameter value.

[-provider-uri {scheme://(hostname|IPv4 Address|'['IPv6 Address']')…}] - Trust Score Provider URI of Component

Selects the dynamic authorization trust score components that match this parameter value.

[-max-score <integer>] - Max Trust Score of Component

Selects the dynamic authorization trust score components that match this parameter value.

[-min-score <integer>] - Min Trust Score of Component

Selects the dynamic authorization trust score components that match this parameter value.

[-score-field <text>] - Score field to check in JSON response

Selects the dynamic authorization trust score components that match this parameter value.

[-score-type {trust-score|risk-score}] - Score Type

This parameter specifies if the score returned from the components is trust score or risk score. The trust score is in ascending order with a higher score denoting a higher trust level, while the risk score is in descending order. The default value is *trust-score* .

[-provider-http-headers <text>,…] - Provider HTTP headers

Selects the dynamic authorization trust score components that match this parameter value.

Examples

The example below displays information about all dynamic authorization trust score components, both built-in and custom:

```
cluster1::> security dynamic-authorization trust-score-component create
-component comp1 -weight 20 -max-score 100 -provider-uri
https://provider.example.com/trust-scores/users/admin1/component1.json
-score-field score

cluster1::> security dynamic-authorization trust-score-component show
Percentage
Vserver           Component Name                    Score Weight   Score
Weight
---------------   -------------------------------   ------------
------------
cluster1          authentication_history_policy              20
33.33
cluster1          comp1                                      20
33.33
cluster1          trusted_device                             20
33.33
svm0              authentication_history_policy              20
50.00
svm0              trusted_device                             20
50.00

5 entries were displayed.
```

The following command displays the details of all components matching the name *comp1* :

```
cluster1::> security dynamic-authorization trust-score-component show
-vserver cluster1 -component comp1 -instance
Vserver: cluster1
            Trust Score Component Name: comp1
               Weight of the Component: 20
Max Percentage Weight of the component: 50.00
 Trust Score Provider URI of Component:
https://provider.example.com/trust-scores/users/admin1/component1.json
                Max Score of Component: 100
 Score field to check in JSON response: score
                 Provider HTTP headers: -
```

security dynamic-authorization user-trust-score reset

Resets trust score of user

Availability: This command is available to *cluster* administrators at the *admin* privilege level.

Description

The `security dynamic-authorization user-trust-score reset` command resets the trust score of the specified user.

Parameters

`-vserver <vserver name>` - Vserver

Selects the Vserver that match this parameter value.

`-username <text>` - Username

Reset the trust score for this user.

`-component <text>` - Component Name

The component for which the user trust score has to be reset.

Examples

The example below resets the user trust score.

```
cluster1::> security dynamic-authorization user-trust-score reset -vserver
vs1 -username Tsmith -component authentication_history_policy
```

Copyright information

Trademark information