security session commands

ONTAP commands

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-cli-9131/security-session-kill-cli.html on February 03, 2026. Always check docs.netapp.com for the latest.

Table of Contents

security session commands . . . 1
- security session kill-cli . . . 1
  - Description . . . 1
  - Parameters . . . 1
  - Examples . . . 2
- security session show . . . 4
  - Description . . . 4
  - Parameters . . . 5
  - Examples . . . 6
- security session limit create . . . 8
  - Description . . . 8
  - Parameters . . . 8
  - Examples . . . 8
- security session limit delete . . . 9
  - Description . . . 9
  - Parameters . . . 9
  - Examples . . . 9
- security session limit modify . . . 9
  - Description . . . 9
  - Parameters . . . 9
  - Examples . . . 10
- security session limit show . . . 10
  - Description . . . 10
  - Parameters . . . 10
  - Examples . . . 10
- security session limit application create . . . 11
  - Description . . . 11
  - Parameters . . . 11
  - Examples . . . 11
- security session limit application delete . . . 11
  - Description . . . 12
  - Parameters . . . 12
  - Examples . . . 12
- security session limit application modify . . . 12
  - Description . . . 12
  - Parameters . . . 12
  - Examples . . . 12
- security session limit application show . . . 13
  - Description . . . 13
  - Parameters . . . 13
  - Examples . . . 13
- security session limit location create . . . 14
  - Description . . . 14

Parameters . . . 14
Examples . . . 14
security session limit location delete . . . 14
Description . . . 14
Parameters . . . 14
Examples . . . 15
security session limit location modify . . . 15
Description . . . 15
Parameters . . . 15
Examples . . . 15
security session limit location show . . . 16
Description . . . 16
Parameters . . . 16
Examples . . . 16
security session limit request create . . . 17
Description . . . 17
Parameters . . . 17
Examples . . . 17
security session limit request delete . . . 17
Description . . . 18
Parameters . . . 18
Examples . . . 18
security session limit request modify . . . 18
Description . . . 18
Parameters . . . 18
Examples . . . 18
security session limit request show . . . 19
Description . . . 19
Parameters . . . 19
Examples . . . 19
security session limit user create . . . 20
Description . . . 20
Parameters . . . 20
Examples . . . 20
security session limit user delete . . . 20
Description . . . 21
Parameters . . . 21
Examples . . . 21
security session limit user modify . . . 21
Description . . . 21
Parameters . . . 21
Examples . . . 22
security session limit user show . . . 22
Description . . . 22
Parameters . . . 22

Examples . . . 23
security session limit vserver create . . . 23
Description . . . 23
Parameters . . . 23
Examples . . . 23
security session limit vserver delete . . . 24
Description . . . 24
Parameters . . . 24
Examples . . . 24
security session limit vserver modify . . . 24
Description . . . 24
Parameters . . . 24
Examples . . . 25
security session limit vserver show . . . 25
Description . . . 25
Parameters . . . 25
Examples . . . 25
security session request-statistics show-by-application . . . 26
Description . . . 26
Parameters . . . 26
Examples . . . 28
security session request-statistics show-by-location . . . 29
Description . . . 29
Parameters . . . 29
Examples . . . 31
security session request-statistics show-by-request . . . 33
Description . . . 33
Parameters . . . 33
Examples . . . 35
security session request-statistics show-by-user . . . 35
Description . . . 35
Parameters . . . 35
Examples . . . 37
security session request-statistics show-by-vserver . . . 39
Description . . . 39
Parameters . . . 39
Examples . . . 41

security session commands

security session kill-cli

Kill a CLI session

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

Description

The `security session kill-cli` command is used to terminate CLI sessions. If the session being killed is actively processing a non-read command, the kill will wait until the command is complete before terminating the session. If the session being killed is actively processing a read (show) command, the kill will wait until the current row is returned before terminating the session.

Parameters

`-node {<nodename>|local}` - Node

Selects the sessions that match this parameter value. This identifies the node that is processing the session.

`[-interface {cli|ontapi|rest}]` - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that is processing the session.

`[-start-time <MM/DD HH:MM:SS>]` - Start Time

Selects the sessions that match this parameter value. This identifies the start time of the current active session.

`-session-id <integer>` - Session ID

Selects the sessions that match this parameter value. This number uniquely identifies a management session within a given node.

`[-vserver <vserver>]` - Vserver

Selects the sessions that match this parameter value. This identifies the Vserver associated with this management session.

`[-username <text>]` - Username

Selects the sessions that match this parameter value. This identifies the authenticated user associated with this management session.

`[-application <text>]` - Client Application

Selects the sessions that match this parameter value. This identifies the calling application by name.

`[-location <text>]` - Client Location

Selects the sessions that match this parameter value. This identifies the location of the calling client application. This is typically the IP address of the calling client, or "console" or "localhost" for console or localhost connections.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When a session is not actively executing a command request (the session is idle), this indicates the time (in seconds) since the last request completed.

[-state {pending|active|idle}] - Session State

Selects the sessions that match this parameter value. This identifies the state (pending, active, or idle) of the session. The state is "pending" if it hit a session limit and the session is waiting for another session to end. The state is "idle" for CLI sessions that are waiting at the command prompt. The state is "active" if the session is actively working on a request.

[-request <text>] - Active Command

Selects the sessions that match this parameter value. This identifies the request (command) that is currently being handled by the session.

Examples

The following example illustrates killing a CLI session by specifying the node and the session id.

```
cluster1::> security session show -node node1

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 16:58:13 1358    console     console           cluster1 admin
-
    Active Seconds: 0  Request: security session show
03/27 16:58:17 1359    ssh         10.98.16.164      cluster1 admin
650
2 entries were displayed.

cluster1::>

cluster1::> security session kill-cli -node node1 -session-id 1359
1 entry was acted on.

cluster1::> security session show -node node1

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 16:58:13 1358    console     console           cluster1 admin
-
    Active Seconds: 0  Request: security session show

cluster1::>
```

The following example illustrates killing a CLI session by specifying the node and specifying a query on idle-seconds.

```
cluster1::> security session show -node node1

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 16:58:13 1358    console     console           cluster1 admin
-
    Active Seconds: 0  Request: security session show
03/27 17:13:36 1479    ssh         10.98.16.164      cluster1 admin
83
2 entries were displayed.

cluster1::> security session kill-cli -node node1 -session-id * -idle
-seconds > 80
1 entry was acted on.

cluster1::> security session show

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 16:58:13 1358    console     console           cluster1 admin
-
    Active Seconds: 0  Request: security session show

cluster1::>
```

security session show

Show current CLI, ONTAPI, and REST sessions

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

Description

The `security session show` command displays all active management sessions across the cluster.

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that is processing the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that is processing the session.

[-start-time <MM/DD HH:MM:SS>] - Start Time

Selects the sessions that match this parameter value. This identifies the start time of the current active session.

[-session-id <integer>] - Session ID

Selects the sessions that match this parameter value. This number uniquely identifies a management session within a given node.

[-vserver <vserver>] - Vserver

Selects the sessions that match this parameter value. This identifies the Vserver associated with this management session.

[-username <text>] - Username

Selects the sessions that match this parameter value. This identifies the authenticated user associated with this management session.

[-application <text>] - Client Application

Selects the sessions that match this parameter value. This identifies the calling application by name.

[-location <text>] - Client Location

Selects the sessions that match this parameter value. This identifies the location of the calling client application. This is typically the IP address of the calling client, or "console" or "localhost" for console or localhost connections.

[-ipspace <IPspace>] - IPspace of Location

Selects the sessions that match this parameter value. This identifies the IPspace of the client location.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made thus far in the active session. The following commands are not counted: top, up, cd, rows, history, exit.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that have failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took for this session.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took for this session.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that has been taken by all completed requests for the current session; it does not include session idle time.

[-state {pending|active|idle}] - Session State

Selects the sessions that match this parameter value. This identifies the state (pending, active, or idle) of the session. The state is "pending" if it hit a session limit and the session is waiting for another session to end. The state is "idle" for CLI sessions that are waiting at the command prompt. The state is "active" if the session is actively working on a request.

[-request <text>] - Request Input

Selects the sessions that match this parameter value. This identifies the request (command) that is currently being handled by the session.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When a session is not actively executing a command request (the session is idle), this indicates the time (in seconds) since the last request completed.

[-active-seconds <integer>] - Active Seconds

Selects the sessions that match this parameter value. When a session is actively executing a command request, this indicates the time (in seconds) since the current request started.

Examples

The following example illustrates displaying all active sessions across the cluster. In this example, we see one active session on node *node2* from the *console* application. We also see three active sessions on node *node1* . One is from the *console* application and two are from the *ssh* application. Also one of the *ssh* sessions is from user *diag* and the other *ssh* session is from user *admin* .

```
cluster1::> security session show

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 16:58:13 1358    console     console           cluster1 admin
-
    Active Seconds: 0  Request: security session show
03/27 17:17:04 1514    ssh         10.98.16.164      cluster1 admin
139
03/27 17:17:29 1515    ssh         10.98.16.164      cluster1 diag
115

Node: node2               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 17:18:54 1509    console     console           cluster1 admin
23
4 entries were displayed.

cluster1::>
```

The following example illustrates displaying all active sessions that have been idle for longer than 500 seconds.

```
cluster1::> security session show -idle-seconds > 500

Node: node1               Interface: cli
Idle
Start Time     Sess ID Application Location           Vserver Username
Seconds
-------------- ------- ----------- ------------ ------------- --------
--------
03/27 17:17:04 1514    ssh         10.98.16.164      cluster1 admin
607
03/27 17:17:29 1515    ssh         10.98.16.164      cluster1 diag
583
2 entries were displayed.

cluster1::>
```

security session limit create

Create default session limit

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

Description

This command allows creation of a default management session limit that does not yet exist. The default limits can be overridden for specific values within each category by using advanced privilege level commands.

Parameters

`-interface {cli|ontapi|rest}` - Interface

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-category {application|location|request|user|vserver}` - Category

The session type for this default limit. The following categories are supported: application, location, request, user, Vserver.

`-max-active-limit <integer>` - Max-Active Limit

The maximum number of concurrent sessions allowed for this interface and category.

Examples

The following example illustrates creating a default limit for management sessions using the same application.

```
cluster1::> security session limit create -interface ontapi -category
application -max-active-limit 8
```

security session limit delete

Delete default session limit

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

Description

This command allows deletion of a default management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-category {application|location|request|user|vserver}` - Category

The session type for this default limit. The following categories are supported: application, location, request, user, Vserver.

Examples

The following example illustrates deleting all default limits for CLI management sessions.

```
cluster1::> security session limit delete -interface cli -category *
3 entries were deleted.
```

security session limit modify

Modify default session limit

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

Description

This command allows modification of a default management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-category {application|location|request|user|vserver}` - Category

The session type for this default limit. The following categories are supported: application, location, request, user, Vserver.

`[-max-active-limit <integer>]` - Max-Active Limit

The maximum number of concurrent sessions allowed for this interface and category.

Examples

The following example illustrates modifying the default limit for CLI management sessions from the same location.

```
cluster1::> security session limit modify -interface cli -category
location -max-active-limit 4
```

security session limit show

Show default session limits

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

Description

This command shows the default management session limits that have been configured for each interface and category.

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.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-category {application|location|request|user|vserver}] - Category

Selects the sessions that match this parameter value. This identifies the category for the limit. The following categories are supported: application, location, request, user, and Vserver.

[-max-active-limit <integer>] - Max-Active Limit

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the default limits for management sessions.

```
cluster1::> security session limit show
Interface Category    Max-Active
--------- ----------- ----------
cli       user                 2
cli       vserver              4
ontapi    vserver              2
3 entries were displayed.
```

security session limit application create

Create per-application session limit

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

Description

This command allows creation of a per-application management session limit that does not yet exist.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-application <text>` - Application (privilege: advanced)

The specified application to which this limit applies. The limit with the application name *`-default-`* is the limit used for any application without a specific configured limit.

`-max-active-limit <integer>` - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and application.

Examples

The following example illustrates creating a limit for management sessions from a custom application.

```
cluster1::*> security session limit application create -interface ontapi
-application "custom_app" -max-active-limit 8
```

security session limit application delete

Delete per-application session limit

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

Description

This command allows deletion of a per-application management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-application <text>` - Application (privilege: advanced)

The specified application to which this limit applies. The limit with the application name *`-default-`* is the limit used for any application without a specific configured limit.

Examples

The following example illustrates deleting a limit for management sessions from a custom application.

```
cluster1::*> security session limit application delete -interface ontapi
-application "custom_app"
```

security session limit application modify

Modify per-application session limit

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

Description

This command allows modification of a per-application management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-application <text>` - Application (privilege: advanced)

The specified application to which this limit applies. The limit with the application name *`-default-`* is the limit used for any application without a specific configured limit.

`[-max-active-limit <integer>]` - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and application.

Examples

The following example illustrates modifying management session limits for some custom applications.

```
cluster1::*> security session limit application modify -interface ontapi
-application custom* -max-active-limit 4
2 entries were modified.
```

security session limit application show

Show per-application session limits

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

Description

This command shows the per-application management session limits that have been configured for each interface and application.

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.

[-interface {cli|ontapi|rest}] - Interface (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-application <text>] - Application (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the application for the limit. The limit with the application name *-default-* is the limit used for any application without a specific configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the per-application limits for ONTAPI management sessions.

```
cluster1::*> security session limit application show -interface ontapi
Interface Application          Max-Active
--------- -------------------- ----------
ontapi    -default-                     5
ontapi    custom_app                   10
2 entries were displayed.
```

security session limit location create

Create per-location session limit

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

Description

This command allows creation of a per-location management session limit that does not yet exist.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-location <text>` - Location (privilege: advanced)

The specified location to which this limit applies. The limit with the location name *`-default-`* (in the *`Default`* IPspace) is the limit used for any location (in any IPspace) without a specific configured limit.

`[-ipspace <IPspace>]` - IPspace of Location (privilege: advanced)

This identifies the IPspace of the client location. If not specified, changes are made in the *`Default`* IPspace.

`-max-active-limit <integer>` - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and location.

Examples

The following example illustrates creating a CLI limit for specific location.

```
cluster1::*> security session limit location create -interface cli
-location 10.98.16.164 -max-active-limit 1
```

security session limit location delete

Delete per-location session limit

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

Description

This command allows deletion of a per-location management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

-location <text> - Location (privilege: advanced)

The specified location to which this limit applies. The limit with the location name *-default-* (in the *Default* IPspace) is the limit used for any location (in any IPspace) without a specific configured limit.

[-ipspace <IPspace>] - IPspace of Location (privilege: advanced)

This identifies the IPspace of the client location. If not specified, changes are made in the *Default* IPspace.

Examples

The following example illustrates deleting limits for management sessions from a specific set of locations.

```
cluster1::*> security session limit location delete -interface * -location
10.98.*
3 entries were deleted.
```

security session limit location modify

Modify per-location session limit

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

Description

This command allows modification of a per-location management session limit.

Parameters

-interface {cli|ontapi|rest} - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

-location <text> - Location (privilege: advanced)

The specified location to which this limit applies. The limit with the location name *-default-* (in the *Default* IPspace) is the limit used for any location (in any IPspace) without a specific configured limit.

[-ipspace <IPspace>] - IPspace of Location (privilege: advanced)

This identifies the IPspace of the client location. If not specified, changes are made in the *Default* IPspace.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and location.

Examples

The following example illustrates modifying management sessions limits for specific locations.

```
cluster1::*> security session limit location modify -interface * -location
10.98.* -max-active-limit 2
3 entries were modified.
```

security session limit location show

Show per-location session limits

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

Description

This command shows the per-location management session limits that have been configured for each interface and location.

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.

[-interface {cli|ontapi|rest}] - Interface (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-location <text>] - Location (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the location for the limit. The limit with the location name *-default-* (only in the *Default* IPspace) is the limit used for any location (in any IPspace) without a specific configured limit.

[-ipspace <IPspace>] - IPspace of Location (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the IPspace of the client location. The default IPspace is *Default* .

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the per-location limits for management sessions.

```
cluster1::*> security session limit location show
Interface Location             IPspace     Max-Active
--------- -------------------- ----------- ----------
cli       -default-            Default             16
cli       10.98.16.164         Default              0
ontapi    -default-            Default              6
ontapi    10.98.16.164         Default              0
4 entries were displayed.
```

security session limit request create

Create per-request session limit

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

Description

This command allows creation of a per-request management session limit that does not yet exist.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-request <text>` - Request Name (privilege: advanced)

The specified request to which this limit applies. The limit with the request name *`-default-`* is the limit used for any request without a specific configured limit.

`-max-active-limit <integer>` - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and request.

Examples

The following example illustrates creating a limit for number of clients executing a specific API.

```
cluster1::*> security session limit request create -interface ontapi
-request storage-disk-get-iter -max-active-limit 2
```

security session limit request delete

Delete per-request session limit

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

Description

This command allows deletion of a per-request management session limit.

Parameters

-interface {cli|ontapi|rest} - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

-request <text> - Request Name (privilege: advanced)

The specified request to which this limit applies. The limit with the request name *-default-* is the limit used for any request without a specific configured limit.

Examples

The following example illustrates deleting custom limits for that were configured for the volume commands and APIs.

```
cluster1::*> security session limit request delete -interface * -request
volume*
4 entries were deleted.
```

security session limit request modify

Modify per-request session limit

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

Description

This command allows modification of a per-request management session limit.

Parameters

-interface {cli|ontapi|rest} - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

-request <text> - Request Name (privilege: advanced)

The specified request to which this limit applies. The limit with the request name *-default-* is the limit used for any request without a specific configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and request.

Examples

The following example illustrates modifying the limit of the number of clients simulatiously executing a specific API.

```
cluster1::*> security session limit request modify -interface ontapi
-request storage-disk-get-iter -max-active-limit 4
```

security session limit request show

Show per-request session limits

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

Description

This command shows the per-request management session limits that have been configured for each interface and request.

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.

[-interface {cli|ontapi|rest}] - Interface (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-request <text>] - Request Name (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the request (command or API) for the limit. The limit with the request name *`-default-`* is the limit used for any request without a specific configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the per-request limits for management sessions.

```
cluster1::*> security session limit request show
Interface Request                          Max-Active
--------- -------------------------------- ----------
cli       -default-                                10
ontapi    -default-                                 5
ontapi    storage-disk-get-iter                     2
3 entries were displayed.
```

security session limit user create

Create per-user session limit

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

Description

This command allows creation of a per-user management session limit that does not yet exist.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-vserver <vserver>` - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

`-user <text>` - User (privilege: advanced)

The specified user to which this limit applies. The limit with the user name *`-default-`* is the limit used for any user without a specific configured limit.

`-max-active-limit <integer>` - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface, Vserver, and user.

Examples

The following example illustrates creating a per-user limit override for ONTAPI requests for the *`admin`* user in the admin Vserver.

```
cluster1::*> security session limit user create -interface ontapi -vserver
cluster1 -username admin -max-active-limit 16
```

security session limit user delete

Delete per-user session limit

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

Description

This command allows deletion of a per-user management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-vserver <vserver>` - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

`-user <text>` - User (privilege: advanced)

The specified user to which this limit applies. The limit with the user name *`-default-`* is the limit used for any user without a specific configured limit.

Examples

The following example illustrates deleting all user-specific limits for CLI management sessions.

```
cluster1::*> security session limit user delete -interface cli -user !"-
default-"
2 entries were deleted.
```

security session limit user modify

Modify per-user session limit

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

Description

This command allows modification of a per-user management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-vserver <vserver>` - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

`-user <text>` - User (privilege: advanced)

The specified user to which this limit applies. The limit with the user name *`-default-`* is the limit used for

any user without a specific configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface, Vserver, and user.

Examples

The following example illustrates modifying the admin user's limit for CLI management sessions.

```
cluster1::*> security session limit user modify -interface cli -vserver
cluster1 -username admin -max-active-limit 30
```

security session limit user show

Show per-user session limits

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

Description

This command shows the per-user management session limits that have been configured for each interface, Vserver, and user.

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.

[-interface {cli|ontapi|rest}] - Interface (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-vserver <vserver>] - Vserver (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the Vserver for the limit. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

[-user <text>] - User (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the user for the limit. The limit with the user name *`-default-`* is the limit used for any user without a specific configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the per-user limits for CLI management sessions. In this example, there is a default limit of 4 sessions for each user. That limit is expanded to 8 for the admin Vserver. That limit is further expanded to 20 for the *admin* user in the admin Vserver.

```
cluster1::*> security session limit user show -interface cli
Interface Vserver              User                Max-Active
--------- -------------------- ------------------- ----------
cli       Cluster              -default-                    4
cli       cluster1             -default-                    8
cli       cluster1             admin                       20
3 entries were displayed.
```

security session limit vserver create

Create per-vserver session limit

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

Description

This command allows creation of a per-Vserver management session limit that does not yet exist.

Parameters

-interface {cli|ontapi|rest} - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

-vserver <vserver> - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

-max-active-limit <integer> - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and Vserver.

Examples

The following example illustrates creating a per-Vserver limit override for ONTAPI requests on the admin Vserver.

```
cluster1::*> security session limit vserver create -interface ontapi
-vserver cluster1 -max-active-limit 4
```

security session limit vserver delete

Delete per-vserver session limit

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

Description

This command allows deletion of a per-Vserver management session limit. The "Cluster" vserver is used when the specific Vserver doesn’t have a configured limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-vserver <vserver>` - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

Examples

The following example illustrates deleting all per-Vserver limits for management sessions except the default limit.

```
cluster1::*> security session limit vserver delete -interface * -vserver
!Cluster
1 entries was deleted.
```

security session limit vserver modify

Modify per-vserver session limit

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

Description

This command allows modification of a per-Vserver management session limit.

Parameters

`-interface {cli|ontapi|rest}` - Interface (privilege: advanced)

The interface (CLI, ONTAPI, or REST) to which the limit applies.

`-vserver <vserver>` - Vserver (privilege: advanced)

The specified Vserver to which this limit applies. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

The maximum number of concurrent sessions allowed for this interface and Vserver.

Examples

The following example illustrates modifying the admin Vserver's limit for CLI management sessions.

```
cluster1::*> security session limit vserver modify -interface cli -vserver
cluster1 -max-active-limit 40
```

security session limit vserver show

Show per-vserver session limits

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

Description

This command shows the per-Vserver management session limits that have been configured for each interface and Vserver.

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.

[-interface {cli|ontapi|rest}] - Interface (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) to which the limit applies.

[-vserver <vserver>] - Vserver (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the Vserver for the limit. The "Cluster" Vserver is used to limit Vservers that do not have a configured limit.

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying the per-Vserver limits for management sessions.

```
cluster1::*> security session limit vserver show
Interface Vserver              Max-Active
--------- -------------------- ----------
cli       Cluster                       4
ontapi    Cluster                       2
ontapi    cluster1                     16
3 entries were displayed.
```

security session request-statistics show-by-application

Show session request statistics by application

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

Description

The `security session request-statistics show-by-application` command shows historical statistics for management session activity, categorized by application name. CLI sessions connections will have an application name based on the connection method, i.e.: *`ssh`* , *`telnet`* , *`rsh`* , *`console`* , or *`ngsh`* . ONTAPI sessions will extract the application name from the ZAPI request. ONTAP looks for the application name in the following three locations, in the following order of precedence:

```
     1. The "X-Dot-Client-App" HTTP header;
     2. The "app-name" attribute of the "netapp" element, within the ZAPI
XML request;
     3. The "User-Agent" HTTP header.
```

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that processed the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that processed the session.

[-application <text>] - Application

Selects the sessions that match this parameter value. This identifies the calling application by name.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made on a session. The following commands are not counted: top, up, cd, rows, history, exit.

[-blocked <integer>] - Blocked Requests

Selects the sessions that match this parameter value. This identifies the number of requests that were blocked due to configured limits.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took.

[-active <integer>] - Number Active Now

Selects the sessions that match this parameter value. This identifies the number of currently active sessions.

[-max-active <integer>] - Max Number Active

Selects the sessions that match this parameter value. This identifies the maximum number of concurrently active sessions.

[-last-active-seconds <integer>] - Seconds Since Last Session Start

Selects the sessions that match this parameter value. When a session is active, this indicates the time (in seconds) since the last session started.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When no sessions are active, this indicates the time (in seconds) since the last session ended.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that have been taken by all completed requests; it does not include session idle time.

[-average-time <integer>] - Average Time (ms)

Selects the sessions that match this parameter value. This identifies the mean time spent processing requests.

[-success-percent <percent>] - Success Percent

Selects the sessions that match this parameter value. This identifies the percentage of successful requests.

[-blocked-percent <percent>] - Blocked Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that were blocked due to configured limits.

[-failed-percent <percent>] - Failed Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that failed for any reason (including if they were blocked by configured limits).

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying historical statistics for all management session activity across the cluster, categorized by application name.

```
cluster1::> security session request-statistics show-by-application

Node: node1                Interface: cli                  Idle    Total
Application                   Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
console                        2126   0   6  95%   96       68      361
170
ssh                               6   2   3 100%    0        -      794
132444

Node: node1                Interface: ontapi               Idle    Total
Application                   Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
api_test                          2   0   1 100%    0       13        0
18

Node: node2                Interface: cli                  Idle    Total
Application                   Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
console                        2090   0   6  95%   96       90      655
313
4 entries were displayed.

cluster1::>
```

The following example illustrates displaying historical statistics for management session activity on a specific node and for a specific application.

```
cluster1::> security session request-statistics show-by-application -node
node1 -application api_test

Node: node1                Interface: ontapi              Idle    Total
Application                   Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
api_test                          2   0   1 100%    0      102        0
18

cluster1::>
```

security session request-statistics show-by-location

Show session request statistics by location

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

Description

The `security session request-statistics show-by-location` command shows historical statistics for management session activity, categorized by client location.

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that processed the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that processed the session.

[-location <text>] - Client Location

Selects the sessions that match this parameter value. This identifies the location of the calling client application. This is typically the IP address of the calling client, or "console" or "localhost" for console or localhost connections.

[-ipspace <IPspace>] - IPspace of Location

Selects the sessions that match this parameter value. This identifies the IPspace of the client location.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made on a session. The following commands are not counted: top, up, cd, rows, history, exit.

[-blocked <integer>] - Blocked Requests

Selects the sessions that match this parameter value. This identifies the number of requests that were blocked due to configured limits.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took.

[-active <integer>] - Number Active Now

Selects the sessions that match this parameter value. This identifies the number of currently active sessions.

[-max-active <integer>] - Max Number Active

Selects the sessions that match this parameter value. This identifies the maximum number of concurrently active sessions.

[-last-active-seconds <integer>] - Seconds Since Last Session Start

Selects the sessions that match this parameter value. When a session is active, this indicates the time (in seconds) since the last session started.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When no sessions are active, this indicates the time (in seconds) since the last session ended.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that have been taken by all completed requests; it does not include session idle time.

[-average-time <integer>] - Average Time (ms)

Selects the sessions that match this parameter value. This identifies the mean time spent processing requests.

[-success-percent <percent>] - Success Percent

Selects the sessions that match this parameter value. This identifies the percentage of successful requests.

[-blocked-percent <percent>] - Blocked Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that were blocked due to configured limits.

[-failed-percent <percent>] - Failed Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that failed for any reason (including if they were blocked by configured limits).

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying historical statistics for all management session activity across the cluster, categorized by location.

```
cluster1::> security session request-statistics show-by-location

Node: node1               Interface: cli                 Idle    Total
Location          IPspace    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
----------------- ------- -------- --- --- ---- ---- -------- --------
--------
console           Default       21   1   1 100%    0        -      127
6063
localhost         Default     2523   0   5  95%  115       20      280
111

Node: node1               Interface: ontapi              Idle    Total
Location          IPspace    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
----------------- ------- -------- --- --- ---- ---- -------- --------
--------
10.98.17.254      Default        2   0   1 100%    0     2419        0
18

Node: node2               Interface: cli                 Idle    Total
Location          IPspace    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
----------------- ------- -------- --- --- ---- ---- -------- --------
--------
console           Default        6   0   1  83%    1     2941      423
70557
localhost         Default     2502   0   5  95%  114       41      277
110
7 entries were displayed.

cluster1::>
```

The following example illustrates displaying historical statistics for management session activity on a specific node and for a specific location.

```
cluster1::> security session request-statistics show-by-location -node
node2 -location localhost

Node: node2               Interface: cli                  Idle    Total
Location          IPspace    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
----------------- ------- -------- --- --- ---- ---- -------- --------
--------
localhost         Default     2524   0   5  95%  115       30      279
110

cluster1::>
```

security session request-statistics show-by-request

Show session request statistics by request name

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

Description

The `security session request-statistics show-by-request` command shows historical statistics for management session activity, categorized by request (command or API name).

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that processed the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that processed the session.

[-request <text>] - Request Name

Selects the sessions that match this parameter value. This identifies the command associated with these requests.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made on a session. The following commands are not counted: top, up, cd, rows, history, exit.

[-blocked <integer>] - Blocked Requests

Selects the sessions that match this parameter value. This identifies the number of requests that were blocked due to configured limits.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took.

[-active <integer>] - Number Active Now

Selects the sessions that match this parameter value. This identifies the number of currently active requests.

[-max-active <integer>] - Max Number Active

Selects the sessions that match this parameter value. This identifies the maximum number of concurrently active requests.

[-last-active-seconds <integer>] - Seconds Since Last Request Start

Selects the sessions that match this parameter value. When requests are active, this indicates the time (in seconds) since the last request started.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When no requests are active, this indicates the time (in seconds) since the last request ended.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that have been taken by all completed requests; it does not include session idle time.

[-average-time <integer>] - Average Time (ms)

Selects the sessions that match this parameter value. This identifies the mean time spent processing requests.

[-success-percent <percent>] - Success Percent

Selects the sessions that match this parameter value. This identifies the percentage of successful requests.

[-blocked-percent <percent>] - Blocked Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that were blocked due to configured limits.

[-failed-percent <percent>] - Failed Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that failed for any reason (including if they were blocked by configured limits).

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying historical statistics for all management session activity on a specific node, with a specific request query.

```
cluster1::> security session request-statistics show-by-request -node
node1 -request network*

Node: node1                Interface: cli                  Idle    Total
Request Name                  Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
network interface create          2   0   1 100%    0     2556        0
485
network interface modify          1   0   1 100%    0     2518        0
34
network interface show            8   0   1 100%    0     2152       12
1614
network route create              1   0   1 100%    0     2135        0
45
network route show                2   0   1 100%    0     2145        0
17
5 entries were displayed.

cluster1::>
```

security session request-statistics show-by-user

Show session request statistics by username

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

Description

The `security session request-statistics show-by-user` command shows historical statistics for management session activity, categorized by username. Entries for username 'autosupport' reflect commands that are executed by the AutoSupport OnDemand feature.

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that processed the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that processed the session.

[-vserver <vserver>] - Vserver

Selects the sessions that match this parameter value. This identifies the Vserver associated with this management session.

[-username <text>] - Username

Selects the sessions that match this parameter value. This identifies the authenticated user associated with this management session.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made on a session. The following commands are not counted: top, up, cd, rows, history, exit.

[-blocked <integer>] - Blocked Requests

Selects the sessions that match this parameter value. This identifies the number of requests that were blocked due to configured limits.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took.

[-active <integer>] - Number Active Now

Selects the sessions that match this parameter value. This identifies the number of currently active sessions.

[-max-active <integer>] - Max Number Active

Selects the sessions that match this parameter value. This identifies the maximum number of concurrently active sessions.

[-last-active-seconds <integer>] - Seconds Since Last Session Start

Selects the sessions that match this parameter value. When a session is active, this indicates the time (in seconds) since the last session started.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When no sessions are active, this indicates the time (in seconds) since the last session ended.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that have been taken by all completed requests; it does not include session idle time.

[-average-time <integer>] - Average Time (ms)

Selects the sessions that match this parameter value. This identifies the mean time spent processing requests.

[-success-percent <percent>] - Success Percent

Selects the sessions that match this parameter value. This identifies the percentage of successful requests.

[-blocked-percent <percent>] - Blocked Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that were blocked due to configured limits.

[-failed-percent <percent>] - Failed Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that failed for any reason (including if they were blocked by configured limits).

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying historical statistics for all management session activity across the cluster, categorized by username.

```
cluster1::> security session request-statistics show-by-user

Node: node1                Interface: cli                  Idle    Total
Vserver          Username    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------- ---------- -------- --- --- ---- ---- -------- --------
--------
cluster1            admin       81   1   3  80%   16        -     1228
15171
                     diag        1   0   1 100%    0     1982     1511
1511958
              autosupport        4   0   1 100%    0        -        0
17

Node: node1                Interface: ontapi               Idle    Total
Vserver          Username    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------- ---------- -------- --- --- ---- ---- -------- --------
--------
cluster1            admin        2   0   1 100%    0     2585        0
18

Node: node2                Interface: cli                  Idle    Total
Vserver          Username    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------- ---------- -------- --- --- ---- ---- -------- --------
--------
cluster1            admin        6   1   1  83%    1     3106      423
70557
4 entries were displayed.

cluster1::>
```

The following example illustrates displaying historical statistics for management session activity on a specific node and for a specific username.

```
cluster1::> security session request-statistics show-by-user -node node1
-username diag

Node: node1                Interface: cli                  Idle    Total
Vserver          Username    Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------- ---------- -------- --- --- ---- ---- -------- --------
--------
cluster1             diag        1   0   1 100%    0        -     1511
1511958

cluster1::>
```

security session request-statistics show-by-vserver

Show session request statistics by Vserver

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

Description

The `security session request-statistics show-by-vserver` command shows historical statistics for management session activity, categorized by vserver.

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.

[-node {<nodename>|local}] - Node

Selects the sessions that match this parameter value. This identifies the node that processed the session.

[-interface {cli|ontapi|rest}] - Interface

Selects the sessions that match this parameter value. This identifies the interface (CLI, ONTAPI, or REST) that processed the session.

[-vserver <vserver>] - Vserver

Selects the sessions that match this parameter value. This identifies the Vserver associated with this management session.

[-total <integer>] - Total Requests

Selects the sessions that match this parameter value. This identifies the total number of requests that have been made on a session. The following commands are not counted: top, up, cd, rows, history, exit.

[-blocked <integer>] - Blocked Requests

Selects the sessions that match this parameter value. This identifies the number of requests that were blocked due to configured limits.

[-failed <integer>] - Failed Requests

Selects the sessions that match this parameter value. This identifies the number of requests that failed for any reason (including if they were blocked by configured limits).

[-max-time <integer>] - Maximum Time (ms)

Selects the sessions that match this parameter value. This identifies the maximum amount of time (in milliseconds) that any request took.

[-last-time <integer>] - Last Time (ms)

Selects the sessions that match this parameter value. This identifies the amount of time (in milliseconds) that the last request took.

[-active <integer>] - Number Active Now

Selects the sessions that match this parameter value. This identifies the number of currently active sessions.

[-max-active <integer>] - Max Number Active

Selects the sessions that match this parameter value. This identifies the maximum number of concurrently active sessions.

[-last-active-seconds <integer>] - Seconds Since Last Session Start

Selects the sessions that match this parameter value. When a session is active, this indicates the time (in seconds) since the last session started.

[-idle-seconds <integer>] - Idle Seconds

Selects the sessions that match this parameter value. When no sessions are active, this indicates the time (in seconds) since the last session ended.

[-total-seconds <integer>] - Total Seconds

Selects the sessions that match this parameter value. This identifies the total time (in seconds) that have been taken by all completed requests; it does not include session idle time.

[-average-time <integer>] - Average Time (ms)

Selects the sessions that match this parameter value. This identifies the mean time spent processing requests.

[-success-percent <percent>] - Success Percent

Selects the sessions that match this parameter value. This identifies the percentage of successful requests.

[-blocked-percent <percent>] - Blocked Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that were blocked due to configured limits.

[-failed-percent <percent>] - Failed Percent

Selects the sessions that match this parameter value. This identifies the percentage of requests that failed for any reason (including if they were blocked by configured limits).

[-max-active-limit <integer>] - Max-Active Limit (privilege: advanced)

Selects the sessions that match this parameter value. This identifies the configured limit that is used to throttle or reject requests.

Examples

The following example illustrates displaying historical statistics for all management session activity across the cluster, categorized by Vserver.

```
cluster1::> security session request-statistics show-by-vserver

Node: node1                Interface: cli                 Idle    Total
Vserver                       Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------------------- -------- --- --- ---- ---- -------- --------
--------
cluster1                       2725   1   8  94%  146        -     3052
1120

Node: node1                Interface: ontapi              Idle    Total
Vserver                       Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------------------- -------- --- --- ---- ---- -------- --------
--------
cluster1                           2   0   1 100%    0     2742        0
18

Node: node2                Interface: cli                 Idle    Total
Vserver                       Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
-------------------------- -------- --- --- ---- ---- -------- --------
--------
cluster1                       2552   1   6  95%  117        -      705
276
3 entries were displayed.

cluster1::>
```

The following example illustrates displaying historical statistics for management session activity on a specific node, for a specific Vserver.

```
cluster1::> security session request-statistics show-by-vserver -node
node1 -vserver cluster1

Node: node1               Interface: cli                 Idle    Total
Vserver                      Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
cluster1                      2747   1   8  94%  147        -     3055
1112

Node: node1               Interface: ontapi              Idle    Total
Vserver                      Total Now Max Pass Fail  Seconds  Seconds Avg
(ms)
------------------------- -------- --- --- ---- ---- -------- --------
--------
cluster1                          2   0   1 100%    0     2902        0
18
2 entries were displayed.

cluster1::>
```

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.