



# **system services commands**

ONTAP 9.9.1 commands

NetApp  
September 27, 2022

# Table of Contents

system services commands	1
system services firewall modify	1
system services firewall show	1
system services firewall policy clone	2
system services firewall policy create	3
system services firewall policy delete	4
system services firewall policy modify	5
system services firewall policy show	6
system services manager install show	8
system services manager policy add	9
system services manager policy remove	10
system services manager policy setstate	10
system services manager policy show	11
system services manager status show	12
system services ndmp kill-all	14
system services ndmp kill	14
system services ndmp modify	15
system services ndmp off	16
system services ndmp on	16
system services ndmp password	17
system services ndmp probe	18
system services ndmp show	23
system services ndmp status	25
system services ndmp log start	30
system services ndmp log stop	33
system services ndmp node-scope-mode off	34
system services ndmp node-scope-mode on	34
system services ndmp node-scope-mode status	35
system services ndmp service modify	35
system services ndmp service show	36
system services ndmp service start	37
system services ndmp service stop	38
system services ndmp service terminate	38
system services web modify	39
system services web show	40
system services web node show	41

# system services commands

## system services firewall modify

Modify firewall status

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

### Description

The `system services firewall modify` command modifies a node's firewall configuration.

### Parameters

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

Use this parameter to specify the node on which to modify firewall configuration.

**[-enabled {true|false}] - Service Enabled**

Use this parameter to specify whether firewall protection is enabled ("*true*") or disabled ("*false*") for the node's network ports. The default setting is *true*.

**[-logging {true|false}] - (DEPRECATED)-Enable Logging**



This parameter is deprecated and may be removed in a future version of Data ONTAP.

Use this parameter to specify whether logging is enabled ("*true*") or disabled ("*false*") for the firewall service. The default setting is *false*.

### Examples

The following example enables firewall protection and logging for a node named `node1`:

```
cluster1::> system services firewall modify -node node1 -enabled true
-logging true
```

## system services firewall show

Show firewall status

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

### Description

The `system services firewall show` command displays firewall configuration and logging information. If the command is issued without any parameters, it displays information about all nodes in the cluster. You can also query specific nodes for their firewall information by running the command with the `-node` parameter.

## 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 information about the firewall settings on the node you specify.

**[-enabled {true|false}] - Service Enabled**

Selects information about the nodes with the firewall enabled ("*true*") or disabled ("*false*").

**[-logging {true|false}] - (DEPRECATED)-Enable Logging**



This parameter is deprecated and may be removed in a future version of Data ONTAP.

Selects information about the nodes with firewall logging enabled ("*true*") or disabled ("*false*").

## Examples

The following example displays information about firewall configuration for all nodes in the cluster:

```
cluster1::> system services firewall show
Node           Enabled Logging
-----
node0          true    false
node1          true    false
node2          true    false
node3          true    false
4 entries were displayed.
```

## system services firewall policy clone

Clone an existing firewall policy

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

### Description

The `system services firewall policy clone` command creates a new firewall policy that is an exact copy of an existing policy, but has a new name.

## Parameters

**-vserver <text> - Vserver owning the Policy**

Use this parameter to specify the name of the Vserver owning the existing policy to copy.

**-policy <text> - Firewall Policy to be Cloned**

Use this parameter to specify the name of the existing policy to copy.

**[-destination-vserver <text>] - Vserver owning the New Firewall Policy**

Use this parameter to specify the name of the Vserver that will own the new policy to create.

**-destination-policy <text> - Name of New Firewall Policy**

Use this parameter to specify the name of the new policy to create.

## Examples

This example creates a new firewall policy named "data2" on Vserver "vs0" from an existing firewall policy named "data" on Vserver "vs1".

```
cluster1::> system services firewall policy clone -vserver vs0 -policy
data -destination-vserver vs1 -destination-policy data2
```

## system services firewall policy create

Create a firewall policy entry for a network service

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

### Description

The `system services firewall policy create` command creates a firewall policy entry with the specified name and network service. This command is used both to create the first network service associated with a new firewall policy, and to add to an existing firewall policy by associating another network service with an existing policy. You can optionally specify one or more IP addresses with corresponding netmasks that are allowed to use the firewall policy entry.

You can use the [network interface modify](#) command with the `-firewall-policy` parameter to put a firewall policy into effect for a given logical interface by modifying that logical interface to use the specified firewall policy.

### Parameters

**-vserver <vserver> - Vserver Name**

Use this parameter to specify the name of the Vserver on which the policy is to be created.

**-policy <textpolicy\_name> - Policy**

Use this parameter to specify the name of the policy that is to be created.

**-service <service> - Service**

Use this parameter to specify the network service that is associated with the policy. Possible values include:

- dns - The DNS protocol server
- http - The HTTP protocol
- ndmp - The NDMP tape backup protocol
- ndmps - The NDMPs tape backup protocol
- none - No protocol (for creating an empty policy)
- ntp - The NTP protocol
- rsh - The RSH protocol
- snmp - The SNMP protocol
- telnet - The Telnet protocol

**-allow-list <IP Address/Mask>,... - Allowed IPs**

Use this parameter to specify one or more IP addresses with corresponding netmasks that are to be allowed by this firewall policy. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25". Multiple address/netmask pairs should be separated with commas. Use the value 0.0.0.0/0 for "any".

## Examples

The following example creates a firewall policy named data that uses the NDMP protocol and enables access from all IP addresses on the 192.0.2.128/25 subnet:

```
cluster1::> system services firewall policy create -policy data -service
ndmp -allow-list 192.0.2.128/25
```

The following example adds an entry to the firewall policy named data, associating the DNS protocol with that policy and enabling access from all IP addresses on the 192.0.2.128/25 subnet:

```
cluster1::> system services firewall policy create -policy data -service
dns -allow-list 192.0.2.128/25
```

## Related Links

- [network interface modify](#)

# system services firewall policy delete

Remove a service from a firewall policy

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

## Description

The `system services firewall policy delete` command deletes a firewall policy. You cannot delete a policy that is being used by a logical interface. Use the [network interface modify](#) command with the `-firewall-policy` parameter to change a network interface's firewall policy.

## Parameters

### **-vserver <vserver> - Vserver Name**

Use this parameter to specify the Vserver of the policy to delete.

### **-policy <textpolicy\_name> - Policy**

Use this parameter to specify the name of the policy to delete.

### **-service <service> - Service**

Use this parameter to specify the policy's network service to delete.

## Examples

The following example deletes a firewall policy that uses the Telnet protocol on the policy named data:

```
cluster1::> system services firewall policy delete -policy data -service telnet
```

Use wildcards to delete entire policies at once, or particular services from every policy. This example deletes the entire intercluster policy.

```
cluster1::> system services firewall policy delete -policy intercluster -service *
```

This example deletes the telnet service from every policy.

```
cluster1::> system services firewall policy delete -policy * -service telnet
```

## Related Links

- [network interface modify](#)

## system services firewall policy modify

Modify a firewall policy entry for a network service

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

## Description

The [system services firewall modify](#) command enables you to modify the list of IP addresses and netmasks associated with a firewall policy.

## Parameters

### **-vserver <vserver> - Vserver Name**

Use this parameter to specify the Vserver of the policy to modify.

### **-policy <textpolicy\_name> - Policy**

Use this parameter to specify the name of the policy to modify.

### **-service <service> - Service**

Use this parameter to specify the policy's network service to modify.

### **[-allow-list <IP Address/Mask>,...] - Allowed IPs**

Use this parameter to specify one or more IP addresses with corresponding netmasks that are allowed by this firewall policy. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25".

Multiple address/netmask pairs should be separated with commas. Use the value 0.0.0.0/0 for "any".

## Examples

The following example modifies the firewall policy named data that uses the NDMP protocol to enable access from all addresses on the 192.0.2.128 subnet:

```
cluster1::> system services firewall policy modify -policy data -service
ndmp -allow-list 192.0.2.128/25
```

## Related Links

- [system services firewall modify](#)

# system services firewall policy show

Show firewall policies

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

## Description

The `system services firewall policy show` command displays information about firewall policies.

## Parameters

**{ [-fields <fieldname>,...]**

If you specify the `-fields <fieldname>,...` parameter, the command displays only the fields that you specify.

**| [-instance ] }**

Use this parameter to display all the fields for the specified policies.



**[-vserver <vserver>] - Vserver Name**

Use this parameter to display information only about the Vserver you specify.

**[-policy <textpolicy\_name>] - Policy**

Use this parameter to display information about the policy you specify.

**[-service <service>] - Service**

Use this parameter to display information about the services you specify.

**[-allow-list <IP Address/Mask>, ...] - Allowed IPs**

Use this parameter to display information about the firewall policies that match the list of allowed IP addresses and netmasks you specify. The correct format for this parameter is address/netmask, similar to "192.0.2.128/25". Multiple address/netmask pairs should be separated with commas.

**[-ipSPACE <text>] - IPspace**

Use this parameter to display information only about the IPspace you specify.

## Examples

The following example displays information about all firewall policies:

```

cluster1::> system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster1
  data
    dns          0.0.0.0/0, ::/0
    ndmp         0.0.0.0/0, ::/0
    ndmps       0.0.0.0/0, ::/0
cluster1
  intercluster
    ndmp         0.0.0.0/0, ::/0
    ndmps       0.0.0.0/0, ::/0
cluster1
  mgmt
    dns          0.0.0.0/0, ::/0
    http         0.0.0.0/0, ::/0
    ndmp         0.0.0.0/0, ::/0
    ndmps       0.0.0.0/0, ::/0
    ntp         0.0.0.0/0, ::/0
    snmp        0.0.0.0/0, ::/0
cluster1
  mgmt-nfs
    dns          0.0.0.0/0, ::/0
    http         0.0.0.0/0, ::/0
    ndmp         0.0.0.0/0, ::/0
    ndmps       0.0.0.0/0, ::/0
    ntp         0.0.0.0/0, ::/0
    snmp        0.0.0.0/0, ::/0
17 entries were displayed.

cluster1::>

```

## system services manager install show

Display a list of installed services

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

### Description

The `system services manager install show` command displays information about installed services.

### 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.

**[-service <text>] - Service**

Selects information about installed services that have the name you specify.

**[-version <service version>] - Version**

Selects information about installed services that have the version number you specify.

**[-constituent <text>] - Constituent**

Selects information about installed services that have the constituent process you specify.

**[-nodes {<nodename>|local}] - Nodes**

Selects information about services that are installed on the nodes you specify.

**[-description <text>] - Description**

Selects information about installed services that match the description you specify.

## Examples

The following example shows typical output from a two-node cluster.

```
cluster1::> system services manager install show
Service          Version Constituent Nodes
-----
diagnosis
                1.0      schmd      node1, node2
                1.0      shmd      node1, node2
2 entries were displayed.
```

## system services manager policy add

Add a new service policy

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

### Description

The `system services manager policy add` command adds a new service policy to the services manager. Policies determine which versions of a service can run on the nodes of the cluster.

## Parameters

### **-service <text> - Service**

Use this parameter to specify the name of the service for which to add a policy.

### **-version <service version> - Version**

Use this parameter to specify the minimum version number of the service to run.

## Examples

This example adds a service manager policy for version 1.0 of the diagnosis service.

```
cluster1::> system services manager policy add -service diagnosis -version
1.0
```

## system services manager policy remove

Remove a service policy

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

### Description

The `system services manager policy remove` command removes a policy from the services manager. Policies determine which versions of a service can run on the nodes of the cluster.

### Parameters

#### **-service <text> - Service**

Use this parameter to specify the name of the service from which to remove a policy.

#### **-version <service version> - Version**

Use this parameter to specify the version number that is configured by the policy to remove.

### Examples

The following example shows the removal of the service policy for version 1.0 of the diagnosis service.

```
cluster1::> system services manager policy remove -service diagnosis
-version 1.0
```

## system services manager policy setstate

Enable/disable a service policy

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

## Description

The `system services manager policy setstate` command enables or disables services manager policies. Use the [system services manager policy show](#) command to display information about configured policies.

## Parameters

### **-service <text> - Service**

Use this parameter to set the state of the policy you specify.

### **-version <service version> - Version**

Use this parameter to set the state of the policy with the version number you specify.

### **-state {on|off} - State**

Use this parameter with the value "on" to enable the policy. Use this parameter with the value "off" to disable the policy.

## Examples

The following example sets the policy for version 1.0 of the diagnosis service to off.

```
cluster1::> system services manager policy setstate -service diagnosis
-version 1.0 -state off
```

## Related Links

- [system services manager policy show](#)

# system services manager policy show

Display service policies

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

## Description

The `system services manager policy show` command displays information about policies that determine which versions of a service can run on the nodes of the cluster.

Use the [system services manager status show](#) command to view information about services that are configured to run in 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.

**[`-service` <text>] - Service**

Selects policies that apply to the service you specify.

**[`-version` <service version>] - Version**

Selects policies that have the version number you specify.

**[`-constituent` <text>] - Constituent**

Selects policies that have the constituent process you specify.

**[`-state` {on|off}] - State**

Use this parameter with the value "on" to select information about policies that are currently active. Use this parameter with the value "off" to select information about policies that are not currently active.

**[`-num-active` <integer>] - Number Active**

Selects policies that have the number of active (running) instances you specify.

**[`-target-nodes` <service affinity>,...] - Target Nodes**

Selects policies that are configured to run on the nodes you specify.

**[`-tag` <UUID>] - Tag**

Selects policies that have the UUID you specify. Use this parameter with the `-fields` parameter to display a list of the UUIDs of configured services.

## Examples

The following example shows typical output for this command.

```
cluster1::> system services manager policy show
Service          Version State Constituent Number Target
                  Active Nodes
-----
-----
diagnosis
                1.0    on    schmd     1      any
                1.0    on    shmd     1      any
2 entries were displayed.
```

## Related Links

- [system services manager status show](#)

# system services manager status show

Display the status of a service

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

## Description

The `system services manager status show` command displays the status of system services that are configured to run in the cluster.

System services run on the nodes of the cluster based on policies. Policies determine which versions of a service can run on the nodes of the cluster. Use the [system services manager policy show](#) command to view existing policies.

## 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.

**[-service <text>] - Service**

Selects information about services that match the service name you specify.

**[-version <service version>] - Version**

Selects information about services that are configured to run the version number you specify. The configured version is the minimum version that is allowed to run in the cluster according to a policy. Use the [system services manager policy show](#) command to view information about service policies.

**[-constituent <text>] - Constituent**

Selects information about services that have the constituent process you specify.

**[-actual-version <service version>] - Actual Version**

Selects information about services that are running the version number you specify. This number can be higher than the configured version if a more recent version is installed on the node that is running the service.

**[-node <nodename>] - Node**

Selects information about services that the services manager has assigned to run on the nodes you specify. If the service state is "running", the service is running on these nodes.

**[-state <svc\_state>] - State**

Selects information about services that are in the state you specify.

**[-is-running {true|false}] - Is Running**

Use this parameter with the value "true" to select information about services that are currently running. Use this parameter with the value "false" to select information about services that are not currently running.

## Examples

The example below shows typical output for a simple cluster.

```

cluster1::> system services manager status show
Service          Version Constituent Actual  Node           State
                  Version
-----
diagnosis
                1.0      schmd      1.0    cluster1-01    running
                1.0      shmd      1.0    cluster1-01    running
2 entries were displayed.

```

## Related Links

- [system services manager policy show](#)

## system services ndmp kill-all

Kill all NDMP sessions

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

### Description

The `system services ndmp kill-all` command is used to terminate all NDMP sessions on a particular node in the cluster.

### Parameters

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

Node on which all NDMP sessions needs to be terminated.

### Examples

The following example shows how all NDMP sessions on the node named `node1` can be terminated:

```
cluster1::> system services ndmp kill-all -node node1
```

## system services ndmp kill

Kill the specified NDMP session

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

### Description

The `system services ndmp kill` command is used to terminate a specific NDMP session on a particular node in the cluster.



## Parameters

### <integer> - Session Identifier

Session ID of the NDMP session.

## Examples

The following example shows how a specific NDMP session on the node named `node1` can be terminated:

```
cluster1::> system services ndmp kill 4323 -node node1
```

## system services ndmp modify

(DEPRECATED)-Modify NDMP service configuration

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp modify](#)" command.

The `system services ndmp modify` command allows you to modify the NDMP configurations for a node in the cluster. One or more of the following configurations can be modified:

- Enable/disable NDMP service
- Enable/disable sending the NDMP password in clear text. Note that MD5 authentication mode is always enabled.
- NDMP user ID

## Parameters

### **-node {<nodename>|local}** - Node

This specifies the node whose NDMP configuration is to be modified.

### **[-enable {true|false}]** - NDMP Service Enabled

This optionally specifies whether NDMP is enabled on the node. The default setting is `true`.

### **[-clear-text {true|false}]** - Allow Clear Text Password

This optionally specifies whether the NDMP password can be sent in clear text. The default setting is `true`.

### **[-user-id <text>]** - NDMP User ID

This optionally specifies the ID of the NDMP user.

## Examples

The following example modifies the NDMP configuration on a node named node1. The configuration enables NDMP, disables sending the password in clear text, and specifies an NDMP user named ndmp:

```
cluster1::> system services ndmp modify -node node1 -enable true
             -clear-text false -user-id ndmp
```

## Related Links

- [vserver services ndmp modify](#)

## system services ndmp off

(DEPRECATED)-Disable NDMP service

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp off](#)" command.

The `system services ndmp off` command is used to disable the NDMP service on any node in the cluster.

## Parameters

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

The specific node on which NDMP service is to be disabled.

## Examples

The following example is used to turn off the NDMP service on node named node1:

```
cluster1::> system services ndmp off -node node1
```

## Related Links

- [vserver services ndmp off](#)

## system services ndmp on

(DEPRECATED)-Enable NDMP service

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp on](#)" command.

The `system services ndmp on` command is used to enable the NDMP service across any node in the cluster.

## Parameters

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

The specific node on which the NDMP service is to be enabled.

## Examples

The following example is used to turn on the NDMP service on node named node1:

```
cluster1::> system services ndmp on -node node1
```

## Related Links

- [vserver services ndmp on](#)

## system services ndmp password

(DEPRECATED)-Change the NDMP password for the node

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp generate-password](#)" command.

The `system services ndmp password` command is used to change the NDMP password for a node in the cluster.

## Parameters

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

The specific node for which the password is to be changed.

## Examples

The following example is used to change the NDMP password for the node named node1:

```
cluster1::> system services ndmp password -node node1
```

```
Please enter password:
```

```
Confirm password:
```

## Related Links

- [vserver services ndmp generate-password](#)

# system services ndmp probe

Display list of NDMP sessions

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

## Description

The `system services ndmp probe` command displays diagnostic information about all the NDMP sessions in the cluster. The following fields are displayed for each of the sessions:

- Node
- Session identifier
- NDMP version
- Session authorized
- Data state
- Data operation
- Data server halt reason
- Data server connect type
- Data server connect address
- Data server connect port
- Data bytes processed
- Mover state
- Mover mode
- Mover pause reason
- Mover halt reason
- Mover record size
- Mover record number
- Mover bytes moved
- Mover seek position
- Mover bytes left to read
- Mover window offset

- Mover window length
- Mover position
- Mover SetRecordSize flag
- Mover SetWindow flag
- Mover connect type
- Mover connect address
- Mover connect port
- Effective host
- NDMP client address
- NDMP client port
- SCSI device ID
- SCSI hostadapter
- SCSI target ID
- SCSI LUN ID
- Tape device
- Tape mode
- Is Secure Control Connection
- Data Backup Mode
- Data Path
- NDMP Source Address

## Parameters

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

If this parameter is specified, the command displays information about the sessions running on the specified node only. Node should be a valid node name.

### **[-session-id <integer>] - Session Identifier**

If this parameter is specified, the command displays information only about the specified session.

### **[-ndmp-version <integer>] - NDMP Version**

This parameter refers to the NDMP protocol version being used in the session.

### **[-session-authorized {true|false}] - Session Authorized**

This parameter indicates whether an NDMP session is authenticated or not.

### **[-data-state <component state>] - Data State**

This parameter identifies the current state of the data server's state machine.

### **[-data-operation <data operation>] - Data Operation**

This parameter identifies the data server's current operation.

**[-data-halt-reason <halt reason>] - Data Server Halt Reason**

This parameter identifies the event that caused the data server state machine to enter the HALTED state.

**[-data-con-addr-type <address type>] - Data Server Connect Type**

This parameter specifies the type of data connection established by the data server. The data connection can be established locally within a given system or between remote networked systems.

**[-data-con-addr <text>] - Data Server Connect Address**

This parameter specifies the connection endpoint information for the data server's data connection.

**[-data-con-port <integer>] - Data Server Connect Port**

This parameter specifies the TCP/IP port that the data server will use when establishing a data connection.

**[-data-bytes-processed <integer>] - Data Bytes Processed**

This parameter represents the cumulative number of data stream bytes transferred between the backup or recovery method and the data connection during the current data operation.

**[-mover-state <component state>] - Mover State**

This parameter identifies the current state of the NDMP tape server's mover state machine.

**[-mover-mode <mover mode>] - Mover Mode**

This parameter identifies the direction of the mover data transfer.

**[-mover-pause-reason <pause reason>] - Mover Pause Reason**

This parameter identifies the event that caused the mover state machine to enter the PAUSED state.

**[-mover-halt-reason <halt reason>] - Mover Halt Reason**

This parameter identifies the event that caused the mover state machine to enter the HALTED state.

**[-mover-record-size <integer>] - Mover Record Size**

This parameter represents the current mover record size in bytes.

**[-mover-record-num <integer>] - Mover Record Number**

This parameter represents the last tape record processed by the mover.

**[-mover-bytes-moved <integer>] - Mover Bytes Moved**

This parameter represents the cumulative number of data stream bytes written to the data connection or the number of data stream bytes read from the data connection and written to the tape subsystem, depending on the mode of mover operation.

**[-mover-seek-position <integer>] - Mover Seek Position**

This parameter represents the data stream offset of the first byte the DMA requested the mover to transfer to the data connection during a mover read operation.

**[-mover-bytes-left-to-read <integer>] - Mover Bytes Left to Read**

This parameter represents the number of data bytes remaining to be transferred to the data connection to satisfy the current NDMP\_MOVER\_READ request.

**[-mover-window-offset <integer>] - Mover Window Offset**

This parameter represents the absolute offset of the first byte of the mover window within the overall data stream.

**[-mover-window-length <integer>] - Mover Window Length**

This parameter represents the length of the current mover window in bytes.

**[-mover-position <integer>] - Mover Position**

This parameter can be used to list only those sessions, whose mover position matches a specific value. Mover-position should be an integer.

**[-mover-setrecordsize-flag {true|false}] - Mover SetRecordSize Flag**

This parameter is used by the DMA to establish the record size used for mover-initiated tape read and write operations.

**[-mover-setwindow-flag {true|false}] - Mover SetWindow Flag**

This parameter represents whether a mover window has been set or not. A mover window represents the portion of the overall backup stream that is accessible to the mover without intervening DMA tape manipulation.

**[-mover-con-addr-type <address type>] - Mover Connect Type**

This parameter specifies the type of data connection established by the mover. The data connection can be established locally within a given system or between remote networked systems.

**[-mover-con-addr <text>] - Mover Connect Address**

This parameter specifies the endpoint address or addresses that the mover will use when establishing a data connection.

**[-mover-con-port <integer>] - Mover Connect Port**

This parameter specifies the TCP/IP port that the mover will use when establishing a data connection.

**[-eff-host <host type>] - Effective Host**

This parameter indicates the host context in which the NDMP session runs. The valid values are: PRIMARY or PARTNER.

**[-client-addr <text>] - NDMP Client Address**

This parameter specifies the client's IP address.

**[-client-port <integer>] - NDMP Client Port**

This parameter specifies the client's port number.

**[-spt-device-id <text>] - SCSI Device ID**

This parameter specifies the SCSI device ID.

**[-spt-ha <integer>] - SCSI Host Adapter**

This parameter specifies the SCSI host adapter.

**[-spt-scsi-id <integer>] - SCSI Target ID**

This parameter specifies the SCSI target.

**[-spt-scsi-lun <integer>] - SCSI LUN ID**

This parameter specifies the SCSI LUN ID.

**[-tape-device <text>] - Tape Device**

This parameter specifies the name to identify the tape device.

**[-tape-mode <mover mode>] - Tape Mode**

This parameter specifies the mode in which tapes are opened.

**[-is-secure-control-connection {true|false}] - Is Secure Control Connection**

This parameter specifies whether the control connection is secure or not.

**[-data-backup-mode <text>] - Data Backup Mode**

This parameter specifies whether the mode of data backup is Dump or SMTape.

**[-data-path <text>] - Data Path**

This parameter specifies the path of data being backed up.

**[-source-addr <text>] - NDMP Source Address**

This parameter specifies the control connection IP address of the NDMP session.

## Examples

The following example displays diagnostic information about all the sessions in the cluster:



```

cluster1::> system services ndmp probe
Node: cluster1-01
    Session identifier: 4952
        NDMP version: 4
    Session authorized: true
        Data state: IDLE
            Data operation: NOACTION
    Data server halt reason: NA
Data server connect type: LOCAL
    ....
    ...

Node: cluster1-02
    Session identifier: 5289
        NDMP version: 4
    Session authorized: true
        Data state: IDLE
            Data operation: NOACTION
    Data server halt reason: NA
Data server connect type: LOCAL
    ....
    ...

```

The following example displays diagnostic information of sessions running on the node cluster1-01 only:

```

cluster1::> system services ndmp probe -node cluster1-01
Node: cluster1-01
    Session identifier: 4952
        NDMP version: 4
    Session authorized: true
        Data state: IDLE
            Data operation: NOACTION
    Data server halt reason: NA
Data server connect type: LOCAL
    ....
    ...

```

## system services ndmp show

(DEPRECATED)-Display NDMP service configuration

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp show](#)" command.

The `system services ndmp show` command displays the following information about the NDMP configuration across all the nodes in the cluster:

- Node name
- Whether NDMP is enabled on the node
- Whether sending the NDMP password in clear text is enabled on the node
- NDMP user ID

A combination of parameters can be optionally supplied to filter the results based on specific criteria.

## Parameters

**{ [-fields <fieldname>,...]**

If this parameter is specified, the command displays only the fields that you specify.

**| [-instance ] }**

If this parameter is specified, the command displays detailed information about all entries.

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

Selects information about the specified node.

**[-enable {true|false}] - NDMP Service Enabled**

Selects information about the nodes where NDMP is enabled/disabled.

**[-clear-text {true|false}] - Allow Clear Text Password**

Selects information about the nodes whose clear-text setting matches the specified value.

**[-user-id <text>] - NDMP User ID**

Selects information about the nodes that have the specified NDMP user ID.

## Examples

The following example displays information about the NDMP configuration of all nodes in the cluster:

```

cluster1::> system services ndmp show
Node          Enabled   Clear Text  User ID
-----
node0         true     true       ndmp
node1         true     true       ndmp
node2         true     true       ndmp
node3         true     true       ndmp
4 entries were displayed.

```

## Related Links

- [vserver services ndmp show](#)

# system services ndmp status

Display list of NDMP sessions

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

## Description

The `system services ndmp status` command lists all the NDMP sessions in the cluster. By default it lists the following details about the active sessions:

- Node
- Session ID

A combination of parameters can be optionally supplied so as to list only those sessions which match specific conditions. A short description of each of the parameter is provided in the parameters section.

## Parameters

{ [-fields <fieldname>,...]

This optional parameter specifies which all additional fields to display. Any combination of the following fields are valid:

- ndmp-version
- session-authorized
- data-state
- data-operation
- data-halt-reason
- data-con-addr-type
- data-con-addr
- data-con-port
- data-bytes-processed

- mover-state
- mover-mode
- mover-pause-reason
- mover-halt-reason
- mover-record-size
- mover-record-num
- mover-bytes-moved
- mover-seek-position
- mover-bytes-left-to-read
- mover-window-offset
- mover-window-length
- mover-position
- mover-setrecordsize-flag
- mover-setwindow-flag
- mover-con-addr-type
- mover-con-addr
- mover-con-port
- eff-host
- client-addr
- client-port
- spt-device-id
- spt-ha
- spt-scsi-id
- spt-scsi-lun
- tape-device
- tape-modes
- is-secure-control-connection
- data-backup-mode
- data-path
- source-addr

**[ `-instance` ] }**

If this parameter is specified, the command displays detailed information about all the active sessions.

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

If this parameter is specified, the command displays information about the sessions running on the specified node only. Node should be a valid node name.

**[-session-id <integer>] - Session Identifier**

If this parameter is specified, the command displays information about specific NDMP session. A session-id is a number used to identify a particular NDMP session.

**[-ndmp-version <integer>] - NDMP Version**

This parameter refers to the NDMP protocol version being used in the session.

**[-session-authorized {true|false}] - Session Authorized**

This field indicates whether an NDMP session is authenticated or not.

**[-data-state <component state>] - Data State**

This field identifies the current state of the data server's state machine.

**[-data-operation <data operation>] - Data Operation**

This field identifies the data server's current operation.

**[-data-halt-reason <halt reason>] - Data Server Halt Reason**

This field identifies the event that caused the data server state machine to enter the HALTED state.

**[-data-con-addr-type <address type>] - Data Server Connect Type**

This field specifies the type of data connection established by the data server. The data connection can be established locally within a given system or between remote networked systems.

**[-data-con-addr <text>] - Data Server Connect Address**

This specifies the connection endpoint information for the data server's data connection.

**[-data-con-port <integer>] - Data Server Connect Port**

This specifies the TCP/IP port that the data server will use when establishing a data connection.

**[-data-bytes-processed <integer>] - Data Bytes Processed**

This field represents the cumulative number of data stream bytes transferred between the backup or recovery method and the data connection during the current data operation.

**[-mover-state <component state>] - Mover State**

This parameter identifies the current state of the NDMP tape server's mover state machine.

**[-mover-mode <mover mode>] - Mover Mode**

This parameter identifies the direction of the mover data transfer.

**[-mover-pause-reason <pause reason>] - Mover Pause Reason**

This parameter identifies the event that caused the mover state machine to enter the PAUSED state.

**[-mover-halt-reason <halt reason>] - Mover Halt Reason**

This integer field identifies the event that caused the mover state machine to enter the HALTED state.

**[-mover-record-size <integer>] - Mover Record Size**

This field represents the current mover record size in bytes.

**[-mover-record-num <integer>] - Mover Record Number**

This field represents the last tape record processed by the mover.

**[-mover-bytes-moved <integer>] - Mover Bytes Moved**

This field represents the cumulative number of data stream bytes written to the data connection or the number of data stream bytes read from the data connection and written to the tape subsystem, depending on the mode of mover operation.

**[-mover-seek-position <integer>] - Mover Seek Position**

This field represents the data stream offset of the first byte the DMA requested the mover to transfer to the data connection during a mover read operation.

**[-mover-bytes-left-to-read <integer>] - Mover Bytes Left to Read**

This field represents the number of data bytes remaining to be transferred to the data connection to satisfy the current NDMP\_MOVER\_READ request.

**[-mover-window-offset <integer>] - Mover Window Offset**

This field represents the absolute offset of the first byte of the mover window within the overall data stream.

**[-mover-window-length <integer>] - Mover Window Length**

This field represents the length of the current mover window in bytes.

**[-mover-position <integer>] - Mover Position**

This parameter can be used to list only those sessions, whose mover position matches a specific value. Mover-position should be an integer.

**[-mover-setrecordsize-flag {true|false}] - Mover SetRecordSize Flag**

This field is used by the DMA to establish the record size used for mover-initiated tape read and write operations.

**[-mover-setwindow-flag {true|false}] - Mover SetWindow Flag**

This flag represents whether a mover window has been set or not. A mover window represents the portion of the overall backup stream that is accessible to the mover without intervening DMA tape manipulation.

**[-mover-con-addr-type <address type>] - Mover Connect Type**

This field specifies the type of data connection established by the mover. The data connection can be established locally within a given system or between remote networked systems.

**[-mover-con-addr <text>] - Mover Connect Address**

This specifies the endpoint address or addresses that the mover will use when establishing a data connection.

**[-mover-con-port <integer>] - Mover Connect Port**

This specifies the TCP/IP port that the mover will use when establishing a data connection.

**[-eff-host <host type>] - Effective Host**

This field indicates the host context in which the NDMP session runs. The valid values are: PRIMARY or PARTNER.

**[-client-addr <text>] - NDMP Client Address**

This parameter specifies the client's IP address.

**[-client-port <integer>] - NDMP Client Port**

This parameter specifies the client's port number.

**[-spt-device-id <text>] - SCSI Device ID**

This parameter specifies the SCSI device ID.

**[-spt-ha <integer>] - SCSI Host Adapter**

This parameter specifies the SCSI host adapter.

**[-spt-scsi-id <integer>] - SCSI Target ID**

This parameter specifies the SCSI target.

**[-spt-scsi-lun <integer>] - SCSI LUN ID**

This parameter specifies the SCSI LUN ID.

**[-tape-device <text>] - Tape Device**

This parameter specifies the name to identify the tape device.

**[-tape-mode <mover mode>] - Tape Mode**

This parameter specifies the mode in which tapes are opened.

**[-is-secure-control-connection {true|false}] - Is Secure Control Connection**

This parameter specifies whether the control connection is secure or not.

**[-data-backup-mode <text>] - Data Backup Mode**

This parameter specifies whether the mode of data backup is Dump or SMTape.

**[-data-path <text>] - Data Path**

This parameter specifies the path of data being backed up.

**[-source-addr <text>] - NDMP Source Address**

This parameter specifies the control connection IP address of the NDMP session.

## Examples

The following example displays all the NDMP sessions on the cluster:

```
cluster1::> system services ndmp status
                Session
Node            Id
-----
node-01        17479
node-01        19769
node-02        21118
3 entries were displayed.
```

The following example shows how to display only the sessions running on node-01:

```
cluster1::> system services ndmp status -node node-01
                Session
Node            Id
-----
node-01        17479
node-01        19769
2 entries were displayed.
```

## system services ndmp log start

(DEPRECATED)-Start logging for the specified NDMP session

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

### Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp log start](#)" command.

This command is used to start logging on an active NDMP session on a node. You can start logging two different kinds of sessions. The NDMP *server* session manages all NDMP tasks on the node. If you want to log information regarding the NDMP server, use *server* with the `-session-id` parameter to enable logging. If you want to log information about a particular NDMP session, for example a restore operation, then determine the session ID for the session using the "system services ndmp status" command and use that ID with the `-session-id` parameter to enable logging.

### Parameters

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

This parameter specifies the node.

**-session-id {<integer>|server} - Session Identifier**

This parameter specifies the NDMP session-id on which logging needs to be started. The session-id is associated with a unique NDMP session. Specify *server* to start logging on the NDMP server session.



### **-filter <text> - Level Filter**

Use this parameter to specify the filter for a particular session ID. This parameter controls the NDMP modules for which logging is to be enabled. This parameter can take five values. They are as follow : *all* , *none* , *normal* , *backend* or "*filter-expression*". The default value for this is *none* .

- *all* turns on logging for all modules.
- *none* disables logging for all modules.
- *normal* is a short cut parameter that enables logging for all modules except *verbose* and *io\_loop* . The equivalent filter string is *all-verbose-io\_loop*
- *backend* is a short cut parameter that enables logging for all modules except *verbose* , *io\_loop* , *ndmps* and *ndmpd* . The equivalent filter string is *all-verbose-io\_loop-ndmps-ndmpp*
- (*filter-expression*) is a combination of one or more modules for which logs needs to be enabled. Multiple module names can be combined using following operators :
- - to remove the given module from the list of specified modules in the filter string. For example the filter *all-ndmpp* will enable logging for all modules but not *ndmpp* .
- ^ to add the given module or modules to the list of modules specified in the filter string. For example the filter *ndmpp<sup>mover</sup>data* will enable logging for *ndmpp* , *mover* and *data* .

The possible module names and a brief description is given below:

Modules	Description
verbose	verbose message
io	I/O process loop
io_loop	I/O process loop verbose messages
ndmps	NDMP service
ndmpp	NDMP Protocol
rpc	General RPC service
fdc_rpc	RPC to FC driver service
auth	Authentication
mover	NDMP MOVER (tape I/O)
data	NDMP DATA (backup/restore)
scsi	NDMP SCSI (robot/tape ops)
bkup_rpc	RPC to Backup service client
bkup_rpc_s	RPC to Backup service server
cleaner	Backup/Mover session cleaner
conf	Debug configure/reconfigure
dblade	Dblade specific messages
timer	NDMP server timeout messages
vldb	VLDB service
smf	SMF Gateway messages
vol	VOL OPS service
sv	SnapVault NDMP extension
common	NDMP common state
ext	NDMP extensions messages
sm	SnapMirror NDMP extension
ndmprpc	NDMP Mhost RPC server

## Examples

The following example shows how to start logging on a specific NDMP session 33522, running on the node cluster1-01 with filter normal.

```
cluster1::*> system services ndmp log start -node cluster1-01 -session-id
33522 -filter normal
```

The following example shows how to start logging on the NDMP server session, on the node cluster1-01 with filter all.

```
cluster1::*> system services ndmp log start -session-id server -filter all
-node cluster1-01
```

## Related Links

- [vserver services ndmp log start](#)

# system services ndmp log stop

(DEPRECATED)-Stop logging for the specified NDMP session

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "[vserver services ndmp log stop](#)" command.

This command is used to stop logging on an active NDMP session on a node. The NDMP *server* session manages all NDMP tasks on the node. If you want to stop logging information regarding the NDMP server, use *server* with the `-session-id` parameter to disable logging. If you want to stop logging information about a particular NDMP session, for example a restore operation, then determine the session ID for the session using the "system services ndmp status" command and use that ID with the `-session-id` parameter to disable logging.

## Parameters

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

This parameter specifies the node.

**-session-id {<integer>|server} - Session Identifier**

This parameter specifies the NDMP session-id on which logging needs to be stopped. The session-id is associated with a unique NDMP session. Specify *server* to stop logging on the NDMP server session.

## Examples

The following example shows how to stop logging on a specific NDMP session 35512, running on node cluster1-01.

```
cluster1::*> system services ndmp log stop -session-id 35512 -node
cluster1-01
```

The following example shows how to stop logging on the NDMP server session, running on node cluster1-01.

```
cluster1::*> system services ndmp log stop -session-id server -node
cluster1-01
```

## Related Links

- [vserver services ndmp log stop](#)

# system services ndmp node-scope-mode off

(DEPRECATED)-Disable NDMP node-scope-mode

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "`vserver services ndmp``" command.

This command puts NDMP server in Vserver-aware mode. The Vserver-aware commands are available under `vserver services ndmp`.

## Examples

The following example shows how to disable the node-scope-mode of NDMP server.

```
cluster1::> system services ndmp node-scope-mode off
NDMP node-scope-mode is disabled.
```

# system services ndmp node-scope-mode on

(DEPRECATED)-Enable NDMP node-scope-mode

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

## Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "`vserver services ndmp``" command.

This command puts the NDMP server in the node-scope-mode. In the node-scope-mode, NDMP server has the following behavior:

- All NDMP operations are restricted to resources on the node
- Vserver-aware NDMP commands are disabled
- NDMP authentication falls back to DATA ONTAP 8.1 NDMP authentication scheme

## Examples

The following example enables node-scope-mode of operation :

```
cluster1::> system services ndmp node-scope-mode on
NDMP node-scope-mode is enabled.
```

## system services ndmp node-scope-mode status

(DEPRECATED)-Status of NDMP node-scope-mode

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

### Description



This node-scoped NDMP command is deprecated. Node-scoped NDMP functionality may be removed in a future release of Data ONTAP. Use the Vserver-aware "`vserver services ndmp`" command.

This command displays whether the NDMP server is operating in node-scope-mode or not.

- NDMP node-scope-mode is disabled - NDMP server is Vserver-aware
- NDMP node-scope-mode is enabled - NDMP server is node scoped

### Parameters

## Examples

The following example shows how to check the status of NDMP server in a cluster

```
cluster1::> system services ndmp node-scope-mode status
NDMP node-scope-mode is disabled.
```

## system services ndmp service modify

Modify NDMP service configuration

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

### Description

The `system services ndmp service modify` command allows you to modify the NDMP service configurations for a node in the cluster. The following configuration can be modified:

- NDMP Common Sessions

## Parameters

### **-node {<nodename>|local} - Node**

This specifies the node whose NDMP configuration is to be modified.

### **[-common-sessions <integer>] - NDMP Common Sessions**

This optional parameter specifies the number of extra common NDMP sessions supported, in addition to the number of backup and restore sessions supported for a platform. The default value is 4 for all platforms. The number of backup and restore sessions are platform dependent.



Increasing this parameter can make the storage system unresponsive.

## Examples

The following example modifies the NDMP configuration on a node named node1. The configuration sets the NDMP Common Sessions to 16:

```
cluster1::> system services ndmp modify -node node1
           -common-sessions 16
```

## system services ndmp service show

Display NDMP service configuration

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

### Description

The `system services ndmp service show` command displays the following information about the NDMP service configuration across all the nodes in the cluster:

- Node name
- NDMP Common Sessions

A combination of parameters can be optionally supplied to filter the results based on specific criteria.

### 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 information about the specified node.

## **[~~-common-sessions~~ <integer>] - NDMP Common Sessions**

Selects information about the nodes that have the specified number of NDMP common sessions.

### **Examples**

The following example displays information about the NDMP configuration of all nodes in the cluster:

```
cluster1::> system services ndmp service show
Node          Common Sessions
-----
node0         16
node1         16
node2         16
node3         16
4 entries were displayed.
```

## **system services ndmp service start**

Start the NDMP service

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

### **Description**

The `system services ndmp service start` command starts the NDMP service daemon for a node. This is different from the [system services ndmp on](#) command. The [system services ndmp on](#) command enables the daemon to accept NDMP requests. The NDMP service daemon starts automatically on a node when it boots up. Use this command to start the NDMP service daemon that has been stopped by the [system services ndmp service stop](#) command.

### **Parameters**

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

The node on which the NDMP service needs to be started.

### **Examples**

```
cluster1::*> system services ndmp service start -node node0
```

Starts the NDMP service on node0.

### **Related Links**

- [system services ndmp on](#)
- [system services ndmp service stop](#)

# system services ndmp service stop

Stop the NDMP service

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

## Description

The `system services ndmp service stop` command stops the NDMP service daemon on a node. This is a disruptive command and should not be used in normal scenarios. Processing of active sessions continues but the ability to view or kill sessions is lost. This is different from the [system services ndmp off](#) command. The [system services ndmp off](#) command disables new NDMP connections on the node but does not stop the NDMP service daemon.

## Parameters

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

The node on which the NDMP service needs to be stopped.

## Examples

```
cluster1::*> system services ndmp service stop -node node0
```

Stops the NDMP service on node0.

## Related Links

- [system services ndmp off](#)

# system services ndmp service terminate

Terminate all NDMP sessions

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

## Description

The `system services ndmp service terminate` command terminates all active sessions on the node. This command forcefully terminates all NDMP sessions without an opportunity for a graceful shutdown. Use [system services ndmp kill-all](#) for a clean termination of all active sessions on a node.

## Parameters

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

The node on which the NDMP sessions need to be terminated



## Examples

```
cluster1::*> system services ndmp service terminate -node node0
```

Terminates all active NDMP sessions on node0.

## Related Links

- [system services ndmp kill-all](#)

## system services web modify

Modify the cluster-level configuration of web protocols

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

## Description

This command modifies the overall availability of web services in the cluster, including the core protocol configurations for those services. In a pre-root or unclustered scenario, its scope applies to the local node.

## Parameters

### **[`-external {true|false}`] - External Web Services**

Defines whether remote clients can access HTTP or HTTPS service content. Along with the `system services firewall` configuration, this parameter controls the visibility for client connections. The default value for this parameter after installation is 'true', which exports web protocols for remote access. If no value is provided during modification, its behavior does not change.

### **[`-per-address-limit <integer>`] - Per Address Limit**

Limits the number of connections that can be processed concurrently from the same remote address. If more connections are accepted, those in excess of the limit are delayed and processed after the number of connections being processed drops below the limit. The default value is 96.

### **[`-http-enabled {true|false}`] - HTTP Enabled**

Defines whether HTTP is enabled. The default value for this parameter is *false*.

### **[`-csrf-protection-enabled {true|false}`] - CSRF Protection Enabled**

Defines whether CSRF protection is enabled. The default value is *true*.

### **[`-csrf-token-concurrent-limit <integer>`] - Maximum Number of Concurrent CSRF Tokens**

Defines how many concurrent CSRF tokens can exist at any given time. The default value is *500*.

### **[`-csrf-token-idle-timeout <integer>`] - CSRF Token Idle Timeout (Seconds)**

Defines how long (in seconds) an unused CSRF token will exist until it expires. The default value is *900* seconds (15 minutes).

### **[`-csrf-token-absolute-timeout` <integer>] - CSRF Token Absolute Timeout (Seconds)**

Defines how long (in seconds) a CSRF token can exist regardless of usage. The default value is `0/undefined`, which means that it will never time out.

## Examples

The following command changes the maximum size of the wait queue:

```
cluster1::> system services web modify -wait-queue-capacity 256
```

## system services web show

Display the cluster-level configuration of web protocols

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

### Description

This command displays the overall availability of web services in the cluster, including the core protocol configurations for those services. In a pre-root or unclustered scenario, its output applies to the local node. The following information explains the `External Web Services` and `Status` attributes, two features of web services' availability.

The `External Web Services` field indicates whether remote clients are allowed to access the HTTP or HTTPS service content. Along with the `system services firewall` configuration, the `External Web Services` field indicates the visibility for client connections.

The `Status` field describes the aggregated operational state of cluster-level web services as retrieved from the `system services web node` command. The `Status` field does not reflect whether the protocols are externally visible, but whether the server processes are running correctly. For detailed information about individual servers, use the [system services web node show](#) command. The following are the possible values for the `Status` in node configuration or availability:

- `online`, all web services are consistently configured and working correctly.
- `partial`, one or more nodes' web services are unavailable due to an error condition.
- `mixed`, the nodes in the cluster do not share the same web services configuration. This situation might occur if individual nodes were reconfigured with the `system services web node` command.
- `offline`, all of the nodes' web services are unavailable due to an error condition.
- `unclustered`, the current node is not part of an active cluster.

The `HTTP Enabled` field indicates whether HTTP is enabled.

The `per-address-limit` field is the limit of the number of connections that can be processed concurrently from the same remote address. If more connections are accepted, those in excess of the limit are delayed and processed after the number of connections being processed drops below the limit.

## Examples

The following example displays the availability of web services for the cluster.

```
cluster1::> system services web show
External Web Services: true
                    Status: online
    HTTP Protocol Port: 80
    HTTPS Protocol Port: 443
                    HTTP Enabled: true
```

## Related Links

- [system services web node show](#)

# system services web node show

Display the status of the web servers at the node level

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

## Description

This command displays operational configuration for the web server processes on the nodes in the cluster. This output is aggregated to produce the content for the [system services web show](#) command.

## 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 nodes that match this parameter value. Identifies the node where the web server process is being executed.

**[-external {true|false}] - External Web Services**

Selects the nodes that match this parameter value. Defines whether remote clients can access the HTTP or HTTPS service content. Along with the `system services firewall` command configuration, this parameter controls the visibility for client connections. The default value for this parameter after installation is `true`, which exports web protocols for remote access.

**[-http-port <integer>] - HTTP Port**

Selects the nodes that match this parameter value. Defines the HTTP port for the node-level web services.

### **[--https-port <integer>] - HTTPS Port**

Selects the nodes that match this parameter value. Defines the encrypted HTTP (HTTPS) port for the node-level web services.

### **[--http-enabled {true|false}] - HTTP Enabled**

Selects the nodes that match this parameter value. Defines whether HTTP is enabled.

### **[--per-address-limit <integer>] - Per Address Limit**

Selects the nodes that match this parameter value. Limits the number of connections that can be processed concurrently from the same remote address. If more connections are accepted, those in excess of the limit are delayed and processed after the number of connections being processed drops below the limit.

### **[--status {offline|partial|mixed|online|unclustered}] - Protocol Status**

Selects the nodes that match this parameter value. Describes the operational state of node-level web services. This parameter does not reflect whether protocols are externally visible, but whether the server processes are running correctly. The following are the possible values that describe the service availability:

- online, indicates that web services are working correctly.
- offline, indicates that web services are unavailable due to an error condition.
- unclustered, indicates that the current node is not part of an active cluster.

### **[--total-hits <integer>] - Total HTTP Requests**

Selects the nodes that match this parameter value. Indicates the total number of requests serviced by the web server.

### **[--total-bytes <integer>] - Total Bytes Served**

Selects the nodes that match this parameter value. Indicates the total number of bytes returned by the web server.

## **Examples**

The following example displays the status of web servers for nodes in the cluster.

```
cluster1::system services web node> show
          HTTP   HTTP   HTTPS
Node      External enabled Port  Port  Status  Total      Total
Served
-----
node1     true    true   80    443   online   5
1362
node2     true    true   80    443   online   5
1362
2 entries were displayed.
```

## Related Links

- [system services web show](#)

## Copyright Information

Copyright © 2022 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 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.