System configuration API methods

Element Software

NetApp
November 19, 2025

This PDF was generated from https://docs.netapp.com/us-en/element-software-123/api/reference_element_api_disablebmccoldreset.html on November 19, 2025. Always check docs.netapp.com for the latest.

Table of Contents

System configuration API methods . . . 1
- Find more information . . . 2
- DisableBmcColdReset . . . 2
  - Parameter . . . 2
  - Return values . . . 2
  - Request example . . . 2
  - Response example . . . 2
  - New since version . . . 3
- DisableClusterSsh . . . 3
  - Parameter . . . 3
  - Return value . . . 3
  - Request example . . . 3
  - Response example . . . 4
  - New since version . . . 4
- DisableSnmp . . . 4
  - Parameter . . . 4
  - Return value . . . 4
  - Request example . . . 5
  - Response example . . . 5
  - New since version . . . 5
- EnableBmcColdReset . . . 5
  - Parameter . . . 5
  - Return values . . . 5
  - Request example . . . 6
  - Response example . . . 6
  - New since version . . . 6
- EnableClusterSsh . . . 6
  - Parameter . . . 6
  - Return values . . . 7
  - Request example . . . 7
  - Response example . . . 7
  - New since version . . . 8
- EnableSnmp . . . 8
  - Parameter . . . 8
  - Return value . . . 9
  - Request example . . . 9
  - Response example . . . 9
  - New since version . . . 9
- GetBinAssignmentProperties . . . 9
  - Parameter . . . 10
  - Return value . . . 10
  - Request example . . . 10
  - Response example . . . 10

New since version . . . 12
GetClusterSshInfo . . . 12
Parameter . . . 12
Return value . . . 12
Request example . . . 12
Response example . . . 13
New since version . . . 13
GetClusterStructure . . . 13
Parameter . . . 13
Return values . . . 14
Request example . . . 14
Response example . . . 14
New since version . . . 14
GetFipsReport . . . 14
Parameter . . . 14
Return values . . . 14
Request example . . . 15
Response example . . . 15
New since version . . . 16
GetLldpConfig . . . 16
Parameters . . . 16
Return values . . . 16
Request example . . . 17
Response example . . . 17
GetLldpInfo . . . 17
Parameters . . . 17
Return values . . . 17
Request example . . . 18
Response example . . . 18
New since version . . . 18
Find more information . . . 18
GetNodeFipsDrivesReport . . . 18
Parameter . . . 18
Return values . . . 18
Request example . . . 19
Response example . . . 19
New since version . . . 19
GetNtpInfo . . . 19
Parameter . . . 20
Return values . . . 20
Request example . . . 20
Response example . . . 20
New since version . . . 21
GetNvramInfo . . . 21
Parameter . . . 21

Return value . . . 21
Request example . . . 21
Response example . . . 21
New since version . . . 22
Find more information . . . 22
GetProtectionDomainLayout . . . 22
Parameter . . . 22
Return value . . . 22
Request example . . . 22
Response example . . . 22
New since version . . . 24
GetRemoteLoggingHosts . . . 24
Parameters . . . 24
Return value . . . 24
Request example . . . 24
Response example . . . 24
New since version . . . 25
Find more information . . . 25
GetSnmpACL . . . 25
Parameters . . . 25
Return values . . . 25
Request example . . . 26
Response example . . . 26
New since version . . . 26
GetSnmpInfo . . . 26
Parameters . . . 27
Return values . . . 27
Request example . . . 27
Response example . . . 28
New since version . . . 28
Find more information . . . 28
GetSnmpState . . . 28
Parameters . . . 28
Return values . . . 28
Request example . . . 29
Response example . . . 29
New since version . . . 29
Find more information . . . 30
GetSnmpTrapInfo . . . 30
Parameters . . . 30
Return values . . . 30
Request example . . . 30
Response example . . . 31
New since version . . . 31
GetSSLCertificate . . . 31

Parameters . . . 32
Return values . . . 32
Request example . . . 32
Response example . . . 32
New since version . . . 33
ListProtectionDomainLevels . . . 33
Parameter . . . 33
Return values . . . 34
Request example . . . 34
Response example . . . 34
New since version . . . 35
RemoveSSLCertificate . . . 35
Parameters . . . 36
Return values . . . 36
Request example . . . 36
Response example . . . 36
New since version . . . 36
ResetNetworkConfig . . . 36
Parameters . . . 36
Return value . . . 36
Request example . . . 37
Response example . . . 37
New since version . . . 37
ResetSupplementalTlsCiphers . . . 37
Parameter . . . 37
Return values . . . 37
Request example . . . 37
Response example . . . 37
New since version . . . 38
SetClusterStructure . . . 38
Parameter . . . 38
Return values . . . 38
Request example . . . 38
Response example . . . 39
New since version . . . 39
SetLldpConfig . . . 39
Parameters . . . 39
Return values . . . 39
Request example . . . 40
Response example . . . 40
SetNtpInfo . . . 40
Parameters . . . 41
Return values . . . 41
Request example . . . 41
Response example . . . 41

New since version . . . 42
SetProtectionDomainLayout . . . 42
Parameter . . . 42
Return value . . . 42
Request example . . . 42
Response example . . . 44
New since version . . . 45
SetRemoteLoggingHosts . . . 45
Parameter . . . 45
Return values . . . 45
Request example . . . 46
Response example . . . 46
New since version . . . 46
Find more information . . . 46
SetSnmpACL . . . 46
Parameters . . . 47
Return values . . . 47
Request example . . . 47
Response example . . . 48
New since version . . . 48
Find more information . . . 48
SetSnmpInfo . . . 48
Parameters . . . 48
Return values . . . 49
Request example with SNMP v3 enabled . . . 49
Request example with SNMP v2 enabled . . . 50
Response example . . . 50
New since version . . . 51
SetSnmpTrapInfo . . . 51
Parameters . . . 51
Return values . . . 52
Request example . . . 52
Response example . . . 52
New since version . . . 52
SetSSLCertificate . . . 53
Parameters . . . 53
Return values . . . 53
Request example . . . 53
Response example . . . 55
New since version . . . 55
SnmpSendTestTraps . . . 55
Parameters . . . 55
Return value . . . 55
Request example . . . 55
Response example . . . 56

New since version . . . 56
TestAddressAvailability . . . 56
Parameters . . . 56
Return values . . . 56
Request example . . . 57
Response example . . . 57
New since version . . . 57

System configuration API methods

System configuration API methods enable you to obtain and set configuration values that apply to all nodes in the cluster.

- DisableBmcColdReset
- DisableClusterSsh
- DisableSnmp
- EnableBmcColdReset
- EnableClusterSsh
- EnableSnmp
- GetBinAssignmentProperties
- GetClusterSshInfo
- GetClusterStructure
- GetFipsReport
- GetLldpConfig
- GetLldpInfo
- GetNodeFipsDrivesReport
- GetNtpInfo
- GetNvramInfo
- GetProtectionDomainLayout
- GetRemoteLoggingHosts
- GetSnmpACL
- GetSnmpInfo
- GetSnmpState
- GetSnmpTrapInfo
- GetSSLCertificate
- ListProtectionDomainLevels
- RemoveSSLCertificate
- ResetNetworkConfig
- ResetSupplementalTlsCiphers
- SetClusterStructure
- SetLldpConfig
- SetNtpInfo
- SetProtectionDomainLayout
- SetRemoteLoggingHosts
- SetSnmpACL
- SetSnmpInfo

- SetSnmpTrapInfo
- SetSSLCertificate
- SnmpSendTestTraps
- TestAddressAvailability

Find more information

- SolidFire and Element Software Documentation
- Documentation for earlier versions of NetApp SolidFire and Element products

DisableBmcColdReset

You can use the `DisableBmcColdReset` method to disable the background task that periodically resets the Baseboard Management Controller (BMC) for all nodes in the cluster.

Parameter

This method has no input parameter.

Return values

This method has the following return value:

Name	Description	Type
cBmcResetDurationMinutes	Returns the time between reset intervals. The interval should always be 0 after the command completes.	integer

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 0
    }
}
```

New since version

12.0

DisableClusterSsh

You can use the `DisableClusterSsh` method to disable the SSH service for the entire storage cluster. When you add nodes to the storage cluster, the new nodes will inherit this cluster-wide setting.

Parameter

This method has no input parameter.

Return value

This method has the following return value:

Name	Description	Type
result	A JSON object containing the status of the SSH service for the storage cluster, the time remaining until SSH is disabled, and the SSH service status for each node.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DisableClusterSsh",
  "params": {
      },
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result" : {
    "enabled": true,
    "timeRemaining": "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```

New since version

10.3

DisableSnmp

You can use the `DisableSnmp` method to disable SNMP on the cluster nodes.

Parameter

This method has no input parameter.

Return value

This method has no return value.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "result" : {},
  "id" : 1
}
```

New since version

9.6

EnableBmcColdReset

You can use the `EnableBmcColdReset` method to enable a background task that periodically resets the Baseboard Management Controller (BMC) for all nodes in the cluster.

Parameter

This method has the following input parameter:

Name	Description	Type	Default value	Required
timeout	The time between BMC reset operations, in minutes.	integer	20160 minutes	No

Return values

This method has the following return value:

Name	Description	Type
cBmcResetDurationMinutes	Returns the time between reset intervals. The interval should always be 0 after the command completes.	integer

Request example

Requests for this method are similar to the following example:

```
{
    "method": "EnableBmcColdReset",
    "params": {
                "timeout": 36000
    },
    "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 36000
    }
}
```

New since version

12.0

EnableClusterSsh

You can use the `EnableClusterSsh` method to enable the SSH service on all nodes in the storage cluster.

Parameter

This method has the following input parameter:

Name	Description	Type	Default value	Required
duration	The amount of time that the SSH service will remain enabled.	string	None	Yes

Return values

This method has the following return values:

Name	Description	Type
result	A JSON object containing the status of the SSH service for the storage cluster, the time remaining until SSH is disabled, and the SSH service status for each node.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
  "method": "EnableClusterSsh",
  "params": {
      "duration"  : "02:00:00.00"
  },
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result" : {
    "enabled": true,
    "timeRemaining": "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```


New since version

10.3

EnableSnmp

You can use the `EnableSnmp` method to enable SNMP on cluster nodes. When you enable SNMP, the action applies to all nodes in the cluster, and the values that are passed replace all values set in any previous call to `EnableSnmp`.

Parameter

This method has the following input parameter:

Name	Description	Type	Default value	Required
snmpV3Enabled	If set to true, then SNMP v3 is enabled on each node in the cluster. If set to false, then SNMP v2 is enabled.	boolean	false	No

Return value

This method has no return value.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "EnableSnmp",
  "params": {
      "snmpV3Enabled"  : "true"
  },
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {}
}
```

New since version

9.6

GetBinAssignmentProperties

You can use the `GetBinAssignmentProperties` method to retrieve the bin assignment properties in the database.

Parameter

This method has the no input parameters.

Return value

This method has the following return value:

Name	Description	Type
properties	Details the properties for all current bin assignments in the database.	binAssignmentProperties array

Request example

Requests for this method are similar to the following example:

```
{
    "method": "GetBinAssignmentProperties",
    "params": {
    },
    "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "properties": {
            "algorithmRuntimeMS": 1105,
            "areReplicasValid": true,
            "binCount": 65536,
            "isBalanced": true,
            "isStable": true,
            "isWellCoupled": false,
            "layout": [
                {
                    "protectionDomainName": "1",
                    "services": [
                        {
                            "budget": 7281,
                            "serviceID": 16
                        },
```

```
                        {
                            "budget": 7281,
                            "serviceID": 19
                        },
                        {
                            "budget": 7281,
                            "serviceID": 24
                        }
                    ]
                },
                {
                    "protectionDomainName": "2",
                    "services": [
                        {
                            "budget": 7281,
                            "serviceID": 17
                        },
                        {
                            "budget": 7281,
                            "serviceID": 20
                        },
                        {
                            "budget": 7281,
                            "serviceID": 22
                        }
                    ]
                },
                {
                    "protectionDomainName": "3",
                    "services": [
                        {
                            "budget": 7281,
                            "serviceID": 18
                        },
                        {
                            "budget": 7281,
                            "serviceID": 21
                        },
                        {
                            "budget": 7281,
                            "serviceID": 23
                        }
                    ]
                }
            ],
            "numSwaps": 0,
```

```
            "numUpdatingBins": 0,
            "protectionDomainType": "node",
            "reason": "Final",
            "replicationCount": 2,
            "requestRebalance": false,
            "serviceStrandedCapacities": [],
            "timePublished": "2020-04-02T18:34:07.807681Z",
            "validSchemes": []
        }
    }
}
```

New since version

12.0

GetClusterSshInfo

You can use the `GetClusterSshInfo` method to query the status of the SSH service for the entire storage cluster.

Parameter

This method has no input parameter.

Return value

This method has the following return value:

Name	Description	Type
result	A JSON object containing the status of the SSH service for the storage cluster, the time remaining until SSH is disabled, and the SSH service status for each node.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetClusterSshInfo",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result" : {
    “enabled”: “true”,
    “timeRemaining”: "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```

New since version

10.3

GetClusterStructure

You can use the `GetClusterStructure` method to back up the current storage cluster configuration information. If the storage cluster configuration is changed while this method is running, the contents of the configuration backup will be unpredictable. You can save this data to a text file and restore it on other clusters, or the same cluster in the case of a disaster.

Parameter

This method has no input parameter.

Return values

This method has the following return values:

Name	Description	Type
result	A JSON object containing the current storage cluster configuration information.	clusterStructure

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetClusterStructure",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result" : <clusterStructure object containing configuration
information>
    }
```

New since version

10.3

GetFipsReport

You can use the `GetFipsReport` method to check the FIPS 140-2 encryption feature support status of all nodes in the storage cluster.

Parameter

This method has no input parameter.

Return values

This method has the following return values:

Name	Description	Type
result	A JSON object containing the status of FIPS 140-2 feature support for every node, and error information for each node that did not respond to the query.	fipsReport

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetFipsReport",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
    "nodes": [
        {
           "nodeID": 1,
           "fipsDrives": "None",
           "httpsEnabled": true
        },
        {
           "nodeID": 3,
           "fipsDrives": "None",
           "httpsEnabled": true
        }
    ],
    "errorNodes": [
        {
           "nodeID": 2,
           "error": {
               "message": "The RPC timed out.",
               "name": "xRpcTimeout"
               }
        }
    ]
    }
}
```


New since version

10.3

GetLldpConfig

You can use the `GetLldpConfig` method to get the Link Layer Discovery Protocol (LLDP) configuration for each node of a storage cluster.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
lldpConfig	Information about the storage cluster LLDP configuration.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
   "method": "GetLldpConfig",
   "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": null,
        "result": {
            "lldpConfig": {
                "enableLldp": true,
                "enableMed": false,
                "enableOtherProtocols": true
        }
    }
}
```

GetLldpInfo

You can use the `GetLldpInfo` method to get the Link Layer Discovery Protocol (LLDP) configuration for each node of a storage cluster, or an individual storage node.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
lldpInfo	Information about the chassis, interface, and neighbor LLDP settings for each node of a storage cluster.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
   "method": "GetLldpInfo",
   "id" : 1
}
```

Response example

Due to the length of this response example, it is documented in a supplementary topic.

New since version

11.0

Find more information

GetLldpInfo

GetNodeFipsDrivesReport

You can use the `GetNodeFipsDrivesReport` method to check the FIPS 140-2 drive encryption capability status of a single node in the storage cluster. You must run this method against an individual storage node.

Parameter

This method has no input parameter.

Return values

This method has the following return values:

Name	Description	Type
fipsDrives	A JSON object containing the status of FIPS 140-2 feature support for this node. Possible values: • None: Node is not FIPS capable. • Partial: Node is FIPS capable but not all drives in the node are FIPS drives. • Ready: Node is FIPS capable and all drives in the node are FIPS drives (or no drives are present).	string

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

New since version

11.5

GetNtpInfo

You can use the `GetNtpInfo` method to get the current network time protocol (NTP)

configuration information.

Parameter

This method has no input parameter.

Return values

This method has the following return values:

Name	Description	Type
servers	List of NTP servers.	string array
broadcastclient	Indicates whether or not the nodes in the cluster are listening for broadcast NTP messages. Possible values: • true • false	boolean

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetNtpInfo",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {
    "broadcastclient" : false,
    "servers" : [ "us.pool.ntp.org" ]
   }
}
```

New since version

9.6

GetNvramInfo

You can use the `GetNvramInfo` method to get information from each node about the NVRAM card.

Parameter

This method has the following input parameter:

Name	Description	Type	Default value	Required
force	The force parameter must be included on this method to successfully run on all nodes in the cluster.	boolean	None	Yes

Return value

This method has the following return value:

Name	Description	Type
nvramInfo	Arrays of events and errors detected on the NVRAM card.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetNvramInfo",
  "params": {
      "force": true
      },
  "id" : 1
}
```

Response example

Due to the length of this response example, it is documented in a supplementary topic.

New since version

9.6

Find more information

GetNvramInfo

GetProtectionDomainLayout

You can use the `GetProtectionDomainLayout` method to return all protection domain information for a cluster, including which chassis and which custom protection domain each node is in.

Parameter

This method has the no input parameters.

Return value

This method has the following return value:

Name	Description	Type
protectionDomainLayout	List of nodes, each with its associated protection domains.	JSON list of nodeProtectionDomains objects.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetProtectionDomainLayout",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id": 1,
  "result": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
```

```
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR2914008D",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 2,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500EA",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 3,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500C3",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 4,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291400E6",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-2",
```

```
            "protectionDomainType": "custom"
          }
        ]
      }
    ]
  }
}
```

New since version

12.0

GetRemoteLoggingHosts

You can use the `GetRemoteLoggingHosts` method to get the current list of log servers.

Parameters

This method has no input parameters.

Return value

This method has the following return value:

Name	Description	Type
remoteHosts	List of IP address and port information about hosts configured to receive forwarded logging information.	loggingServer array

Request example

Requests for this method are similar to the following example:

```
{
   "id": 3386609,
   "method": "GetRemoteLoggingHosts",
   "params": {}
}
```

Response example

This method returns a response similar to the following example:

```
{
   "id": 3386609,
   "result": {
      "remoteHosts": [
         {
           "host": "172.16.1.20",
           "port": 10514
         },
         {
           "host": "172.16.1.25"
         }
      ]
   }
}
```

New since version

9.6

Find more information

SetRemoteLoggingHosts

GetSnmpACL

You can use the `GetSnmpACL` method to get the current SNMP access permissions on the cluster nodes.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
networks	List of networks and what type of access they have to the SNMP servers running on the cluster nodes. This value is present if SNMP v3 is disabled.	network array

Name	Description	Type
usmUsers	List of users and the type of access they have to the SNMP servers running on the cluster nodes. This value is present if SNMP v3 is enabled.	usmUser array

Request example

Requests for this method are similar to the following example:

```
{
"method": "GetSnmpACL",
"params": {},
"id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {
     "usmUsers"  : [
       {
          "name": "jdoe",
          "access": "rouser",
          "secLevel": "priv",
          "password": "mypassword",
          "passphrase": "mypassphrase",
       }
     ]
   }
}
```

New since version

9.6

GetSnmpInfo

You can use the `GetSnmpInfo` method to get the current simple network management protocol (SNMP) configuration information.

Parameters

> GetSnmpInfo is deprecated for versions later than Element version 8.0. The GetSnmpState and SetSnmpACL methods replace the GetSnmpInfo method.

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
networks	List of networks and access types enabled for SNMP. **Note:** networks is only displayed if SNMP v3 is disabled.	network
enabled	Indicates if the nodes in the cluster are configured for SNMP. Possible values: • true • false	boolean
snmpV3Enabled	If the node in the cluster is configured for SNMP v3. Possible values: • true • false	boolean
usmUsers	If SNMP v3 is enabled, a list of user access parameters for SNMP is returned from the cluster. This is returned instead of the networks parameter.	usmUser

Request example

Requests for this method are similar to the following example:

```
{
   "method": "GetSnmpInfo",
   "params": {},
   "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
   "id" : 1,
   "result" : {
      "enabled" : true,
      "networks" : [
         {
            "access" : "rosys",
            "cidr" : 0,
            "community" : "public",
            "network" : "localhost"
         }
      ]
   }
}
```

New since version

9.6

Find more information

- GetSnmpState
- SetSnmpACL

GetSnmpState

You can use the `GetSnmpState` method to get the current state of the SNMP feature.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
enabled	Possible values: • true • false Default value is false. Returns true if the nodes in the cluster are configured for SNMP.	boolean
snmpV3Enabled	Possible values: • true • false Default value is false. Returns true if the nodes in the cluster are configured for SNMP v3.	boolean

Request example

Requests for this method are similar to the following example:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {
   "enabled": true,
   "snmpV3Enabled": false
   }
}
```

New since version

9.6

Find more information

SetSnmpACL

GetSnmpTrapInfo

You can use the `GetSnmpTrapInfo` method to get current SNMP trap configuration information.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
trapRecipients	List of hosts that are to receive the traps generated by the cluster.	snmpTrapRecipient array
clusterFaultTrapsEnabled	The value true indicates that a solidFireClusterFaultNotification is configured to be sent to the list of trap recipients when a cluster fault is logged.	boolean
clusterFaultResolvedTrapsEnabled	The value true indicates that a solidFireClusterFaultResolvedNotification is configured to be sent to the list of trap recipients when a cluster fault is resolved.	boolean
clusterEventTrapsEnabled	The value true indicates that a solidFireClusterEventNotification is configured to be sent to the list of trap recipients when a cluster event is logged.	boolean

Request example

Requests for this method are similar to the following example:

```
{
   "method":"GetSnmpTrapInfo"
   "params":{},
   "id":1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id": 1,
  "result": {
    "clusterEventTrapsEnabled": true,
    "clusterFaultResolvedTrapsEnabled": true,
    "clusterFaultTrapsEnabled": true,
    "trapRecipients": [
     {
      "community": "public",
      "host": "192.168.151.60",
      "port": 162
     },
     {
      "community": "solidfireAlerts",
      "host": "NetworkMonitor",
      "port": 162
     },
     {
      "community": "wakeup",
      "host": "PhoneHomeAlerter",
      "port": 1008
     }
   ]
 }
}
```

New since version

9.6

GetSSLCertificate

You can use the `GetSSLCertificate` method to retrieve the SSL certificate that is currently active on the storage nodes of the cluster.

Parameters

This method has no input parameters.

Return values

This method has the following return values:

Name	Description	Type
certificate	The full PEM-encoded text of the certificate.	string
details	The decoded information of the certificate.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
    "method" : "GetSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Response example

This method returns a response similar to the following example:


```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
```

```
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n",
        "details": {
            "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
            "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
            "notAfter": "2027-03-06T22:50:26Z",
            "notBefore": "2017-03-08T22:50:26Z",
            "serial": "CC1B221598E37FF3",
            "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
            "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
        }
    }
}
```


New since version

10.0

ListProtectionDomainLevels

You can use the `ListProtectionDomainLevels` method to list the tolerance and resiliency levels of the storage cluster. Tolerance levels indicate the cluster's ability to continue reading and writing data in the event of a failure, and resiliency levels indicate the storage cluster's ability to automatically heal itself from one or more failures.

Parameter

This method has no input parameter.

Return values

This method has the following return values:

Name	Description	Type
protectionDomainLevels	A list of the different protection domain levels, where each supplies the storage cluster's tolerance and resiliency information.	protectionDomainLevel

Request example

Requests for this method are similar to the following example:

```
{
  "method": "ListProtectionDomainLevels",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "protectionDomainLevels": [
            {
                "protectionDomainType": "node",
                "resiliency": {
                    "protectionSchemeResiliencies": [
                            {
                                "protectionScheme": "doubleHelix",
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
                    ],
                    "singleFailureThresholdBytesForBlockData": 0,
                    "sustainableFailuresForEnsemble": 1
                },
                "tolerance": {
                    "protectionSchemeTolerances": [
                            {
                                "protectionScheme": "doubleHelix",
```

```
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
                        ],
                        "sustainableFailuresForEnsemble": 1
                    }
                },
                {
                    "protectionDomainType": "chassis",
                    "resiliency": {
                        "protectionSchemeResiliencies": [
                                {
                                    "protectionScheme": "doubleHelix",
                                    "sustainableFailuresForBlockData": 0,
                                    "sustainableFailuresForMetadata": 1
                                }
                        ],
                        "singleFailureThresholdBytesForBlockData": 0,
                        "sustainableFailuresForEnsemble": 1
                    },
                    "tolerance": {
                        "protectionSchemeTolerances": [
                                {
                                    "protectionScheme": "doubleHelix",
                                    "sustainableFailuresForBlockData": 0,
                                    "sustainableFailuresForMetadata": 1
                                }
                        ],
                        "sustainableFailuresForEnsemble": 1
                    }
                }
            ]
        }
    }
```


New since version

11.0

RemoveSSLCertificate

You can use the `RemoveSSLCertificate` method to remove the user SSL certificate and private key for the storage nodes in the cluster. After the certificate and private key are removed, the storage nodes are configured to use the default certificate and private key.

Parameters

This method has no input parameters.

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
    "method" : "RemoveSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id" : 3,
    "result" : {}
}
```

New since version

10.0

ResetNetworkConfig

You can use the `ResetNetworkConfig` method to help resolve network configuration issues for an individual node. This method resets an individual node's network configuration to the factory default settings.

Parameters

This method has no input parameters.

Return value

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
   "method": "ResetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Response example

This method does not return a response.

New since version

11.0

ResetSupplementalTlsCiphers

You can use the `ResetSupplementalTlsCiphers` method to restore the list of supplemental TLS ciphers to the default. You can use this method on the entire cluster.

Parameter

This method has no input parameters.

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {}
}
```

New since version

11.3

SetClusterStructure

You can use the `SetClusterStructure` method to restore the storage cluster configuration information from a backup. When you call the method, you pass the clusterStructure object containing the configuration information you want to restore as the params parameter.

Parameter

This method has the following input parameter:

Name	Description	Type
params	A JSON object containing the current storage cluster configuration information.	clusterStructure

Return values

This method has the following return values:

Name	Description	Type
result	Asynchronous result handle.	asyncHandle

Request example

Requests for this method are similar to the following example:

```
{
  "method": "SetClusterStructure",
  "params": <insert clusterStructure object here>,
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result" : {
    "asyncHandle": 1
    }
}
```

New since version

10.3

SetLldpConfig

You can use the `SetLldpConfig` method to configure the Link Layer Discovery Protocol (LLDP) settings for a storage cluster.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
enableOtherProtocols	Enable automatic use of other discovery protocols - CDP, FDP, EDP, and SONMP.	boolean	true	No
enableMed	Enable Media Endpoint Discovery (LLDP-MED).	boolean	false	No
enableLldp	Enable or disable LLDP.	boolean	true	No

Return values

This method has the following return value:

Name	Description	Type
lldpConfig	Information about the current storage cluster LLDP configuration, including newly changed settings.	JSON object

Request example

Requests for this method are similar to the following example:

```
{
  "id": 3920,
  "method":"SetLldpConfig",
    "params": {
        "lldpConfig": {
            "enableMed": true
        }
    }
  }
```

Response example

This method returns a response similar to the following example:

```
{
  "id": 3920,
  "result": {
    "lldpConfig": {
        "enableLldp": true,
        "enableMed": true,
        "enableOtherProtocols": true
     }
  }
}
```

SetNtpInfo

You can use the `SetNtpInfo` method to configure NTP on cluster nodes. The values you set with this interface apply to all nodes in the cluster. If an NTP broadcast server periodically broadcasts time information on your network, you can optionally configure nodes as broadcast clients.

Parameters

> Ensure that you use NTP servers that are internal to your network, rather than the installation defaults.

This method has the following input parameters:

Name	Description	Type	Default value	Required
servers	List of NTP servers to add to each node NTP configuration.	string array	None	Yes
broadcastclient	Enables every node in the cluster as a broadcast client.	boolean	false	No

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
   "method": "SetNtpInfo",
   "params": {
     "servers"  : [
       "ntpserver1.example.org",
       "ntpserver2.example.org",
       "ntpserver3.example.org"
     ],
     "broadcastclient" : false
   },
   "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id" : 1,
    "result" : {}
}
```

New since version

9.6

SetProtectionDomainLayout

You can use the `SetProtectionDomainLayout` method to assign nodes to custom protection domains.

Information must be provided for all active nodes in the cluster and no information can be provided for inactive nodes. All nodes in a given chassis must be assigned to the same custom protection domain. The same protectionDomainType must be supplied for all nodes. protectionDomainTypes that are not custom, such as node and chassis, should not be included. If either of these are provided, then the custom protection domains are ignored and an appropriate error is returned.

Custom protection domains are not supported with the following configurations:

- Storage clusters containing shared chassis
- Two-node storage clusters

The method returns an error when used on storage clusters with these configurations.

Parameter

This method has the following input parameters:

Name	Description	Type	Default value	Required
protectionDomainLayout	Protection domain information for each node.	JSON list of nodeProtectionDomains objects.	None	Yes

Return value

This method has the following return value:

Name	Description	Type
protectionDomainLayout	List of nodes, each with its associated protection domains.	JSON list of nodeProtectionDomains objects.

Request example

Requests for this method are similar to the following example:

```
{
  "id": 1,
  "method": "SetProtectionDomainLayout",
  "params": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 2,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 3,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 4,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      }
    ]
  }
}
```

Response example

This method returns a response similar to the following example:


```
{
  "id": 1,
  "result": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR2914008D",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 2,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500EA",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 3,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500C3",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
```

```
      },
      {
        "nodeID": 4,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291400E6",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      }
    ]
  }
}
```


New since version

12.0

SetRemoteLoggingHosts

You can use the `SetRemoteLoggingHosts` method to configure remote logging from the nodes in the storage cluster to a centralized log server or servers. Remote logging is performed over TCP using the default port 514. This API does not add to the existing logging hosts. Rather, it replaces what currently exists with new values specified by this API method. You can use `GetRemoteLoggingHosts` to determine what the current logging hosts are and then use `SetRemoteLoggingHosts` to set the desired list of current and new logging hosts.

Parameter

This method has the following input parameter:

Name	Description	Type	Default value	Required
remoteHosts	List of hosts that are log message recipients.	loggingServer array	None	Yes

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
   "id": 1,
   "method": "SetRemoteLoggingHosts",
   "params": {
     "remoteHosts": [
        {
          "host": "172.16.1.20",
          "port": 10514
        },
        {
          "host": "172.16.1.25"
        }
      ]
   }
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id" : 1,
    "result" : {}
}
```

New since version

9.6

Find more information

GetRemoteLoggingHosts

SetSnmpACL

You can use the `SetSnmpACL` method to configure SNMP access permissions on the cluster nodes. The values you set with this interface apply to all nodes in the cluster, and the values that are passed replace all values set in any previous call to `SetSnmpACL`. Also note that the values set with this interface replace all network or usmUsers values set with the `SetSnmpInfo` method.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
networks	List of networks and what type of access they have to the SNMP servers running on the cluster nodes. See SNMP network object for possible networks values. This parameter is required if SNMP v3 is disabled.	network	None	No
usmUsers	List of users and the type of access they have to the SNMP servers running on the cluster nodes. This parameter is required if SNMP v3 is enabled.	usmUser	None	No

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
  "method": "SetSnmpACL",
  "params": {
    "usmUsers"  : [
      {
         "name": "jdoe",
         "access": "rouser",
         "secLevel": "priv",
         "password": "mypassword",
         "passphrase": "mypassphrase",
      }
    ]
  },
  "id" : 1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1,
  "result" : {}
}
```

New since version

9.6

Find more information

SetSnmpInfo

SetSnmpInfo

You can use the `SetSnmpInfo` method to configure SNMP version 2 and version 3 on cluster nodes. The values you set with this interface apply to all nodes in the cluster, and the values that are passed replace all values set in any previous call to `SetSnmpInfo`.

Parameters

> SetSnmpInfo is deprecated for Element versions 6.0 and later. Use the EnableSnmp and SetSnmpACL methods instead.

This method has the following input parameters:

Name	Description	Type	Default value	Required
networks	List of networks and what type of access they have to the SNMP servers running on the cluster nodes. See the SNMP network object for possible values. This parameter is required for SNMP v2 only.	network array	None	No
enabled	If set to true, SNMP is enabled on each node in the cluster.	boolean	false	No
snmpV3Enabled	If set to true, SNMP v3 is enabled on each node in the cluster.	boolean	false	No
usmUsers	If SNMP v3 is enabled, this value must be passed in place of the networks parameter. This parameter is required for SNMP v3 only.	usmUser	None	No

Return values

This method has no return values.

Request example with SNMP v3 enabled

Requests for this method are similar to the following example:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":true,
    "usmUsers":[
      {
        "name":"user1",
        "access":"rouser",
        "secLevel":"auth",
        "password":"namex1",
        "passphrase":"yourpassphrase"
      }
    ]
  },
 "id":1
}
```

Request example with SNMP v2 enabled

Requests for this method are similar to the following example:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":false,
    "networks":[
      {
        "community":"public",
        "access":"ro",
        "network":"localhost",
      }
    ]
  },
  "id":1
}
```

Response example

This method returns a response similar to the following example:

```
{
  "id" : 1
  "result" :{
  }
}
```

New since version

9.6

SetSnmpTrapInfo

You can use the `SetSnmpTrapInfo` method to enable and disable the generation of cluster SNMP notifications (traps) and to specify the set of hosts that receive the notifications. The values you pass with each `SetSnmpTrapInfo` method call replace all values set in any previous call.

Parameters

This method has the following input parameters:

Name	Description	Type
trapRecipients	List of hosts that are to receive the traps generated by the storage cluster. At least one object is required if any one of the trap types is enabled. This parameter is required only if any boolean parameters are set to true. (No default value. Not required.)	snmpTrapRecipient array
clusterFaultTrapsEnabled	If set to true, a corresponding cluster fault notification is sent to the configured list of trap recipients when a cluster fault is logged. (Default value: false. Not required.)	boolean
clusterFaultResolvedTrapsEnabled	If set to true, a corresponding cluster fault resolved notification is sent to the configured list of trap recipients when a cluster fault is resolved. (Default value: false. Not required.)	boolean

Name	Description	Type
clusterEventTrapsEnabled	If set to true, a corresponding cluster event notification is sent to the configured list of trap recipients when a cluster event is logged. (Default value: false. Not required.)	boolean

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
"method":"SetSnmpTrapInfo",
"params":{
    "clusterFaultTrapsEnabled":true,
    "clusterFaultResolvedTrapsEnabled":true,
    "clusterEventTrapsEnabled":true,
    "trapRecipients":[
    {
      "host":"192.30.0.10",
      "port":162,
      "community":"public"
    }
   ]
  },
  "id":1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id" : 1,
    "result" : {}
}
```

New since version

9.6

SetSSLCertificate

You can use the `SetSSLCertificate` method to set a user SSL certificate and private key for the storage nodes in the cluster.

After using the API, you must reboot the management node.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
certificate	The PEM-encoded text version of the certificate. **Note:** When setting a node or cluster certificate, the certificate must include the extendedKeyUsage extension for serverAuth. This extension allows the certificate to be used without error on common operating systems and browsers. If the extension is not present, the API will reject the certificate as invalid.	string	None	Yes
privateKey	The PEM-encoded text version of the private key.	string	None	Yes

Return values

This method has no return values.

Request example

Requests for this method are similar to the following example:

```
{
    "method" : "SetSSLCertificate",
    "params" : {
```

```
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEWMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrgpGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yjUGQO352ylc9HXHcn6lb
/jyl0DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAoIBAH1jlIZr6/sltqVW\nO0qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuHl1esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIJIMEgnfuLZp8IelJQXn\nSFJbk2ECgYEA
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nlHzPlhms6hxexwz1dzAp
gog/NOM+2bAc0rn0dqvtV4doejtlDZKRqrNCf/cuN2QX\njaCJClCWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhzXpLr+v30Hy2h0yAlBS\nny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nC9MJtXGfhp//G0bzwsRzZxOBsUJb15tppaZIs9MCgYAJricpkKjM
0xlZ1jdvXsos\nPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+AOeQXw3vgAhJ/qNJ\njQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nzPssy6t+QE
La1fFbAXkZ5Pg1ITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\n+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\njS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\n3rnR8AqAm4VMzqRahs2PWNe2Hl4J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nInDXvTgXMdMoet4BKnftelrXFKHgGqXJoczq4JWzGS
IHNgvkrH60\n-----END RSA PRIVATE KEY-----\n",
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
```

```
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id" : 2,
    "result" : {}
}
```

New since version

10.0

SnmpSendTestTraps

`SnmpSendTestTraps` enables you to test SNMP functionality for a cluster. This method instructs the cluster to send test SNMP traps to the currently configured SNMP manager.

Parameters

This method has no input parameters.

Return value

This method has the following return value:

Name	Description	Type
status	Status of the test.	string

Request example

Requests for this method are similar to the following example:

```
{
    "method": "SnmpSendTestTraps",
    "params": {},
    "id": 1
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "status": "complete"
    }
}
```

New since version

9.6

TestAddressAvailability

You can use the `TestAddressAvailability` method to check to see if a certain IP address is in use on an interface within the storage cluster.

Parameters

This method has the following input parameters:

Name	Description	Type	Default value	Required
interface	The target network interface (such as eth0, Bond10G, etc).	string	None	Yes
address	The IP address to scan for on the target interface.	string	None	Yes
virtualNetworkTag	The target VLAN ID.	integer	None	No
timeout	The timeout in seconds for testing the target address.	integer	5	No

Return values

This method has the following return values:

Name	Description	Type
address	The IP address tested.	string

available	True if the requested IP address is in use, and false if it is not.	boolean

Request example

Requests for this method are similar to the following example:

```
{
    "method": "TestAddressAvailability",
    "params": {
        "interface": "Bond10G",
        "address": "10.0.0.1",
        "virtualNetworkTag": 1234
    }
}
```

Response example

This method returns a response similar to the following example:

```
{
    "id": 1,
    "result": {
        "address":"10.0.0.1",
        "available": true
    }
}
```

New since version

11.0

Copyright information

Copyright © 2025 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.