



Manage LDAP server configurations

ONTAP 9.13.1 REST API reference

NetApp
May 08, 2024

Table of Contents

- Manage LDAP server configurations 1
 - Name-services LDAP endpoint overview 1
 - Retrieve an LDAP configuration for all SVMs 14
 - Create an LDAP configuration for an SVM 29
 - Delete LDAP configuration for an SVM 46
 - Retrieve LDAP configuration for an SVM 48
 - Update LDAP configuration for an SVM 56

Manage LDAP server configurations

Name-services LDAP endpoint overview

Overview

LDAP servers are used to centrally maintain user information. LDAP configurations must be set up to lookup information stored in the LDAP directory on the external LDAP servers. This API is used to retrieve and manage LDAP server configurations.

Retrieving LDAP information

The LDAP GET endpoint retrieves all of the LDAP configurations in the cluster.

Examples

Retrieving all of the fields for all LDAP configurations

```
# The API:
/api/name-services/ldap

# The call:
curl -X GET "https://<mgmt-ip>/api/name-services/ldap?fields=*" -H
"accept: application/hal+json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
        "name": "vs1",
        "_links": {
          "self": {
            "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
          }
        }
      },
      "servers": [
        "10.10.10.10",
        "domainB.example.com"
      ],
      "schema": "ad_idmu",
      "port": 389,
      "ldaps_enabled": false,
```

```

"min_bind_level": "anonymous",
"bind_dn": "cn=Administrators,cn=users,dc=domainA,dc=example,dc=com",
"base_dn": "dc=domainA,dc=example,dc=com",
"base_scope": "subtree",
"use_start_tls": true,
"session_security": "none",
"referral_enabled": false,
"bind_as_cifs_server": false,
"query_timeout": 3,
"is_owner": true,
"user_scope": "subtree",
"group_scope": "subtree",
"netgroup_scope": "subtree",
"is_netgroup_byhost_enabled": false,
"netgroup_byhost_scope": "subtree",
"group_membership_filter": "",
"status": {
  "state": "down",
  "message": "The LDAP configuration is invalid. Verify that the AD
domain or servers are reachable and that the network configuration is
correct",
  "dn_message": [
    "No LDAP DN configured"
  ],
  "code": 4915258,
  "ipv4_state": "down",
  "ipv6_state": "down"
},
"try_channel_binding": true,
"restrict_discovery_to_site" : false,
"_links": {
  "self": {
    "href": "/api/name-services/ldap/179d3c85-7053-11e8-b9b8-
005056b41bd1"
  }
},
{
  "svm": {
    "uuid": "6a52023b-7066-11e8-b9b8-005056b41bd1",
    "name": "vs2",
    "_links": {
      "self": {
        "href": "/api/svm/svms/6a52023b-7066-11e8-b9b8-005056b41bd1"
      }
    }
  }
}

```

```

},
"ad_domain": "example.com",
"schema": "rfc_2307",
"port": 389,
"ldaps_enabled": false,
"min_bind_level": "simple",
"bind_dn": "cn=Administrators,cn=users,dc=domainB,dc=example,dc=com",
"base_dn": "dc=domainB,dc=example,dc=com",
"base_scope": "subtree",
"use_start_tls": true,
"session_security": "sign",
"referral_enabled": false,
"bind_as_cifs_server": false,
"query_timeout": 0,
"is_owner": true,
"user_scope": "subtree",
"group_scope": "subtree",
"netgroup_scope": "subtree",
"is_netgroup_byhost_enabled": false,
"netgroup_byhost_scope": "subtree",
"group_membership_filter": "",
"status": {
  "state": "up",
  "message": "Successfully connected to LDAP server \"172.20.192.44\".
Successfully connected to LDAP server
\"fd20:8b1e:b255:5056:999:d9:516c:bf69\".",
  "dn_message": [
    "All the configured DNs are available."
  ],
  "code": 0,
  "ipv4_state": "up",
  "ipv6_state": "up"
},
"try_channel_binding": true,
"restrict_discovery_to_site": true,
"_links": {
  "self": {
    "href": "/api/name-services/ldap/6a52023b-7066-11e8-b9b8-
005056b41bd1"
  }
}
},
"num_records": 2,
"_links": {
  "self": {

```

```
    "href": "/api/name-services/ldap?fields=*"
  }
}
```

Retrieving all of the LDAP configurations that have the *use_start_tls* set to *true*

```
# The API:
/api/name-services/ldap

# The call:
curl -X GET "https://<mgmt-ip>/api/name-services/ldap?use_start_tls=true"
-H "accept: application/hal+json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "6a52023b-7066-11e8-b9b8-005056b41bd1",
        "name": "vs2",
        "_links": {
          "self": {
            "href": "/api/svm/svms/6a52023b-7066-11e8-b9b8-005056b41bd1"
          }
        }
      },
      "use_start_tls": true,
      "_links": {
        "self": {
          "href": "/api/name-services/ldap/6a52023b-7066-11e8-b9b8-005056b41bd1"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/name-services/ldap?use_start_tls=true"
    }
  }
}
```

Retrieving the LDAP configuration of a specific SVM

```

# The API:
/api/name-services/ldap/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
    "name": "vs1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
      }
    }
  },
  "servers": [
    "10.10.10.10",
    "domainB.example.com"
  ],
  "schema": "ad_idmu",
  "port": 389,
  "ldaps_enabled": false,
  "min_bind_level": "anonymous",
  "bind_dn": "cn=Administrators,cn=users,dc=domainA,dc=example,dc=com",
  "base_dn": "dc=domainA,dc=example,dc=com",
  "base_scope": "subtree",
  "use_start_tls": true,
  "referral_enabled": false,
  "session_security": "none",
  "bind_as_cifs_server": true,
  "query_timeout": 3,
  "is_owner": true,
  "try_channel_binding": true,
  "restrict_discovery_to_site": false,
  "_links": {
    "self": {
      "href": "/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1"
    }
  }
}

```


Retrieving all the fields of the LDAP configuration of a specific SVM

```
# The API:
/api/name-services/ldap/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1?fields=*" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "179d3c85-7053-11e8-b9b8-005056b41bd1",
    "name": "vs1",
    "_links": {
      "self": {
        "href": "/api/svm/svms/179d3c85-7053-11e8-b9b8-005056b41bd1"
      }
    }
  },
  "servers": [
    "10.10.10.10",
    "domainB.example.com"
  ],
  "schema": "ad_idmu",
  "port": 389,
  "ldaps_enabled": false,
  "min_bind_level": "anonymous",
  "bind_dn": "cn=Administrators,cn=users,dc=domainA,dc=example,dc=com",
  "base_dn": "dc=domainA,dc=example,dc=com",
  "base_scope": "subtree",
  "use_start_tls": true,
  "referral_enabled": false,
  "session_security": "none",
  "bind_as_cifs_server": true,
  "query_timeout": 3,
  "is_owner": true,
  "user_scope": "subtree",
  "group_scope": "subtree",
  "netgroup_scope": "subtree",
  "is_netgroup_byhost_enabled": false,
  "netgroup_byhost_scope": "subtree",
  "group_membership_filter": "",
  "try_channel_binding": true,
```

```
"restrict_discovery_to_site": false,
"status": {
  "state": "down",
  "message": "The LDAP configuration is invalid. Verify that the AD domain
or servers are reachable and that the network configuration is correct",
  "dn_message": [
    "No LDAP DN configured"
  ],
  "code": 4915258,
  "ipv4_state": "down",
  "ipv6_state": "down"
},
"_links": {
  "self": {
    "href": "/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1"
  }
}
}
```

Retrieving the LDAP server status of a specific SVM

```
# The API:
/api/name-services/ldap/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/name-services/ldap/9e4a2e3b-f66f-11ea-aec8-0050568e155c?fields=status" -H "accept: application/json"

# The response:
{
  "svm": {
    "uuid": "9e4a2e3b-f66f-11ea-aec8-0050568e155c",
    "name": "vs2"
  },
  "status": {
    "state": "up",
    "message": "Successfully connected to LDAP server \"172.20.192.44\".
Successfully connected to LDAP server
\"fd20:8b1e:b255:5056:999:d9:516c:bf69\".",
    "code": 0,
    "ipv4_state": "up",
    "ipv6_state": "up"
  }
}
```

Retrieving all of the LDAP configurations that have the *restrict_discovery_to_site* set to *true*

```

# The API:
/api/name-services/ldap

# The call:
curl -X GET "https://<mgmt-ip>/api/name-
services/ldap?restrict_discovery_to_site=true" -H "accept:
application/hal+json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "6a52023b-7066-11e8-b9b8-005056b41bd1",
        "name": "vs2",
        "_links": {
          "self": {
            "href": "/api/svm/svms/6a52023b-7066-11e8-b9b8-005056b41bd1"
          }
        }
      },
      "restrict_discovery_to_site": true,
      "_links": {
        "self": {
          "href": "/api/name-services/ldap/6a52023b-7066-11e8-b9b8-
005056b41bd1"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/name-services/ldap?restrict_discovery_to_site=true"
    }
  }
}

```

Creating an LDAP configuration

The LDAP POST endpoint creates an LDAP configuration for the specified SVM.

Examples

Creating an LDAP configuration with all the fields specified

```
# The API:
/api/name-services/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/name-services/ldap" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"svm\": {
\"uuid\": \"179d3c85-7053-11e8-b9b8-005056b41bd1\" }, \"servers\": [
\"10.10.10.10\", \"domainB.example.com\" ], \"schema\": \"ad_idmu\",
\"port\": 389, \"ldaps_enabled\": false, \"min_bind_level\":
\"anonymous\", \"bind_dn\":
\"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"base_scope\": \"subtree\", \"use_start_tls\": false,
\"session_security\": \"none\", \"referral_enabled\": false,
\"bind_as_cifs_server\": false, \"query_timeout\": 4, \"user_dn\":
\"cn=abc,users,dc=com\", \"user_scope\": \"subtree\", \"group_dn\":
\"cn=abc,users,dc=com\", \"group_scope\": \"subtree\", \"netgroup_dn\":
\"cn=abc,users,dc=com\", \"netgroup_scope\": \"subtree\",
\"netgroup_byhost_dn\": \"cn=abc,users,dc=com\",
\"netgroup_byhost_scope\": \"subtree\", \"is_netgroup_byhost_enabled\":
false, \"group_membership_filter\": \"\", \"skip_config_validation\":
false } "
```

Creating an LDAP configuration with Active Directory domain and preferred Active Directory servers specified

```
# The API:
/api/name-services/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/name-services/ldap" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"svm\": {
\"name\": \"vs2\" }, \"ad_domain\": \"domainA.example.com\",
\"preferred_ad_servers\": [ \"11.11.11.11\" ], \"port\": 389,
\"ldaps_enabled\": false, \"bind_dn\":
\"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"session_security\": \"none\", \"referral_enabled\": false,
\"query_timeout\": 3}"
```

Creating an LDAP configuration with a number of optional fields not specified

```
# The API:
/api/name-services/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/name-services/ldap" -H "accept:
application/hal+json" -H "Content-Type: application/json" -d "{ \"svm\": {
\"name\": \"vs2\" }, \"servers\": [ \"11.11.11.11\" ], \"port\": 389,
\"bind_dn\": \"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\",
\"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\",
\"session_security\": \"none\"}"
```

Creating an LDAP configuration with Active Directory domain specified and *restrict_discovery_to_site* set to *true*

```
# The API:
/api/name-services/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/name-services/ldap" -H "accept: application/hal+json" -H "Content-Type: application/json" -d "{ \"svm\": { \"name\": \"vs2\" }, \"ad_domain\": \"example.com\", \"port\": 389, \"bind_dn\": \"cn=Administrators,cn=users,dc=domainA,dc=example,dc=com\", \"bind_password\": \"abc\", \"base_dn\": \"dc=domainA,dc=example,dc=com\", \"session_security\": \"none\", \"restrict_discovery_to_site\": true}"
```

Updating an LDAP configuration

The LDAP PATCH endpoint updates the LDAP configuration for the specified SVM. The following example shows a PATCH operation:

```
# The API:
/api/name-services/ldap/{svm.uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"servers\": [ \"55.55.55.55\" ], \"schema\": \"ad_idmu\", \"port\": 636, \"ldaps_enabled\": true, \"use_start_tls\": false, \"referral_enabled\": false, \"restrict_discovery_to_site\": false}"
```

Deleting an LDAP configuration

The LDAP DELETE endpoint deletes the LDAP configuration for the specified SVM. The following example shows a DELETE operation:

```
# The API:
/api/name-services/ldap/{svm.uuid}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/name-services/ldap/179d3c85-7053-11e8-b9b8-005056b41bd1" -H "accept: application/hal+json"
```

Retrieve an LDAP configuration for all SVMs

GET /name-services/ldap

Introduced In: 9.6

Retrieves the LDAP configurations for all SVMs.

Parameters

| Name | Type | In | Required | Description |
|----------------------------|---------|-------|----------|--|
| ad_domain | string | query | False | Filter by ad_domain <ul style="list-style-type: none">• Introduced in: 9.7 |
| preferred_ad_servers | string | query | False | Filter by preferred_ad_servers <ul style="list-style-type: none">• Introduced in: 9.7 |
| netgroup_byhost_dn | string | query | False | Filter by netgroup_byhost_dn <ul style="list-style-type: none">• Introduced in: 9.9 |
| is_netgroup_byhost_enabled | boolean | query | False | Filter by is_netgroup_byhost_enabled <ul style="list-style-type: none">• Introduced in: 9.9 |
| try_channel_binding | boolean | query | False | Filter by try_channel_binding <ul style="list-style-type: none">• Introduced in: 9.10 |
| svm.uuid | string | query | False | Filter by svm.uuid <ul style="list-style-type: none">• Introduced in: 9.7 |

| Name | Type | In | Required | Description |
|-----------------------|---------|-------|----------|--|
| svm.name | string | query | False | Filter by svm.name <ul style="list-style-type: none"> • Introduced in: 9.7 |
| netgroup_byhost_scope | string | query | False | Filter by netgroup_byhost_scope <ul style="list-style-type: none"> • Introduced in: 9.9 |
| servers | string | query | False | Filter by servers <ul style="list-style-type: none"> • Introduced in: 9.7 |
| base_scope | string | query | False | Filter by base_scope <ul style="list-style-type: none"> • Introduced in: 9.7 |
| is_owner | boolean | query | False | Filter by is_owner <ul style="list-style-type: none"> • Introduced in: 9.9 |
| min_bind_level | string | query | False | Filter by min_bind_level <ul style="list-style-type: none"> • Introduced in: 9.7 |
| use_start_tls | boolean | query | False | Filter by use_start_tls <ul style="list-style-type: none"> • Introduced in: 9.7 |
| query_timeout | integer | query | False | Filter by query_timeout <ul style="list-style-type: none"> • Introduced in: 9.9 |
| bind_dn | string | query | False | Filter by bind_dn <ul style="list-style-type: none"> • Introduced in: 9.7 |

| Name | Type | In | Required | Description |
|---------------------|---------|-------|----------|---|
| session_security | string | query | False | Filter by session_security • Introduced in: 9.7 |
| base_dn | string | query | False | Filter by base_dn • Introduced in: 9.7 |
| user_dn | string | query | False | Filter by user_dn • Introduced in: 9.9 |
| bind_as_cifs_server | boolean | query | False | Filter by bind_as_cifs_server • Introduced in: 9.9 |
| group_scope | string | query | False | Filter by group_scope • Introduced in: 9.9 |
| user_scope | string | query | False | Filter by user_scope • Introduced in: 9.9 |
| referral_enabled | boolean | query | False | Filter by referral_enabled • Introduced in: 9.9 |
| schema | string | query | False | Filter by schema • Introduced in: 9.7 |
| status.code | integer | query | False | Filter by status.code • Introduced in: 9.9 |

| Name | Type | In | Required | Description |
|-------------------|---------|-------|----------|--|
| status.dn_message | string | query | False | Filter by status.dn_message • Introduced in: 9.9 |
| status.ipv6_state | string | query | False | Filter by status.ipv6_state • Introduced in: 9.13 |
| status.message | string | query | False | Filter by status.message • Introduced in: 9.9 |
| status.ipv4_state | string | query | False | Filter by status.ipv4_state • Introduced in: 9.13 |
| status.state | string | query | False | Filter by status.state • Introduced in: 9.9 |
| netgroup_dn | string | query | False | Filter by netgroup_dn • Introduced in: 9.9 |
| ldaps_enabled | boolean | query | False | Filter by ldaps_enabled • Introduced in: 9.9 |
| group_dn | string | query | False | Filter by group_dn • Introduced in: 9.9 |

| Name | Type | In | Required | Description |
|----------------------------|---------------|-------|----------|---|
| group_membership_filter | string | query | False | Filter by group_membership_filter • Introduced in: 9.9 |
| restrict_discovery_to_site | boolean | query | False | Filter by restrict_discovery_to_site • Introduced in: 9.13 |
| netgroup_scope | string | query | False | Filter by netgroup_scope • Introduced in: 9.9 |
| port | integer | query | False | Filter by port • Introduced in: 9.7 • Max value: 65535 • Min value: 1 |
| fields | array[string] | query | False | Specify the fields to return. |
| max_records | integer | query | False | Limit the number of records returned. |
| return_records | boolean | query | False | The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1 |

| Name | Type | In | Required | Description |
|----------------|---------------|-------|----------|--|
| return_timeout | integer | query | False | <p>The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.</p> <ul style="list-style-type: none"> • Max value: 120 • Min value: 0 • Default value: 1 |
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |

Response

Status: 200, Ok

| Name | Type | Description |
|-------------|---------------------------------------|-------------------------|
| _links | _links | |
| num_records | integer | Number of LDAP records. |
| records | array[ldap_service] | |

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "base_scope": "base",
    "group_scope": "base",
    "min_bind_level": "anonymous",
    "netgroup_byhost_scope": "base",
    "netgroup_scope": "base",
    "port": 389,
    "preferred_ad_servers": {
    },
    "servers": {
    },
    "session_security": "none",
    "status": {
      "code": 65537300,
      "dn_message": {
      },
      "ipv4_state": "up",
      "ipv6_state": "up",
      "state": "up"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  },
}
```

```
"user_scope": "base"
}
}
```

Error

Status: Default

Following error codes can be thrown as part of LDAP status information, if LDAP status is needed to be retrieved.

| Error Code | Description |
|------------|--|
| 4915229 | DNS resolution failed due to an internal error. Contact technical support if this issue persists |
| 4915231 | DNS resolution failed for one or more of the specified LDAP servers. Verify that a valid DNS server is configured |
| 23724132 | DNS resolution failed for all the specified LDAP servers. Verify that a valid DNS server is configured |
| 4915258 | The LDAP configuration is invalid. Verify that the Active Directory domain or servers are reachable and that the network configuration is correct |
| 4915263 | Failed to check the current status of LDAP server. Reason:<Reason for="" the="" failure=""></Reason> |
| 4915234 | The specified LDAP server or preferred Active Directory server is not supported because it is one of the following: multicast, loopback, 0.0.0.0, or broadcast |
| 4915265 | The specified bind password or bind DN is invalid |
| 4915264 | Certificate verification failed. Verify that a valid certificate is installed |

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| next | href | |
| self | href | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

status

| Name | Type | Description |
|------------|---------------|--|
| code | integer | Code corresponding to the error message. If there is no error, it will be 0 to indicate success. |
| dn_message | array[string] | |
| ipv4_state | string | The status of the LDAP service with IPv4 address. |
| ipv6_state | string | The status of the LDAP service with IPv6 address. |
| message | string | Provides additional details on the error if <code>ipv4_state</code> or <code>ipv6_state</code> is down. If both <code>ipv4_state</code> and <code>ipv6_state</code> are up, it provides details of the IP addresses that are connected successfully. |

| Name | Type | Description |
|-------|--------|---|
| state | string | The status of the LDAP service for the SVM. The LDAP service is up if either <code>ipv4_state</code> or <code>ipv6_state</code> is up. The LDAP service is down if both <code>ipv4_state</code> and <code>ipv6_state</code> are down. |

svm

| Name | Type | Description |
|------------------------|------------------------|-----------------------------------|
| _links | _links | |
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

ldap_service

| Name | Type | Description |
|------------------------|------------------------|--|
| _links | _links | |
| ad_domain | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| base_dn | string | Specifies the default base DN for all searches. |
| base_scope | string | Specifies the default search scope for LDAP queries: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

| Name | Type | Description |
|----------------------------|---------|---|
| bind_as_cifs_server | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| bind_dn | string | Specifies the user that binds to the LDAP servers. |
| bind_password | string | Specifies the bind password for the LDAP servers. |
| group_dn | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |
| group_membership_filter | string | Specifies the custom filter used for group membership lookups from an LDAP server. |
| group_scope | string | <p>Specifies the default search scope for LDAP for group lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |

| Name | Type | Description |
|-----------------------|--------|--|
| min_bind_level | string | <p>The minimum bind authentication level. Possible values are:</p> <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |
| netgroup_byhost_dn | string | <p>Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups.</p> |
| netgroup_byhost_scope | string | <p>Specifies the default search scope for LDAP for netgroup by host lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| netgroup_dn | string | <p>Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.</p> |
| netgroup_scope | string | <p>Specifies the default search scope for LDAP for netgroup lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

| Name | Type | Description |
|----------------------------|------------------------|---|
| port | integer | The port used to connect to the LDAP Servers. |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | Specifies the maximum time to wait for a query response from the LDAP server, in seconds. |
| referral_enabled | boolean | Specifies whether or not LDAP referral is enabled. |
| restrict_discovery_to_site | boolean | Specifies whether or not LDAP server discovery is restricted to site-scope. |
| schema | string | <p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |
| session_security | string | <p>Specifies the level of security to be used for LDAP communications:</p> <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |

| Name | Type | Description |
|---------------------|---------------------|--|
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |
| user_scope | string | <p>Specifies the default search scope for LDAP for user lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Create an LDAP configuration for an SVM

POST /name-services/ldap

Introduced In: 9.6

Creates an LDAP configuration for an SVM.

Important notes

- Each SVM can have one LDAP configuration.
- The LDAP servers and Active Directory domain are mutually exclusive fields. These fields cannot be empty. At any point in time, either the LDAP servers or Active Directory domain must be populated.
- LDAP configuration with Active Directory domain cannot be created on an admin SVM.
- IPv6 must be enabled if IPv6 family addresses are specified.

The following parameters are optional:

- preferred AD servers
- schema
- port
- ldaps_enabled
- min_bind_level
- bind_password
- base_scope
- use_start_tls
- session_security
- referral_enabled
- bind_as_cifs_server
- query_timeout
- user_dn
- user_scope
- group_dn
- group_scope
- netgroup_dn
- netgroup_scope
- netgroup_byhost_dn
- netgroup_byhost_scope
- is_netgroup_byhost_enabled
- group_membership_filter
- skip_config_validation

- `try_channel_binding`
- `restrict_discovery_to_site`

Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the "servers" field. The Active Directory domain or LDAP servers are validated as part of this operation.

LDAP validation fails in the following scenarios:

1. The server does not have LDAP installed.
2. The server or Active Directory domain is invalid.
3. The server or Active Directory domain is unreachable.

Parameters

| Name | Type | In | Required | Description |
|-----------------------------|---------|-------|----------|---|
| <code>return_records</code> | boolean | query | False | <p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> • Default value: |

Request Body

| Name | Type | Description |
|-------------------------|------------------------|--|
| <code>_links</code> | _links | |
| <code>ad_domain</code> | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| <code>base_dn</code> | string | Specifies the default base DN for all searches. |
| <code>base_scope</code> | string | <p>Specifies the default search scope for LDAP queries:</p> <ul style="list-style-type: none"> • <code>base</code> - search the named entry only • <code>onelevel</code> - search all entries immediately below the DN • <code>subtree</code> - search the named DN entry and the entire subtree below the DN |

| Name | Type | Description |
|----------------------------|---------|---|
| bind_as_cifs_server | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| bind_dn | string | Specifies the user that binds to the LDAP servers. |
| bind_password | string | Specifies the bind password for the LDAP servers. |
| group_dn | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |
| group_membership_filter | string | Specifies the custom filter used for group membership lookups from an LDAP server. |
| group_scope | string | <p>Specifies the default search scope for LDAP for group lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |
| min_bind_level | string | <p>The minimum bind authentication level. Possible values are:</p> <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |

| Name | Type | Description |
|-----------------------|---------------|---|
| netgroup_byhost_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups. |
| netgroup_byhost_scope | string | Specifies the default search scope for LDAP for netgroup by host lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| netgroup_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups. |
| netgroup_scope | string | Specifies the default search scope for LDAP for netgroup lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| port | integer | The port used to connect to the LDAP Servers. |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | Specifies the maximum time to wait for a query response from the LDAP server, in seconds. |
| referral_enabled | boolean | Specifies whether or not LDAP referral is enabled. |

| Name | Type | Description |
|----------------------------|------------------------|---|
| restrict_discovery_to_site | boolean | Specifies whether or not LDAP server discovery is restricted to site-scope. |
| schema | string | <p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |
| session_security | string | <p>Specifies the level of security to be used for LDAP communications:</p> <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |

| Name | Type | Description |
|------------|--------|--|
| user_scope | string | <p>Specifies the default search scope for LDAP for user lookups:</p> <ul style="list-style-type: none">• base - search the named entry only• onelevel - search all entries immediately below the DN• subtree - search the named DN entry and the entire subtree below the DN |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "group_scope": "base",
  "min_bind_level": "anonymous",
  "netgroup_byhost_scope": "base",
  "netgroup_scope": "base",
  "port": 389,
  "preferred_ad_servers": {
  },
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "ipv4_state": "up",
    "ipv6_state": "up",
    "state": "up"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "user_scope": "base"
}
```

Response

Status: 201, Created

| Name | Type | Description |
|-------------|---------------------------------------|-------------------------|
| _links | _links | |
| num_records | integer | Number of LDAP records. |
| records | array[ldap_service] | |

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "base_scope": "base",
    "group_scope": "base",
    "min_bind_level": "anonymous",
    "netgroup_byhost_scope": "base",
    "netgroup_scope": "base",
    "port": 389,
    "preferred_ad_servers": {
    },
    "servers": {
    },
    "session_security": "none",
    "status": {
      "code": 65537300,
      "dn_message": {
      },
      "ipv4_state": "up",
      "ipv6_state": "up",
      "state": "up"
    },
    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  },
}
```

```
"user_scope": "base"
}
}
```

Headers

| Name | Description | Type |
|----------|---|--------|
| Location | Useful for tracking the resource location | string |

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|---|
| 262186 | LDAP Servers cannot be used with Active Directory domain and/or preferred Active Directory servers |
| 2621488 | Invalid SVM context |
| 2621706 | The specified SVM UUID is incorrect for the specified SVM name |
| 4915203 | The specified LDAP schema does not exist |
| 262222 | The specified LDAP servers or preferred Active Directory servers contain duplicate server entries |
| 4915229 | DNS resolution failed due to an internal error. Contact technical support if this issue persists |
| 4915231 | DNS resolution failed for one or more of the specified LDAP servers. Verify that a valid DNS server is configured |
| 23724132 | DNS resolution failed for all the specified LDAP servers. Verify that a valid DNS server is configured |
| 4915234 | The specified LDAP server or preferred Active Directory server is not supported because it is one of the following: multicast, loopback, 0.0.0.0, or broadcast |
| 4915248 | LDAP servers cannot be empty or "-". Specified Active Directory domain is invalid because it is empty or "-" or it contains either the special characters or "-" at the start or end of the domain) |
| 4915251 | STARTTLS and LDAPS cannot be used together |

| Error Code | Description |
|------------|---|
| 4915257 | The LDAP configuration is invalid. Verify that bind-dn and bind password are correct |
| 4915258 | The LDAP configuration is invalid. Verify that the Active Directory domain or servers are reachable and that the network configuration is correct |
| 4915259 | LDAP configurations with Active Directory domains are not supported on admin SVM. |
| 4915265 | The specified bind password or bind DN is invalid |
| 4915264 | Certificate verification failed. Verify that a valid certificate is installed |
| 13434916 | The SVM is in the process of being created. Wait a few minutes, and then try the command again. |
| 23724130 | Cannot use an IPv6 name server address because there are no IPv6 LIFs |
| 4915252 | LDAP Referral is not supported with STARTTLS, with session security levels sign, seal or with LDAPS. |
| 4915266 | LDAP site discovery restriction cannot be applied to a mixed version cluster. |
| 656477 | Need default site to be specified to enable site restriction. |
| 4915206 | CIFS server is not configured for the vserver. LDAP client configuration requires CIFS server for binding. |

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

status

| Name | Type | Description |
|------------|---------------|--|
| code | integer | Code corresponding to the error message. If there is no error, it will be 0 to indicate success. |
| dn_message | array[string] | |
| ipv4_state | string | The status of the LDAP service with IPv4 address. |
| ipv6_state | string | The status of the LDAP service with IPv6 address. |
| message | string | Provides additional details on the error if <code>ipv4_state</code> or <code>ipv6_state</code> is down. If both <code>ipv4_state</code> and <code>ipv6_state</code> are up, it provides details of the IP addresses that are connected successfully. |
| state | string | The status of the LDAP service for the SVM. The LDAP service is up if either <code>ipv4_state</code> or <code>ipv6_state</code> is up. The LDAP service is down if both <code>ipv4_state</code> and <code>ipv6_state</code> are down. |

svm

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|------|--------|-----------------------------------|
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

ldap_service

| Name | Type | Description |
|---------------------|------------------------|--|
| _links | _links | |
| ad_domain | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| base_dn | string | Specifies the default base DN for all searches. |
| base_scope | string | Specifies the default search scope for LDAP queries: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| bind_as_cifs_server | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| bind_dn | string | Specifies the user that binds to the LDAP servers. |
| bind_password | string | Specifies the bind password for the LDAP servers. |
| group_dn | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |

| Name | Type | Description |
|----------------------------|---------|---|
| group_membership_filter | string | Specifies the custom filter used for group membership lookups from an LDAP server. |
| group_scope | string | <p>Specifies the default search scope for LDAP for group lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |
| min_bind_level | string | <p>The minimum bind authentication level. Possible values are:</p> <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |
| netgroup_byhost_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups. |

| Name | Type | Description |
|----------------------------|---------------|---|
| netgroup_byhost_scope | string | Specifies the default search scope for LDAP for netgroup by host lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| netgroup_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups. |
| netgroup_scope | string | Specifies the default search scope for LDAP for netgroup lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| port | integer | The port used to connect to the LDAP Servers. |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | Specifies the maximum time to wait for a query response from the LDAP server, in seconds. |
| referral_enabled | boolean | Specifies whether or not LDAP referral is enabled. |
| restrict_discovery_to_site | boolean | Specifies whether or not LDAP server discovery is restricted to site-scope. |

| Name | Type | Description |
|------------------------|------------------------|---|
| schema | string | <p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |
| session_security | string | <p>Specifies the level of security to be used for LDAP communications:</p> <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |

| Name | Type | Description |
|------------|--------|---|
| user_scope | string | Specifies the default search scope for LDAP for user lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| next | href | |
| self | href | |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Delete LDAP configuration for an SVM

DELETE /name-services/ldap/{svm.uuid}

Introduced In: 9.6

Deletes the LDAP configuration of the specified SVM. LDAP can be removed as a source from the ns-switch if LDAP is not used as a source for lookups.

Parameters

| Name | Type | In | Required | Description |
|----------|--------|------|----------|---|
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |

Response

Status: 200, Ok

Error

Status: Default, Error

| Name | Type | Description |
|-------|-----------------------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Retrieve LDAP configuration for an SVM

GET /name-services/ldap/{svm.uuid}

Introduced In: 9.6

Retrieves LDAP configuration for an SVM. All parameters for the LDAP configuration are displayed by default.

Parameters

| Name | Type | In | Required | Description |
|----------|---------------|-------|----------|---|
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |
| fields | array[string] | query | False | Specify the fields to return. |

Response

Status: 200, Ok

| Name | Type | Description |
|--------------------------------------|------------------------|---|
| <code>_links</code> | _links | |
| <code>ad_domain</code> | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| <code>base_dn</code> | string | Specifies the default base DN for all searches. |
| <code>base_scope</code> | string | Specifies the default search scope for LDAP queries: <ul style="list-style-type: none"> • <code>base</code> - search the named entry only • <code>onelevel</code> - search all entries immediately below the DN • <code>subtree</code> - search the named DN entry and the entire subtree below the DN |
| <code>bind_as_cifs_server</code> | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| <code>bind_dn</code> | string | Specifies the user that binds to the LDAP servers. |
| <code>bind_password</code> | string | Specifies the bind password for the LDAP servers. |
| <code>group_dn</code> | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |
| <code>group_membership_filter</code> | string | Specifies the custom filter used for group membership lookups from an LDAP server. |

| Name | Type | Description |
|----------------------------|---------|--|
| group_scope | string | <p>Specifies the default search scope for LDAP for group lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |
| min_bind_level | string | <p>The minimum bind authentication level. Possible values are:</p> <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |
| netgroup_byhost_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups. |
| netgroup_byhost_scope | string | <p>Specifies the default search scope for LDAP for netgroup by host lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

| Name | Type | Description |
|----------------------------|---------------|--|
| netgroup_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups. |
| netgroup_scope | string | Specifies the default search scope for LDAP for netgroup lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| port | integer | The port used to connect to the LDAP Servers. |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | Specifies the maximum time to wait for a query response from the LDAP server, in seconds. |
| referral_enabled | boolean | Specifies whether or not LDAP referral is enabled. |
| restrict_discovery_to_site | boolean | Specifies whether or not LDAP server discovery is restricted to site-scope. |
| schema | string | The name of the schema template used by the SVM. <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |

| Name | Type | Description |
|------------------------|------------------------|---|
| session_security | string | Specifies the level of security to be used for LDAP communications: <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |
| user_scope | string | Specifies the default search scope for LDAP for user lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "group_scope": "base",
  "min_bind_level": "anonymous",
  "netgroup_byhost_scope": "base",
  "netgroup_scope": "base",
  "port": 389,
  "preferred_ad_servers": {
  },
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "ipv4_state": "up",
    "ipv6_state": "up",
    "state": "up"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "user_scope": "base"
}
```

Error

Status: Default, Error

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

status

| Name | Type | Description |
|------------|---------------|--|
| code | integer | Code corresponding to the error message. If there is no error, it will be 0 to indicate success. |
| dn_message | array[string] | |
| ipv4_state | string | The status of the LDAP service with IPv4 address. |
| ipv6_state | string | The status of the LDAP service with IPv6 address. |
| message | string | Provides additional details on the error if <code>ipv4_state</code> or <code>ipv6_state</code> is down. If both <code>ipv4_state</code> and <code>ipv6_state</code> are up, it provides details of the IP addresses that are connected successfully. |
| state | string | The status of the LDAP service for the SVM. The LDAP service is up if either <code>ipv4_state</code> or <code>ipv6_state</code> is up. The LDAP service is down if both <code>ipv4_state</code> and <code>ipv6_state</code> are down. |

svm

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|------|--------|-----------------------------------|
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Update LDAP configuration for an SVM

```
PATCH /name-services/ldap/{svm.uuid}
```

Introduced In: 9.6

Updates an LDAP configuration of an SVM.

Important notes

- Both mandatory and optional parameters of the LDAP configuration can be updated.
- The LDAP servers and Active Directory domain are mutually exclusive fields. These fields cannot be empty. At any point in time, either the LDAP servers or Active Directory domain must be populated.
- IPv6 must be enabled if IPv6 family addresses are specified.

Configuring more than one LDAP server is recommended to avoid a single point of failure. Both FQDNs and IP addresses are supported for the "servers" field. The Active Directory domain or LDAP servers are validated as part of this operation.

LDAP validation fails in the following scenarios:

1. The server does not have LDAP installed.
2. The server or Active Directory domain is invalid.
3. The server or Active Directory domain is unreachable

Parameters

| Name | Type | In | Required | Description |
|----------|--------|------|----------|---|
| svm.uuid | string | path | True | UUID of the SVM to which this object belongs. |

Request Body

| Name | Type | Description |
|---------------------|------------------------|--|
| _links | _links | |
| ad_domain | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| base_dn | string | Specifies the default base DN for all searches. |
| base_scope | string | Specifies the default search scope for LDAP queries: <ul style="list-style-type: none">• base - search the named entry only• onelevel - search all entries immediately below the DN• subtree - search the named DN entry and the entire subtree below the DN |
| bind_as_cifs_server | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| bind_dn | string | Specifies the user that binds to the LDAP servers. |
| bind_password | string | Specifies the bind password for the LDAP servers. |

| Name | Type | Description |
|----------------------------|---------|--|
| group_dn | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |
| group_membership_filter | string | Specifies the custom filter used for group membership lookups from an LDAP server. |
| group_scope | string | Specifies the default search scope for LDAP for group lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |
| min_bind_level | string | The minimum bind authentication level. Possible values are: <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |
| netgroup_byhost_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups. |

| Name | Type | Description |
|----------------------------|---------------|---|
| netgroup_byhost_scope | string | Specifies the default search scope for LDAP for netgroup by host lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| netgroup_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups. |
| netgroup_scope | string | Specifies the default search scope for LDAP for netgroup lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| port | integer | The port used to connect to the LDAP Servers. |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | Specifies the maximum time to wait for a query response from the LDAP server, in seconds. |
| referral_enabled | boolean | Specifies whether or not LDAP referral is enabled. |
| restrict_discovery_to_site | boolean | Specifies whether or not LDAP server discovery is restricted to site-scope. |

| Name | Type | Description |
|------------------------|------------------------|---|
| schema | string | <p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |
| session_security | string | <p>Specifies the level of security to be used for LDAP communications:</p> <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |

| Name | Type | Description |
|------------|--------|--|
| user_scope | string | <p>Specifies the default search scope for LDAP for user lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_scope": "base",
  "group_scope": "base",
  "min_bind_level": "anonymous",
  "netgroup_byhost_scope": "base",
  "netgroup_scope": "base",
  "port": 389,
  "preferred_ad_servers": {
  },
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "ipv4_state": "up",
    "ipv6_state": "up",
    "state": "up"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "user_scope": "base"
}
```

Response

Status: 200, Ok

Error

Status: Default

ONTAP Error Response Codes

| Error Code | Description |
|------------|---|
| 262186 | LDAP Servers cannot be used with Active Directory domain and/or preferred Active Directory servers |
| 2621488 | Invalid SVM context |
| 2621706 | The specified SVM UUID is incorrect for the specified SVM name |
| 4915203 | The specified LDAP schema does not exist |
| 262222 | The specified LDAP servers or preferred Active Directory servers contain duplicate server entries |
| 4915229 | DNS resolution failed due to an internal error. Contact technical support if this issue persists |
| 4915231 | DNS resolution failed for one or more of the specified LDAP servers. Verify that a valid DNS server is configured |
| 23724132 | DNS resolution failed for all the specified LDAP servers. Verify that a valid DNS server is configured |
| 4915234 | The specified LDAP server or preferred Active Directory server is not supported because it is one of the following: multicast, loopback, 0.0.0.0, or broadcast |
| 4915248 | LDAP servers cannot be empty or "-". Specified Active Directory domain is invalid because it is empty or "-" or it contains either the special characters or "-" at the start or end of the domain. |
| 4915251 | STARTTLS and LDAPS cannot be used together |
| 4915257 | The LDAP configuration is invalid. Verify that the distinguished names and bind password are correct |
| 4915258 | The LDAP configuration is invalid. Verify that the Active Directory domain or servers are reachable and that the network configuration is correct |
| 4915259 | LDAP configurations with Active Directory domains are not supported on admin SVM. |
| 23724130 | Cannot use an IPv6 name server address because there are no IPv6 LIFs |
| 4915252 | LDAP Referral is not supported with STARTTLS, with session security levels sign, seal or with LDAPS. |

| Error Code | Description |
|------------|--|
| 4915266 | LDAP site discovery restriction cannot be applied to a mixed version cluster. |
| 656477 | Need default site to be specified to enable site restriction. |
| 4915206 | CIFS server is not configured for the vserver. LDAP client configuration requires CIFS server for binding. |

| Name | Type | Description |
|-------|-------|-------------|
| error | error | |

Example error

```
{
  "error": {
    "arguments": {
      "code": "string",
      "message": "string"
    },
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

| Name | Type | Description |
|------|--------|-------------|
| href | string | |

_links

| Name | Type | Description |
|------|----------------------|-------------|
| self | href | |

status

| Name | Type | Description |
|------------|---------------|--|
| code | integer | Code corresponding to the error message. If there is no error, it will be 0 to indicate success. |
| dn_message | array[string] | |
| ipv4_state | string | The status of the LDAP service with IPv4 address. |
| ipv6_state | string | The status of the LDAP service with IPv6 address. |
| message | string | Provides additional details on the error if <code>ipv4_state</code> or <code>ipv6_state</code> is down. If both <code>ipv4_state</code> and <code>ipv6_state</code> are up, it provides details of the IP addresses that are connected successfully. |
| state | string | The status of the LDAP service for the SVM. The LDAP service is up if either <code>ipv4_state</code> or <code>ipv6_state</code> is up. The LDAP service is down if both <code>ipv4_state</code> and <code>ipv6_state</code> are down. |

svm

| Name | Type | Description |
|--------|------------------------|-------------|
| _links | _links | |

| Name | Type | Description |
|------|--------|-----------------------------------|
| name | string | The name of the SVM. |
| uuid | string | The unique identifier of the SVM. |

ldap_service

| Name | Type | Description |
|---------------------|------------------------|--|
| _links | _links | |
| ad_domain | string | This parameter specifies the name of the Active Directory domain used to discover LDAP servers for use by this client. This is mutually exclusive with <code>servers</code> during POST and PATCH. |
| base_dn | string | Specifies the default base DN for all searches. |
| base_scope | string | Specifies the default search scope for LDAP queries: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| bind_as_cifs_server | boolean | Specifies whether or not CIFS server's credentials are used to bind to the LDAP server. |
| bind_dn | string | Specifies the user that binds to the LDAP servers. |
| bind_password | string | Specifies the bind password for the LDAP servers. |
| group_dn | string | Specifies the group Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for group lookups. |

| Name | Type | Description |
|----------------------------|---------|---|
| group_membership_filter | string | Specifies the custom filter used for group membership lookups from an LDAP server. |
| group_scope | string | <p>Specifies the default search scope for LDAP for group lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| is_netgroup_byhost_enabled | boolean | Specifies whether or not netgroup by host querying is enabled. |
| is_owner | boolean | Specifies whether or not the SVM owns the LDAP client configuration. |
| ldaps_enabled | boolean | Specifies whether or not LDAPS is enabled. |
| min_bind_level | string | <p>The minimum bind authentication level. Possible values are:</p> <ul style="list-style-type: none"> • anonymous - anonymous bind • simple - simple bind • sasl - Simple Authentication and Security Layer (SASL) bind |
| netgroup_byhost_dn | string | Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup by host lookups. |

| Name | Type | Description |
|----------------------------|---------------|--|
| netgroup_byhost_scope | string | <p>Specifies the default search scope for LDAP for netgroup by host lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| netgroup_dn | string | <p>Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.</p> |
| netgroup_scope | string | <p>Specifies the default search scope for LDAP for netgroup lookups:</p> <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |
| port | integer | <p>The port used to connect to the LDAP Servers.</p> |
| preferred_ad_servers | array[string] | |
| query_timeout | integer | <p>Specifies the maximum time to wait for a query response from the LDAP server, in seconds.</p> |
| referral_enabled | boolean | <p>Specifies whether or not LDAP referral is enabled.</p> |
| restrict_discovery_to_site | boolean | <p>Specifies whether or not LDAP server discovery is restricted to site-scope.</p> |

| Name | Type | Description |
|------------------------|------------------------|---|
| schema | string | <p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> • AD-IDMU - Active Directory Identity Management for UNIX • AD-SFU - Active Directory Services for UNIX • MS-AD-BIS - Active Directory Identity Management for UNIX • RFC-2307 - Schema based on RFC 2307 • Custom schema |
| servers | array[string] | |
| session_security | string | <p>Specifies the level of security to be used for LDAP communications:</p> <ul style="list-style-type: none"> • none - no signing or sealing • sign - sign LDAP traffic • seal - seal and sign LDAP traffic |
| skip_config_validation | boolean | Indicates whether or not the validation for the specified LDAP configuration is disabled. |
| status | status | |
| svm | svm | |
| try_channel_binding | boolean | Specifies whether or not channel binding is attempted in the case of TLS/LDAPS. |
| use_start_tls | boolean | Specifies whether or not to use Start TLS over LDAP connections. |
| user_dn | string | Specifies the user Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for user lookups. |

| Name | Type | Description |
|------------|--------|---|
| user_scope | string | Specifies the default search scope for LDAP for user lookups: <ul style="list-style-type: none"> • base - search the named entry only • onelevel - search all entries immediately below the DN • subtree - search the named DN entry and the entire subtree below the DN |

error_arguments

| Name | Type | Description |
|---------|--------|------------------|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|-----------|--|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

Copyright information

Copyright © 2024 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.