



# **Manage LDAP server configuration**

ONTAP 9.12.1 REST API reference

NetApp  
May 08, 2024

# Table of Contents

- Manage LDAP server configuration . . . . . 1
  - Security authentication cluster LDAP endpoint overview . . . . . 1
  - Delete the LDAP configuration for the cluster . . . . . 3
  - Retrieve the LDAP configuration for the cluster . . . . . 4
  - Update the LDAP configuration for the cluster . . . . . 12
  - Create the LDAP configuration for the cluster . . . . . 23

# Manage LDAP server configuration

## Security authentication cluster LDAP endpoint overview

### Overview

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

### Examples

#### Retrieving the cluster LDAP information

The cluster LDAP GET request retrieves the LDAP configuration of the cluster.

The following example shows how a GET request is used to retrieve the cluster LDAP information:

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X GET "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json"

# The response:
{
  "servers": [
    "10.10.10.10",
    "domainB.example.com"
  ],
  "schema": "ad_idmu",
  "port": 389,
  "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",
  "try_channel_binding": true,
  "_links": {
    "self": {
      "href": "/api/security/authentication/cluster/ldap"
    }
  }
}
```

## Creating the cluster LDAP configuration

The cluster LDAP POST operation creates an LDAP configuration for the cluster.

The following example shows how to issue a POST request with all of the fields specified:

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"servers\": [ \"10.10.10.10\", \"domainB.example.com\" ], \"schema\":
\"ad_idmu\", \"port\": 389, \"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\"}"
```

The following example shows how to issue a POST request with a number of optional fields not specified:

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X POST "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/hal+json" -H "Content-Type: application/json" -d
"{ \"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\"}"
```

## Updating the cluster LDAP configuration

The cluster LDAP PATCH request updates the LDAP configuration of the cluster.

The following example shows how a PATCH request is used to update the cluster LDAP configuration:

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X PATCH "https://<mgmt-ip>/api/security/authentication/cluster/ldap"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
\"servers\": [ \"55.55.55.55\" ], \"schema\": \"ad_idmu\", \"port\": 636,
\"use_start_tls\": false }"
```

## Deleting the cluster LDAP configuration

The cluster LDAP DELETE request deletes the LDAP configuration of the cluster.

The following example shows how a DELETE request is used to delete the cluster LDAP configuration:

```
# The API:
/api/security/authentication/cluster/ldap

# The call:
curl -X DELETE "https://<mgmt-
ip>/api/security/authentication/cluster/ldap" -H "accept:
application/hal+json"
```

## Delete the LDAP configuration for the cluster

DELETE /security/authentication/cluster/ldap

**Introduced In:** 9.6

Deletes the LDAP configuration of the cluster.

## Response

Status: 200, Ok

## Error

Status: Default, Error

Name	Type	Description
error	<a href="#">error</a>	

## 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[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Retrieve the LDAP configuration for the cluster

GET /security/authentication/cluster/ldap

Introduced In: 9.6

Retrieves the cluster LDAP configuration.

## Parameters

Name	Type	In	Required	Description
fields	array[string]	query	False	Specify the fields to return.

## Response

Status: 200, Ok

Name	Type	Description
<a href="#">_links</a>	<a href="#">_links</a>	
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"><li>• base - search the named entry only</li><li>• onelevel - search all entries immediately below the DN</li><li>• subtree - search the named DN entry and the entire subtree below the DN</li></ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
port	integer	<p>The port used to connect to the LDAP Servers.</p>
query_timeout	integer	<p>Specifies the maximum time to wait for a query response from the LDAP server, in seconds.</p>

Name	Type	Description
schema	string	<p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

### 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,
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "state": "up"
  },
  "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	<a href="#">href</a>	

status

Name	Type	Description
code	integer	Code corresponding to the status message.
dn_message	array[string]	
message	string	Provides additional details on the status of the LDAP service.
state	string	Specifies the status of the LDAP service.

error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

# Update the LDAP configuration for the cluster

PATCH /security/authentication/cluster/ldap

**Introduced In:** 9.6

Both mandatory and optional parameters of the LDAP configuration can be updated. 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` property. The 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 is invalid.
3. The server is unreachable.

## Request Body

Name	Type	Description
<code>_links</code>	<a href="#">_links</a>	
<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"><li>• base - search the named entry only</li><li>• onelevel - search all entries immediately below the DN</li><li>• subtree - search the named DN entry and the entire subtree below the DN</li></ul>
<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.

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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
port	integer	<p>The port used to connect to the LDAP Servers.</p>
query_timeout	integer	<p>Specifies the maximum time to wait for a query response from the LDAP server, in seconds.</p>



Name	Type	Description
schema	string	<p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

### 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,
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "state": "up"
  },
  "user_scope": "base"
}
```

### Response

Status: 200, Ok

## Error

Status: Default

### ONTAP Error Response Codes

Error Code	Description
4915203	The specified LDAP schema does not exist.
4915208	The specified LDAP 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	Specified LDAP 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 FQDN is not valid because it is empty or "-" or it contains either special characters or "-" at the start or end of the domain.
4915251	STARTTLS and LDAPS cannot be used together
4915257	The LDAP configuration is not valid. Verify that the Distinguished Names and bind password are correct.
4915258	The LDAP configuration is not valid. Verify that the servers are reachable and that the network configuration is correct.
23724130	Cannot use an IPv6 name server address because there are no IPv6 interfaces.
4915252	LDAP referral is not supported with STARTTLS, with session security levels sign, seal or with LDAPS.

Name	Type	Description
error	<a href="#">error</a>	

### 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	<a href="#">href</a>	

status

Name	Type	Description
code	integer	Code corresponding to the status message.
dn_message	array[string]	
message	string	Provides additional details on the status of the LDAP service.
state	string	Specifies the status of the LDAP service.

cluster\_ldap

Name	Type	Description
_links	<a href="#">_links</a>	
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"><li>• base - search the named entry only</li><li>• onelevel - search all entries immediately below the DN</li><li>• subtree - search the named DN entry and the entire subtree below the DN</li></ul>

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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

Name	Type	Description
port	integer	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.
schema	string	<p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
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.



Name	Type	Description
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Create the LDAP configuration for the cluster

POST /security/authentication/cluster/ldap

**Introduced In:** 9.6

A cluster can have only one LDAP configuration. IPv6 must be enabled if IPv6 family addresses are specified.

## Required properties

- `servers` - List of LDAP servers used for this client configuration.
- `bind_dn` - Specifies the user that binds to the LDAP servers.
- `base_dn` - Specifies the default base DN for all searches.

## Recommended optional properties

- `schema` - Schema template name.
- `port` - Port used to connect to the LDAP Servers.
- `ldaps_enabled` - Specifies whether or not LDAPS is enabled.
- `min_bind_level` - Minimum bind authentication level.
- `bind_password` - Specifies the bind password for the LDAP servers.
- `base_scope` - Specifies the default search scope for LDAP queries.
- `use_start_tls` - Specifies whether or not to use Start TLS over LDAP connections.
- `session_security` - Specifies the level of security to be used for LDAP communications.
- `bind_as_cifs_server` - Indicates if CIFS server's credentials are used to bind to the LDAP server.
- `query_timeout` - Maximum time to wait for a query response from the LDAP server, in seconds.
- `user_dn` - User Distinguished Name (DN) used as the starting point in the LDAP directory tree for user lookups.
- `user_scope` - Default search scope for LDAP for user lookups.
- `group_dn` - Group Distinguished Name (DN) used as the starting point in the LDAP directory tree for group lookups.
- `group_scope` - Default search scope for LDAP for group lookups.
- `netgroup_dn` - Netgroup Distinguished Name (DN) used as the starting point in the LDAP directory tree for netgroup lookups.
- `netgroup_scope` - Default search scope for LDAP for netgroup lookups.
- `netgroup_byhost_dn` - Netgroup Distinguished Name (DN) used as the starting point in the LDAP directory tree for netgroup by host lookups.
- `netgroup_byhost_scope` - Default search scope for LDAP for netgroup by host lookups.
- `is_netgroup_byhost_enabled` - Specifies whether netgroup by host querying is enabled.
- `group_membership_filter` - Custom filter used for group membership lookup from an LDAP server.
- `skip_config_validation` - Indicates whether or not the validation for the specified LDAP configuration is disabled.

## Default property values

- `schema` - *RFC-2307*
- `port` - *389*

- `ldaps_enabled` - *false*
- `min_bind_level` - *simple*
- `base_scope` - *subtree*
- `use_start_tls` - *false*
- `session_security` - *none*
- `query_timeout` - *3*
- `user_scope` - *subtree*
- `group_scope` - *subtree*
- `netgroup_scope` - *subtree*
- `netgroup_byhost_scope` - *subtree*
- `is_netgroup_byhost_enabled` - *false*
- `skip_config_validation` - *false*
- `try_channel_binding` - *true*

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` property. The 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 is invalid.
3. The server is unreachable.

## Request Body

Name	Type	Description
<code>_links</code>	<a href="#">_links</a>	
<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"> <li>• <code>base</code> - search the named entry only</li> <li>• <code>onelevel</code> - search all entries immediately below the DN</li> <li>• <code>subtree</code> - search the named DN entry and the entire subtree below the DN</li> </ul>

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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>

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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
port	integer	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.

Name	Type	Description
schema	string	<p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

### 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,
  "servers": {
  },
  "session_security": "none",
  "status": {
    "code": 65537300,
    "dn_message": {
    },
    "state": "up"
  },
  "user_scope": "base"
}
```

### Response

Status: 201, Created

Name	Type	Description
_links	<a href="#">_links</a>	
num_records	integer	Number of LDAP records.
records	array[ <a href="#">ldap_service</a> ]	



**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": {
      },
      "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
4915203	The specified LDAP schema does not exist.
4915207	The specified LDAP 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 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 FQDN is invalid because it is empty or "-" or it contains either 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 bind-dn and bind password are correct.
4915258	The LDAP configuration is invalid. Verify that the servers are reachable and that the network configuration is correct.
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 interfaces.
4915252	LDAP referral is not supported with STARTTLS, with session security levels sign, seal or with LDAPS.

Name	Type	Description
error	<a href="#">error</a>	

### 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	<a href="#">href</a>	

status

Name	Type	Description
code	integer	Code corresponding to the status message.
dn_message	array[string]	
message	string	Provides additional details on the status of the LDAP service.
state	string	Specifies the status of the LDAP service.

cluster\_ldap

Name	Type	Description
_links	<a href="#">_links</a>	
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"><li>• base - search the named entry only</li><li>• onelevel - search all entries immediately below the DN</li><li>• subtree - search the named DN entry and the entire subtree below the DN</li></ul>

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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

Name	Type	Description
port	integer	The port used to connect to the LDAP Servers.
query_timeout	integer	Specifies the maximum time to wait for a query response from the LDAP server, in seconds.
schema	string	<p>The name of the schema template used by the SVM.</p> <ul style="list-style-type: none"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
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.



Name	Type	Description
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

#### \_links

Name	Type	Description
next	<a href="#">href</a>	
self	<a href="#">href</a>	

#### svm

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

#### ldap\_service

Name	Type	Description
_links	<a href="#">_links</a>	
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.

Name	Type	Description
base_dn	string	Specifies the default base DN for all searches.
base_scope	string	<p>Specifies the default search scope for LDAP queries:</p> <ul style="list-style-type: none"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

Name	Type	Description
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"> <li>• anonymous - anonymous bind</li> <li>• simple - simple bind</li> <li>• sasl - Simple Authentication and Security Layer (SASL) bind</li> </ul>
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
netgroup_dn	string	Specifies the netgroup Distinguished Name (DN) that is used as the starting point in the LDAP directory tree for netgroup lookups.

Name	Type	Description
netgroup_scope	string	Specifies the default search scope for LDAP for netgroup lookups: <ul style="list-style-type: none"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>
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"> <li>• AD-IDMU - Active Directory Identity Management for UNIX</li> <li>• AD-SFU - Active Directory Services for UNIX</li> <li>• MS-AD-BIS - Active Directory Identity Management for UNIX</li> <li>• RFC-2307 - Schema based on RFC 2307</li> <li>• Custom schema</li> </ul>
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"> <li>• none - no signing or sealing</li> <li>• sign - sign LDAP traffic</li> <li>• seal - seal and sign LDAP traffic</li> </ul>
skip_config_validation	boolean	Indicates whether or not the validation for the specified LDAP configuration is disabled.
status	<a href="#">status</a>	
svm	<a href="#">svm</a>	
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"> <li>• base - search the named entry only</li> <li>• onelevel - search all entries immediately below the DN</li> <li>• subtree - search the named DN entry and the entire subtree below the DN</li> </ul>

#### error\_arguments

Name	Type	Description
code	string	Argument code

Name	Type	Description
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	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.