



Manage LDAP server configuration

ONTAP 9.6 REST API reference

NetApp
August 29, 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 5
 - Update the LDAP configuration for the cluster 9
 - Create the LDAP configuration for the cluster 16

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 operation retrieves the LDAP configuration of the cluster.

The following example shows how a GET operation 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",
  "_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 operation updates the LDAP configuration of the cluster.

The following example shows how a PATCH operation 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 operation deletes the LDAP configuration of the cluster.

The following example shows how a DELETE operation 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
```

The DELETE operation removes the LDAP configuration of the cluster.

Learn more

- [DOC /security/authentication/cluster/ldap](#)

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 the LDAP configuration for the cluster

GET /security/authentication/cluster/ldap

Retrieves the cluster LDAP configuration.

Learn more

- [DOC /security/authentication/cluster/ldap](#)

Parameters

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

Response

Status: 200, Ok

Name	Type	Description
_links	_links	
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_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
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
port	integer	<p>The port used to connect to the LDAP Servers.</p>
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
use_start_tls	boolean	<p>Specifies whether or not to use Start TLS over LDAP connections.</p>

Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "bind_password": "string",
  "min_bind_level": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string"
}
```

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	

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 the LDAP configuration for the cluster

PATCH /security/authentication/cluster/ldap

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' field. 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

Learn more

- [DOC /security/authentication/cluster/ldap](#)

Request Body

Name	Type	Description
_links	_links	
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_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
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
port	integer	The port used to connect to the LDAP Servers.

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
use_start_tls	boolean	<p>Specifies whether or not to use Start TLS over LDAP connections.</p>

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "bind_password": "string",
  "min_bind_level": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string"
}
```

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

Error Code	Description
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 the Distinguished Names and bind password are correct
4915258	The LDAP configuration is invalid. 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 LIFs

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	

cluster_ldap

Name	Type	Description
_links	_links	
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_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
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

Name	Type	Description
port	integer	The port used to connect to the LDAP Servers.
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]	
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
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
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`

A cluster can have only one LDAP configuration. IPv6 must be enabled if IPv6 family addresses are specified. The following parameters are optional:

- schema
- port
- min_bind_level
- bind_password
- base_scope
- use_start_tls
- session_security 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 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.

Learn more

- [DOC /security/authentication/cluster/ldap](#)

Request Body

Name	Type	Description
<code>_links</code>	_links	
<code>base_dn</code>	string	Specifies the default base DN for all searches.

Name	Type	Description
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_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
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
port	integer	The port used to connect to the LDAP Servers.
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
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.

Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "base_dn": "string",
  "base_scope": "string",
  "bind_dn": "string",
  "bind_password": "string",
  "min_bind_level": "string",
  "port": 389,
  "schema": "string",
  "servers": [
    "string"
  ],
  "session_security": "string"
}
```

Response

Status: 201, Created

Name	Type	Description
_links	_links	
num_records	integer	Number of LDAP records.

Name	Type	Description
records	array[ldap_service]	

Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "ad_domain": "string",
      "base_dn": "string",
      "base_scope": "string",
      "bind_dn": "string",
      "bind_password": "string",
      "min_bind_level": "string",
      "port": 389,
      "preferred_ad_servers": [
        "string"
      ],
      "schema": "string",
      "servers": [
        "string"
      ],
      "session_security": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      }
    }
  ]
}
```

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
23724130	Cannot use an IPv6 name server address because there are no IPv6 LIFs

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	

cluster_ldap

Name	Type	Description
_links	_links	
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_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
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

Name	Type	Description
port	integer	The port used to connect to the LDAP Servers.
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]	
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
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.

_links

Name	Type	Description
next	href	
self	href	

svm

Name	Type	Description
<u>_links</u>	_links	
name	string	The name of the SVM.

Name	Type	Description
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_dn	string	Specifies the user that binds to the LDAP servers.
bind_password	string	Specifies the bind password for the LDAP servers.
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

Name	Type	Description
port	integer	The port used to connect to the LDAP Servers.
preferred_ad_servers	array[string]	
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
svm	svm	
use_start_tls	boolean	Specifies whether or not to use Start TLS over LDAP connections.

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.