EMC® ScaleIO®

Version 2.0.x

User Roles and LDAP Usage Technical Notes

302-002-667

REV 06

EMC²

Copyright © 2016-2017 Dell Inc. or its subsidiaries All rights reserved.

Published March 2017

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

Figures 5

Preface 7

Chapter 1 Overview 9

Chapter 2 User Roles 11
Overview of user roles 12
Local domain roles 12
LDAP domain roles 13
LDAP login requirements 14
Local versus LDAP users 14
Superuser 15
Resetting the Administrator 16

Chapter 3 Command Authorization 17
Administrator 18
Configurator 18
Backend Configurator 18
Frontend Configurator 21
Monitor 21
Technician 23
Security 23
CLI commands that do not require specific roles 23

Chapter 4 Preparation examples for various operating systems 25
Settings on the LDAPS server 26
Linux 26
Pre-configuration preparations 26
Installation and configuration 28
SLES 29
Pre-configuration preparation 29
Installation and Configuration 30
Ubuntu 31
Pre-configuration preparation 31
Installation and configuration 37
Windows 37
Pre-configuration preparation 38
Installation and configuration 48
Preparation for non-secured LDAP 49

Chapter 5 Configuring LDAP Authentication on the ScaleIO MDM 51
Preparing for LDAP authentication 52
Configuring LDAP in the ScaleIO system 52
CLI basics 52
Add the Service 53

Group Assignment..... 55
Query properties.....57
Authentication Method.....58
Logging in to the System.....59
Using LDAP with ScaleIO..... 59
Example of LDAP use with ScaleIO.....59
Cross domain authentication..... 60

Chapter 6 Configuring LDAP Authentication on the ScaleIO Gateway 63
Preliminary configurations 64
Configuring the ScaleIO gateway..... 64
Editing the gateway.properties file..... 66

Chapter 7 LDAP facts 69
AD configuration propagation..... 70
Changing Group to Role Association.....70

FIGURES

1 Local domain nested roles model....13
2 LDAP domain segregated roles model....14

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Related documentation

The release notes for your version includes the latest information for your product.

The following EMC publication sets provide information about your ScaleIO or ScaleIO Ready Node product:

- ScaleIO software (downloadable as ScaleIO Software <version> Documentation set)
- ScaleIO Ready Node with AMS (downloadable as ScaleIO Ready Node with AMS Documentation set)
- ScaleIO Ready Node no AMS (downloadable as ScaleIO Ready Node no AMS Documentation set)
- VxRack Node 100 Series (downloadable as VxRack Node 100 Series Documentation set)

You can download the release notes, the document sets, and other related documentation from EMC Online Support.

Typographical conventions

EMC uses the following type style conventions in this document:

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values

|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. You will see several options for contacting EMC Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to techpubcomments@emc.com.

CHAPTER 1

Overview

This document is a high-level description of the user roles and LDAP feature as implemented in ScaleIO v2.0.0.x and higher, and ScaleIO Ready Node v2.0.1 and higher.

Where features are relevant only for a specific system type, this is noted throughout the document. It is assumed that readers of this document are familiar with LDAP technology in general.

CHAPTER 2

User Roles

This chapter explains the user roles in ScaleIO. Topics include:

- Overview of user roles 12
- Local domain roles 12
- LDAP domain roles 13
- Local versus LDAP users 14
- Superuser 15

Overview of user roles

ScaleIO supports different types of user roles.

These user roles are:

- Monitor
- Frontend Configurator
- Backend Configurator
- Configurator (an aggregation of both Frontend and Backend Configurator
- Administrator
- Security
- Superuser

Each role is associated with different commands (see Command Authorization on page 17). The authorization of each role according to the set of commands that it may invoke is defined differently, depending on whether local or LDAP authentication is used.

Local domain roles

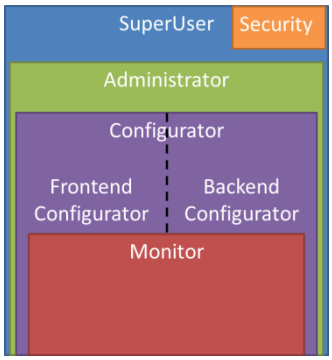
The roles in local domain, apart from Security, are defined in a nested manner:

1. Monitor: May only perform monitoring operations that do not affect the system.
2. Frontend Configurator: May perform Monitor operations and frontend-related configurations that include volume manipulations (adding, deleting, mapping, and snapshots) and SDC operations (adding, deleting, and mapping). For example, in the GUI, Frontend Configurator correlates with the **Frontend** view.
3. Backend Configurator: May performs Monitor operations and backend-related configurations. For example, in the GUI, Backend Configurator correlates with the **Backend** view. Operations include:
   - Protection Domain and Storage Pool operations
   - Manipulating Fault Sets and SDS
   - Mapping SDS devices, and
   - Others
4. Configurator: Does not exist as a default option, but can be configured from the Frontend and Backend Configurators.
5. Administrator: May perform all Configurator operations and also define the Configurator- and Monitor-level users.
6. Security: May define administrators and control LDAP.
7. Superuser: May perform all operations and configuration tasks. There can only be one Superuser, and it is always a local user.

Note

The Backend Configurator role must be assigned to the users who need to update the system license.

Figure 1 Local domain nested roles model



This maintains the same usage manner as was defined prior to adding LDAP. Each role is authorized commands related to its definition, in addition to the commands permitted by lower-level roles. The Security role is the only role that is separated.

LDAP domain roles

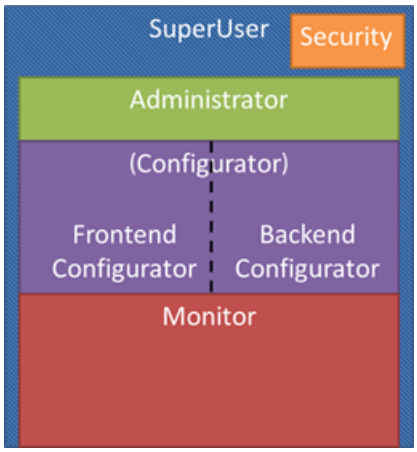
The roles in LDAP domain are similar by name to the local user roles, but are defined in a more mutually exclusive manner:

1. Monitor: May only perform monitoring operations that do not affect the system.
2. Frontend Configurator: May perform any frontend-related configurations that include volume manipulations (adding, deleting, mapping, and snapshots) and SDC operations (adding, deleting, and mapping). For example, in the GUI it correlates with the Frontend view's operations.
3. Backend Configurator: May perform any backend-related configurations. For example, in the GUI, Backend Configurator correlates with the Backend view's operations. Operations include:
   - Protection Domain and Storage Pool operations
   - Manipulating Fault Sets and SDS
   - Mapping SDS devices, and
   - Others
4. Administrator: May define Configurator and Monitor users.
5. Security: May define administrators and control LDAP.
6. Superuser: CANNOT be an LDAP user.

Note

The Backend Configurator role must be assigned to the users who need to update the system license.

Figure 2 LDAP domain segregated roles model



Here the roles are separated. Each role is authorized to a separate set of commands that are related to its functionality, with basically no overlap. The only "odd-man-out" is the Configurator, which is constructed from Frontend and Backend Configurator, and does not exist per se. This model allows better granularity when defining users.

LDAP login requirements

Logging in to these components using LDAP user roles requires the following:

Component	Requirements
CLI, REST	At least one LDAP service in the system (not necessarily the one you log in with) must be assigned to the Administrator group. CLI and REST command execution will be according to the user role and permissions. Any LDAP user can log in (CLI command execution is according to the user role and permissions).
GUI, Plugin, IM (IM and Plugin are not applicable for ScaleIO Ready Node)	Monitor role Additional roles can also be assigned in order to perform operations other than queries, but Monitor role is mandatory.
ESRS	Backend Configurator role When performing system registration for ESRS, the MDM remote syslog feature is enabled. Backend Configurator user role is required when accessing the MDM which will perform this operation.

Local versus LDAP users

The authorization permissions of each user role are defined differently for local authentication and for LDAP authentication. Although the role names are similar, the permissions granted to them are not.

User roles defined in the LDAP domain are mutually exclusive, with no overlap (apart from the Configurator role). If you want to give an LDAP user permission to perform

both monitoring and configuration roles, for example, assign that user to both Backend/Frontend Configurator and Monitor LDAP groups.

The Configurator and Super User roles do not exist at all for LDAP.

The following table describes the permissions that can be defined for local domain users and for LDAP domain users:

User role	Query		Configure parameters		Configure user credentials	
	Local	LDAP	Local	LDAP	Local	LDAP
Monitor	Yes	Yes	No	No	No	No
Configurator (this role is only applicable for local users)	Yes	N/A	Yes (an aggregation of both Frontend and Backend Configurator)	N/A	No	N/A
Backend Configurator	Yes	No	Yes Backend operations only (Protection Domains, Storage Pools, Fault Sets, SDSs, Devices, other system settings)		No	No
Frontend Configurator	Yes	No	Yes Frontend operations only (Volumes, SDCs, Snapshots)		No	No
Administrator	Yes	No	Yes	No	May configure Configurator and Monitor users	
Security Roles	No	No	No	No	May define Administrator users and control LDAP	
Superuser (only one Superuser is allowed per system, and it must be a local user)	Yes	N/A	Yes	N/A	Yes	N/A

Superuser

The Superuser is a new role that replaces the default administrator in the earlier versions. This is the default user for setting up the system. It has all the privileges of all the roles.

It is recommended that the Superuser role be used in the following cases:

- When setting up a new system.

- When there is no need to define separate or additional users.

Superuser comes with the default credentials of:

- Username: admin
- Password: admin

The Superuser is only available in the Local domain and cannot be an LDAP user. One may disable that user to ensure that all users are associated with a certain person. To disable the Superuser, run the following command:

```
scli --disable_admin [--i_am_sure]
```

Note

Having a single Superuser dictates that the audit log will not track a certain person per se.

To re-enable the Superuser, use the `reset_admin` command. See Resetting the Administrator on page 16.

Resetting the Administrator

In emergency cases, there may be a need to override the LDAP authentication and restore the Superuser. To do so, follow the Reset Administrator procedure described in your system's User Guide.

Once executed, the Superuser (admin) is available, and the authentication method becomes both LDAP and local authentication.

CHAPTER 3

Command Authorization

This chapter lists the different roles and the commands associated with them. Topics include:

- Administrator 18
- Configurator 18
- Monitor 21
- Technician 23
- Security 23
- CLI commands that do not require specific roles 23

Administrator

The commands associated with the Administrator role are:

- `add_user`
- `delete_user`
- `disable_admin`
- `login_on_behalf`
- `modify_user`
- `query_user`
- `query_users`
- `reset_password`
- `set_user_authentication_method`
- `set_cli_password_acceptance`

Configurator

The configurator is the aggregation of both the Backend Configurator and Frontend Configurator.

Backend Configurator

The commands associated with the Backend Configurator role are:

- `abort_remove_sds`
- `abort_remove_sds_device`
- `abort_upgrade`
- `activate_protection_domain`
- `activate_sds_dev`
- `add_protection_domain`
- `add_fault_set`
- `add_sds`
- `add_sds_device`
- `add_sds_ip`
- `add_sds_to_fault_set`
- `add_tie_breaker`
- `add_sds_rfcache_device`
- `add_secondary_mdm`
- `add_standby_mdm`
- `add_storage_pool`
- `allow_commands_during_upgrade`
- `clear_fault_set`

- clear_sds_device_error
- clear_rfcache_error
- disable_fault_set
- disable_con_matrix_bypass
- disable_data_integrity_scanner
- disable_sds_rfcache
- enable_fault_set
- enable_con_matrix_bypass
- enable_data_integrity_scanner
- enable_sds_rfcache
- enter_maintenance_mode
- exit_maintenance_mode
- finalize_upgrade
- force_complete_vtree_removal
- inactivate_protection_domain
- modify_sds_device_capacity
- modify_sds_ip_role
- modify_sds_port
- modify_management_ip
- modify_rebuild_migration_parallelism
- modify_spare_policy
- modify_zero_padding_policy
- purge_rmcache
- refresh_mdm_cluster_capabilities
- remove_protection_domain
- remove_fault_set
- remove_sds
- remove_sds_device
- remove_sds_from_fault_set
- remove_sds_ip
- remove_tie_breaker
- remove_sds_rfcache_device
- remove_secondary_mdm
- remove_standby_mdm
- remove_storage_pool
- rename_protection_domain
- rename_fault_set
- rename_sds
- rename_device

- rename_mdm
- rename_sds_rfcache_device
- rename_storage_pool
- rename_system
- replace_cluster_mdm
- reset_device_error_counters
- reset_diag_counters
- reset_oscillating_failure_counters
- set_cap_alrt_threshold
- set_checksum_mode
- set_sds_network_limits
- set_drl_properties
- set_guid_display_mode
- set_initial_license_type
- set_license
- set_manager_id
- set_oscillating_failure_counter_parameters
- set_performance_parameters
- set_rebalance_mode
- set_rebalance_throttle_policy
- set_rebuild_mode
- set_rebuild_throttle_policy
- set_rfcache_parameters
- set_rfcache_usage
- set_rmcache_enabled
- set_rmcache_frozen
- set_rmcache_size
- set_rmcache_write_handling_mode
- set_syslog_facility
- set_thick_volume_percent
- set_trace_component_freq
- set_trace_freq_map
- set_use_rmcache
- set_vol_use_rmcache
- start_sds_net_test
- start_device_test
- start_remote_syslog
- start_upgrade
- stop_remote_syslog

- switch_cluster_mode
- switch_mdm_ownership
- switch_to_cluster_mode
- switch_to_single_mode
- update_device_original_path
- update_sds_rfcache_device_original_path

Frontend Configurator

The commands associated with the Frontend Configurator role are:

- add_scsi_initiator
- add_sdc
- add_volume
- map_vol_to_scsi_initiator
- map_volume_to_sdc
- modify_sdc_volume_limit
- modify_volume_capacity
- remove_sdc
- remove_scsi_initiator
- remove_snap_group
- remove_volume
- rename_sdc
- rename_volume
- scsi_release_test
- scsi_reserve_test
- scsi_reset_test
- set_obfuscation_properties
- set_restricted_sdc_mode
- snapshot_revert
- snapshot_volume
- unmap_vol_from_scsi_initiator
- unmap_volume_from_sdc

Monitor

The commands associated with the Monitor role are:

- custom_event
- debug_action
- query_all
- query_all_approved_sdcs
- query_all_fault_sets

- query_all_sdcs
- query_all_sdss
- query_all_proto
- query_all_scsi_initiators
- query_all_vols
- query_all_volumes
- query_protection_domain
- query_protection_domain_network
- query_protection_domain_proto
- query_fault_set
- query_sdc
- query_sds
- query_sds_net_test
- query_deleted_volumes
- query_dev_latency_meters
- query_device_errors
- query_device_test_results
- query_diag_counters
- query_latency_meters
- query_license
- query_multiple_objects
- query_objects
- query_oscillating_network_counters
- query_poll
- query_properties
- query_remote_read_only_limit_state
- query_remote_syslog_counters
- query_restricted_sdc_mode
- query_sdc_vol_limit
- query_sds_failures
- query_single_object
- query_storage_pool_proto
- query_trace_freq_map
- query_vol_to_scsi_initiator
- query_volume
- query_volume_sdc_bwc
- query_volume_tree
- query_ldap

Technician

The following commands should only be used by an EMC-certified technician:

- `disable_secure_communication`
- `rescue_mode`
- `reset_admin`

Security

The commands associated with the Security role are:

- `add_ldap_service`
- `assign_ldap_group_to_roles`
- `generate_certificate`
- `generate_mdm_certificate`
- `generate_mdm_csr_file`
- `remove_ldap_group_from_role_assignment`
- `remove_ldap_service`
- `rename_ldap_service`
- `replace_mdm_security_files`
- `set_component_authentication_properties`
- `set_management_client_communication`

CLI commands that do not require specific roles

The commands that do not require any specific role are:

- `add_primary_mdm`
- `create_mdm_cluster`
- `Login`
- `Logout`
- `query_cluster`
- `query_cluster_mdm`
- `query_version`
- `set_password`

CHAPTER 4

Preparation examples for various operating systems

This chapter provides examples for preparing servers running various operating systems for use with the ScaleIO LDAP feature. These examples apply to a secured LDAPS environment.

Topics include:

- Settings on the LDAPS server 26
- Linux 26
- SLES 29
- Ubuntu 31
- Windows 37
- Preparation for non-secured LDAP 49

Settings on the LDAPS server

The examples in this chapter include the following assumptions:

Setting	Configuration
OS	Windows
IP address	192.168.1.1
User name	administrator
Password	password
Domain name	ldaps.local
FQDN	example.ldaps.local
Certificate name	scaleio.cer
Certificate location	C:\Cert

Note

For an explanation of how to adapt these examples to a non-secured LDAP environment, see Preparation for non-secured LDAP on page 49.

Linux

This section contains procedures for setting up the Linux operating system for use with LDAP.

Pre-configuration preparations

The following tasks are required in order to prepare a Linux server for use with the ScaleIO LDAP feature:

1. Verifying the installation of the openldap package on page 26
2. Creating a cacerts directory on page 27
3. Editing the /etc/resolv.conf file on page 27
4. Adding the LDAPS server details to the /etc/hosts file on page 27
5. Copying the Scaleio.cer file and running cacertdir_rehash on page 27

Verifying the installation of the openldap package

Verify that the package is installed:

```
rpm -qa | grep openldap
```

Output example:

```
openldap-2.4.23-32.el6_4.1.x86_64
```

Creating a cacerts directory

Create a `cacerts` directory in a predefined location.

Procedure

1. Create a directory named `cacerts` under the location: `/etc/openldap`.
2. Verify that the following entry appears in `/etc/openldap/ldap.conf`:

```
TLS_CACERTDIR /etc/openldap/cacerts
```

Editing the /etc/resolv.conf file

Edit the `/etc/resolv.conf` file, and verify that:

- The LDAP server IP address is the first address (or the only one)
- The search parameter is configured to `ldaps://example.ldaps.local`:
  - `cat /etc/resolv.conf`
  - `nameserver 192.168.1.1`
  - `nameserver 8.8.8.8`
  - `nameserver 9.9.9.9`
  - `search ldaps.local`

Adding the LDAPS server details to the /etc/hosts file

Add the LDAPS server IP address, IFQDN, and hostname to the `/etc/hosts` file:

```
127.0.0.1 localhost
127.0.1.1 SioVM_226
192.168.10.45     SioGwHA

# The following lines are desirable for IPv6 capable hosts:
:1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


192.168.10.226 SioVM_226
192.168.10.227 SioVM_227
192.168.10.228 SioVM_228
192.168.10.229 SioVM_229
192.168.1.1   example.ldaps.local  example
```

Copying the Scaleio.cer file and running cacertdir_rehash

Copy the `Scaleio.cer` file and run `cacertdir_rehash`:

Procedure

1. Copy the `scaleio.cer` file to `/etc/openldap/cacerts`, using winscp.
2. Run the command: `cacertdir_rehash /etc/openldap/cacerts`

Installation and configuration

After preparing the server for LDAP, install the MDM package and configure LDAP authentication:

1. Installing the MDM package or ScaleIO system on page 28
2. Configuring LDAP authentication on page 28

Installing the MDM package or ScaleIO system

Install the MDM package, or the entire ScaleIO system.

For details, refer to the *ScaleIO Deployment Guide*.

Configuring LDAP authentication

Run the following scli command to configure the LDAP authentication.

For example, to configure the sio_1 user:

```
scli --add_ldap_service --ldap_service_uri "ldaps://
example.ldaps.local" --ldap_base_dn "OU=OU1,DC=ldaps,DC=local"
scli --assign_ldap_groups_to_roles --ldap_service_id
<LDAP_SERVICE_ID_FROM_PREVIOUS_COMMAND> --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"
scli --set_user_authentication_method --
native_and_ldap_authentication
scli --login --username sio_1@ldaps.local --password password --
ldap_authentication
```

Note

In the command `scli --add_ldap_service`, the optional parameter `--ldap_service name` may also be used. The output would be:

```
[root@rhel-sio ~]# scli --add_ldap_service --ldap_service_uri
"ldaps://example.ldaps.local" --ldap_base_dn
"OU=OU1,DC=ldaps,DC=local"

Successfully added a LDAP service.  Object ID d39003a500000000 with
URI: ldaps://example.ldaps.local and base DN:
OU=OU1,DC=ldaps,DC=local
[root@rhel-sio ~]# scli --assign_ldap_groups_to_roles --
ldap_service_id d39003a500000000 --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"

Assignment of roles to LDAP groups completed successfully
[root@rhel-sio ~]# scli --set_user_authentication_method --
native_and_ldap_authentication

Authentication method changed successfully
[root@rhel-sio ~]# scli --login --username sio_1@ldaps.local --
password password --ldap_authentication

Logged in. User role is Administrator. System ID is 5a5e09fb146eafcb
[root@rhel-sio ~]#
```

If there are problems, verify that the LDAP configuration is correct:

```
[root@rhel-sio ~]# scli --query_user_authentication_properties
------------------------------------------------------------
System has 1 configured LDAP services
------------------------------------------------------------
LDAP service ID: d39003a500000000
LDAP service URI: ldaps://example.ldaps.local
Users base DN: ou=ou1,dc=ldaps,dc=local
LDAP service has 1 configured groups.
        Role: Administrator
        Group DN: CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local
------------------------------------------------------------
```

SLES

This section contains procedures for setting up the SLES operating system for use with LDAP.

Pre-configuration preparation

The following tasks are required in order to prepare a SLES server for use with the ScaleIO LDAP feature:

1. Verifying the installation of the openldap package on page 29
2. Creating a cacerts directory on page 29
3. Editing the /etc/resolv.conf file on page 30
4. Adding the LDAPS server details to the /etc/hosts file on page 30
5. Copying the Scaleio.cer file on page 30

Verifying the installation of the openldap package

Verify that the `openldap` package is installed.

```
rpm -qa | grep openldap
```

Output example:

`openldap-2.4.23-32.el6_4.1.x86_64`

Creating a cacerts directory

Create the `cacerts` directory:

Procedure

1. Create a directory called `cacerts` under this location: `/etc/openldap`
2. Verify that the following entries are displayed in `/etc/openldap/ldap.conf`:

   `TLS_CACERTDIR /etc/openldap/cacerts`

   `TLS_REQCERT allow`

Editing the /etc/resolv.conf file

Edit the `/etc/resolv.conf` file, and verify that:

- The LDAPS server IP address is the first, or only, IP address.
- The search parameter is configured to `ldaps://example.ldaps.local`:
  - `cat /etc/resolv.conf`
  - `nameserver 192.168.1.1`
  - `nameserver 8.8.8.8`
  - `nameserver 9.9.9.9`
  - `search ldaps.local`

Adding the LDAPS server details to the /etc/hosts file

Add the LDAPS server IP address, IFQDN, and hostname to the file `/etc/hosts`:

```
127.0.0.1 localhost
127.0.1.1 SioVM_226
192.168.10.45     SioGwHA

# The following lines are desirable for IPv6 capable hosts:
:1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


192.168.10.226 SioVM_226
192.168.10.227 SioVM_227
192.168.10.228 SioVM_228
192.168.10.229 SioVM_229
192.168.1.1   example.ldaps.local  example
```

Copying the Scaleio.cer file

Copy the `scaleio.cer` file to `/etc/openldap/cacerts` using winscp.

Installation and Configuration

After preparing the server for LDAP, install the MDM package and configure LDAP authentication:

1. Installing the MDM package or ScaleIO system on page 30
2. Configuring LDAP Authentication on page 30

Installing the MDM package or ScaleIO system

Install the MDM package, or the entire ScaleIO system.

For details, refer to the *ScaleIO Deployment Guide*.

Configuring LDAP Authentication

Run the following scli command to configure the LDAP authentication:

For example, cto configure the sio_1 user:

```
scli --add_ldap_service --ldap_service_uri "ldaps://
example.ldaps.local" --ldap_base_dn "OU=OU1,DC=ldaps,DC=local"
```

```
scli --assign_ldap_groups_to_roles --ldap_service_id
<LDAP_SERVICE_ID_FROM_PREVIOUS_COMMAND> --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"

scli --set_user_authentication_method --
native_and_ldap_authentication

scli --login --username sio_1@ldaps.local --password --password  --
ldap_authentication
```

The output would be:

```
[root@rhel-sio ~]# scli --add_ldap_service --ldap_service_uri
"ldaps://example.ldaps.local" --ldap_base_dn
"OU=OU1,DC=ldaps,DC=local"

Successfully added a LDAP service.  Object ID d39003a500000000 with
URI: ldaps://example.ldaps.local and base DN: OU=OU1,DC=ldaps,DC=local
[root@rhel-sio ~]# scli --assign_ldap_groups_to_roles --
ldap_service_id d39003a500000000 --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"

Assignment of roles to LDAP groups completed successfully
[root@rhel-sio ~]# scli --set_user_authentication_method --
native_and_ldap_authentication

Authentication method changed successfully
[root@rhel-sio ~]# scli --login --username sio_1@ldaps.local --
password password --ldap_authentication

Logged in. User role is Administrator. System ID is 5a5e09fb146eafcb
[root@rhel-sio ~]#
```

If there are problems, verify that the LDAP configuration is correct as follows:

```
[root@rhel-sio ~]# scli --query_authentication_parameters
------------------------------------------------------------
System has 1 configured LDAP services
------------------------------------------------------------
LDAP service ID: d39003a500000000
LDAP service URI: ldaps://example.ldaps.local
Users base DN: ou=ou1,dc=ldaps,dc=local
LDAP service has 1 configured groups.
        Role: Administrator
        Group DN: CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local
------------------------------------------------------------
```

Ubuntu

This section contains procedures for setting up the Ubuntu operating system for use with LDAP.

Pre-configuration preparation

Configuring secured LDAP nodes on the server

Configure secured LDAP nodes in the ScaleIO server.

Procedure

1. Add the DNS parameters to your network interface in `/etc/network/interfaces`.

   Ensure that you enter it under eth0 or any other route-able interface.

   For example:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo

iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.1
    netmask 255.255.240.0
    gateway 192.168.1.2
    dns-nameservers 8.8.8.8
    dns-nameservers 9.9.9.9
    dns-search ldaps.local

# IPv4 configuration
auto eth1
iface eth1 inet static
    address 7.1.1.226
    netmask 255.255.0.0

# IPv6 configuration
auto eth1
iface eth1 inet6 static
    pre-up modprobe ipv6
    address 260:0:170:790D:250:56FF:FE89:C21F
    netmask 64
```

   In this example, the address 9.9.9.9 is for external IP communications; it is needed for the APT repository.

   Ensure that you can ping 8.8.8.8 and 9.9.9.9.

2. Reboot the server.
3. Verify that the `file /etc/resolv.conf` is updated:

```
#     Dynamic resolv.conf(5) file for glibc resolver(3)
generated by resolvconf(8)

#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE
OVERWRITTEN

nameserver 8.8.8.8

nameserver 9.9.9.9

nameserver 10.10.10.10

search ldaps.local
```

4. Run `nslookup` for the LDAPS server hostname and IP address:

```
root@SioVM_228:~# nslookup example
Server:         192.168.1.1
Address:        192.168.1.1#53

Name:     example.ldaps.local
Address:  192.168.1.1

root@SioVM_228:~# nslookup 192.168.1.1
Server:         192.168.1.1
Address:        192.168.1.1#53

1.1.168.192.in-addr.arpa      name =   example.ldaps.local.

root@SioVM_228:~#
```

5. Run the following command, and wait until the operation is finished:

```
sudo apt-get update
```

6. Run the command:

```
sudo apt-get install openssh-client ldap-utils
```

7. Copy the `scaleio.cer` file from the LDAPS server (see its location above) to `/etc/ssl/certs`.
8. Run the following command and wait until the operation is finished:

```
sudo update-ca-certificates
```

9. Add the following lines to the file `/etc/ldap/ldap.conf` and ensure that all the other lines are commented out:

   `URI ldaps://example.ldaps.local/`

   `TLS_REQCERT allow`

   The file contents should be similar to the following example:

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE    dc=example,dc=com
#URI    ldap://ldap.example.com ldap://ldap-master.example.com:
666

#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

# TLS certificates (needed for GnuTLS)
# TLS_CACERT    /etc/ssl/certs/ca-certificates.crt
URI ldaps://example.ldaps.local/
TLS_REQCERT allow
```

10. Add the LDAPS server IP address, IFQDN, and hostname to the `/etc/hosts` file:

```
127.0.0.1 localhost
127.0.1.1 SioVM_226
192.168.10.45     SioGwHA

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


192.168.10.226 SioVM_226
192.168.10.227 SioVM_227
192.168.10.228 SioVM_228
192.168.10.229 SioVM_229
192.168.1.1   example.ldaps.local  example
```

11. Test the configuration:

    a. Test the validation of the certificate:

```
sudo openssl s_client -connect example.ldaps.local:636 -
CAfile /etc/ssl/certs/scaleio.cer < /dev/null
```

Output similar to the following appears:

```
sudo openssl s_client -connect example.ldaps.local:636 -
CAfile /etc/ssl/certs/scaleio.cer  < /dev/null
```

The output should be similar to the following example. Note the last line of the output, before "Done".

```
CONNECTED(00000003)
depth=1 DC = local, DC = ldaps, CN = ldaps-example-CA
verify return:1
depth=0 CN = example.ldaps.local
verify return:1
---
Certificate chain
0 s:/CN=example.ldaps.local
   i:/DC=local/DC=ldaps/CN=ldaps-example-CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIF/TCCBOWgAwIBAgITQQAAAAI/
hs4TiVKP4QAAAAAAAjANBgkqhkiG9w0BAQUF
ADBMMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgoJkiaJk/
IsZAEZFgVsZGFw
czEcMBoGA1UEAxMTbGRhcHMtV0lOMTJSMi1EQy1DQTAeFw0xNTA5MDMxNDU4ND
Ja
Fw0xNjA5MDIxNDU4NDJaMCExHzAdBgNVBAMTFldJTjEyUjItREMubGRhcHMubG
9j
YWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDPy34+oVF3p
+z0oC1M
UwWNlyVK78Vs7CsyR5PbwSCEMtjeqW7ND3SFu8siOzywqAs4IA72V388oXh9yl
YM
/MyMdAzgQL4wCwrlnOnWGwrz4gv/sQySmnImmsvBT99E/
xmBjxHUsLyIGa8We8n5
WNhXRaA92tg4aLpOyLOTqMAw+3DlAKwQVefcpu/
OjejyDmuSGa6D42a3E8Im1FA+
```

```
bdmHxZ9grFivcLTdtZ9yrvLV6ge6YXY9R6k5fkcbdoaHywDny2ENgE5zrNgIIX
l7
UHNS2BrWgc0ugNP5txSTRihdhlPBmfjgMCZYRSYleSgIbjrBRrWienPLBdrRUQ
+l
PLpVAgMBAAGjggMBMIIC/
TAvBgkrBgEEAYI3FAIEIh4gAEQAbwBtAGEAaQBuAEMA
bwBuAHQAcgBvAGwAbABlAHIwHQYDVR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBw
MB
MA4GA1UdDwEB/
wQEAwIFoDB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMCAgIA
gDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMAsGCWCGSAFlAwQBLTALBg
lg
hkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0GA1
Ud
DgQWBBTNLBBtk/Ux123+H2zNAY3CQ8a7/zAfBgNVHSMEGDAWgBSJ/
n2QndapHgyp
bFEsIn4/99ERyDCB1AYDVR0fBIHMMIHJMIHGoIHDoIHAhoG9bGRhcDovLy9DTj
1s
ZGFwcy1XSU4xMlIyLURDLUNBLENOPVdJTjEyUjItREMsQ049Q0RQLENOPVB1Ym
xp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb2
4s
REM9bGRhcHMsREM9bG9jYWw/
Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNl
P29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHFBggrBgEFBQcBAQ
SB
uDCBtTCBsgYIKwYBBQUHMAKGgaVsZGFwOi8vL0NOPWxkYXBzLVdJTjEyUjItRE
Mt
Q0EsQ049QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2
Vz
LENOPUNvbmZpZ3VyYXRpb24sREM9bGRhcHMsREM9bG9jYWw/
Y0FDZXJ0aWZpY2F0
ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkwQgYDVR
0R
BDswOaAfBgkrBgEEAYI3GQGgEgQQtfI1dFzIYEGq4QF04AUb94IWV0lOMTJSMi
1E
Qy5sZGFwcy5sb2NhbDANBgkqhkiG9w0BAQUFAAOCAQEAB7TMLHh3GMDjBCSX4k
q6
QTec5safeUMGCCf1fyaUcehCDRpAtbNapre/ShHAfIxNYss3jtsPZhDBXo4v
+bKG
Oc0BVJCN+hNn5gdXsUDIQajA/DO6VkQL
+0ceqa3BwyYy2GGFqwehhKJh6nt8k4tA
lP67BmydoE/OYr3fSxZJaKOPrsgrNG9OeSvDLYRTaUpbZHQdnUxCBaHU
+43lYpmp
vox1zPJ9hfWfcby3Ox/0UnWWnEQammpNSorppCQVGtS80Xaiz6c2/QW3c06i/
cKY
6YS6r40twXcozxZNqwJfMf+JoBJ/S4JH3M6ALzn0nclgl5eQ
+r0DhMtC2fqP8g53
tA==
-----END CERTIFICATE-----
subject=/CN=example.ldaps.local
issuer=/DC=local/DC=ldaps/CN=ldaps-example-CA
---
No client certificate CA names sent

SSL handshake has read 2107 bytes and written 489 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-SHA384
    Session-ID:
000E0000A293DA7B903083F8BCB2737F2C10A98D298BD0E963B73E9EBAA493
0C
    Session-ID-ctx:
```

```
    Master-Key:
2242522F8B151725BDED1DC92264F461F4487DAAEC8DB6F5EA4959A42D4DAB
D4105534110229870FC8B6333B4443E891
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1455035763
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
DONE
```

b. Test the connectivity to the LDAPS server:

```
sudo  ldapsearch -v -x -H ldaps://example.ldaps.local -D
"CN=sio_1,OU=OU1,DC=ldaps,DC=local" -b "DC=ldaps,DC=local" -
w password -s sub "cn=sio_1"
```

Output similar to the following appears:

```
ldap_initialize( ldaps://example.ldaps.local:636/??base )
filter: cn=sio_1
requesting: All userApplication attributes
# extended LDIF
#
# LDAPv3
# base <DC=ldaps,DC=local> with scope subtree
# filter: cn=sio_1
# requesting: ALL
#

# sio_1, OU1, ldaps.local
dn: CN=sio_1,OU=OU1,DC=ldaps,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson

objectClass: user
cn: sio_1
distinguishedName: CN=sio_1,OU=OU1,DC=ldaps,DC=local
instanceType: 4
whenCreated: 20150903151639.0Z
whenChanged: 20160204120821.0Z
uSNCreated: 16441
memberOf: CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local
uSNChanged: 42047
name: sio_1
objectGUID:: nZsX4yqFIEaR3qKEKSyZcw==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 130932822411399444
lastLogoff: 0
lastLogon: 130932822593743040
pwdLastSet: 130990597572374527
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAA9hRku46/nHL6xBLIUAQAAA==
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: sio_1
sAMAccountType: 805306368
lockoutTime: 0
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=ldaps,DC=local
dSCorePropagationData: 16010101000000.0Z
```

```
lastLogonTimestamp: 130990613014592452

# search reference
ref: ldaps://ForestDnsZones.ldaps.local/
DC=ForestDnsZones,DC=ldaps,DC=local

# search reference
ref: ldaps://DomainDnsZones.ldaps.local/
DC=DomainDnsZones,DC=ldaps,DC=local

# search reference
ref: ldaps://ldaps.local/CN=Configuration,DC=ldaps,DC=local

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3
```

Installation and configuration

After preparing the server for LDAP, install the MDM package and configure LDAP authentication:

1. Installing the MDM package or ScaleIO system on page 37
2. Configuring LDAP authentication on page 37

Installing the MDM package or ScaleIO system

Install the MDM package, or the ScaleIO system.

For details, see the *ScaleIO Deployment Guide*.

Configuring LDAP authentication

Run the following scli command to configure the LDAP authentication:

For example, to configure the sio_1 user:

```
scli --add_ldap_service --ldap_service_uri "ldaps://
example.ldaps.local" --ldap_base_dn "OU=OU1,DC=ldaps,DC=local"

scli --assign_ldap_groups_to_roles --ldap_service_id
<LDAP_SERVICE_ID_FROM_PREVIOUS_COMMAND> --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"

scli --set_user_authentication_method --
native_and_ldap_authentication

scli --login --username sio_1@ldaps.local --password --password  --
ldap_authentication
```

Windows

This section contains procedures for setting up the Windows operating system for use with LDAP.

Pre-configuration preparation

The following tasks are required in order to prepare a Windows server for use with the ScaleIO LDAP feature:

1. Verifying the accessibility of the LDAPS server on page 38
2. Running the ldp.exe utility on page 42
3. Importing the CA certificate in Windows Server 2012 or Windows 7 on page 43
4. Importing the CA certificate in Windows 2008 on page 45
5. Testing secured LDAP node connectivity with ldp.exe on page 47

Verifying the accessibility of the LDAPS server

Verify that you have access to the LDAPS server in the ScaleIO system.

Procedure

1. Verify that the LDAPS server is accessible by its IP address and Hostname.

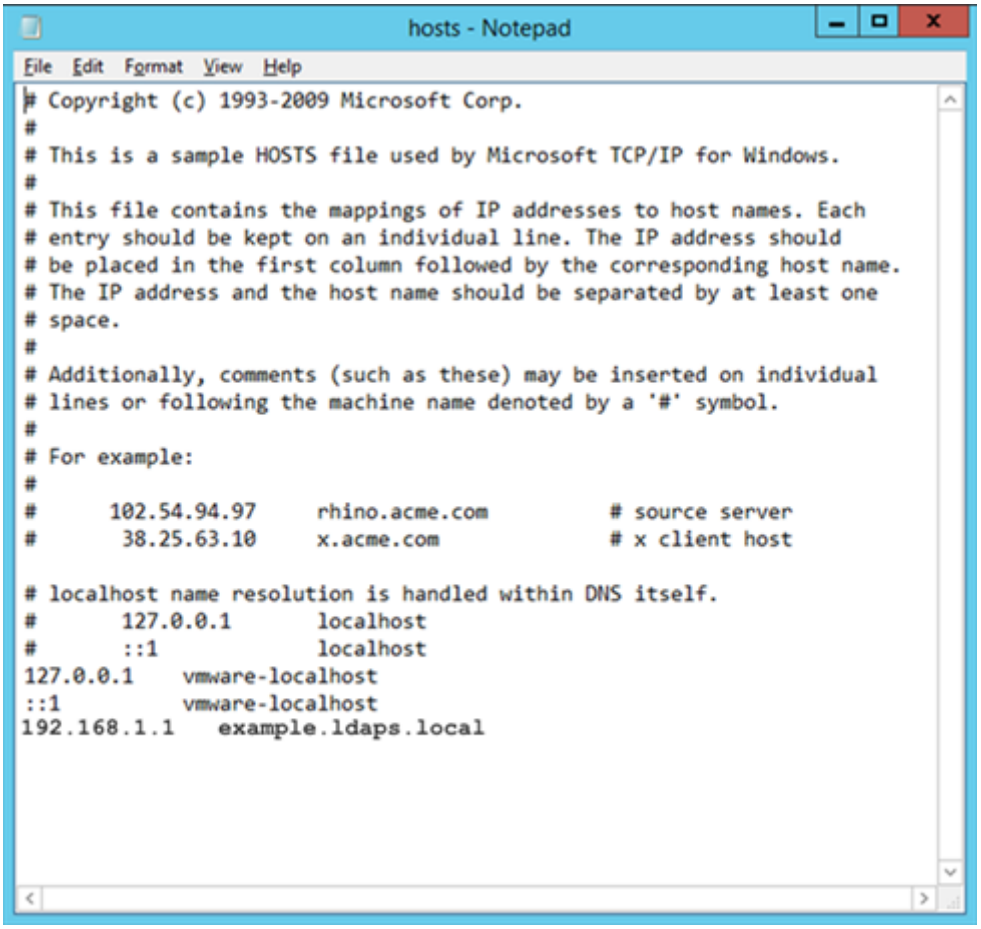
   It is recommended that you edit the hosts file located under `C:\Windows\System32\drivers\etc` and add the following entries:

   ```
   <IP address> <hostname>
   ```

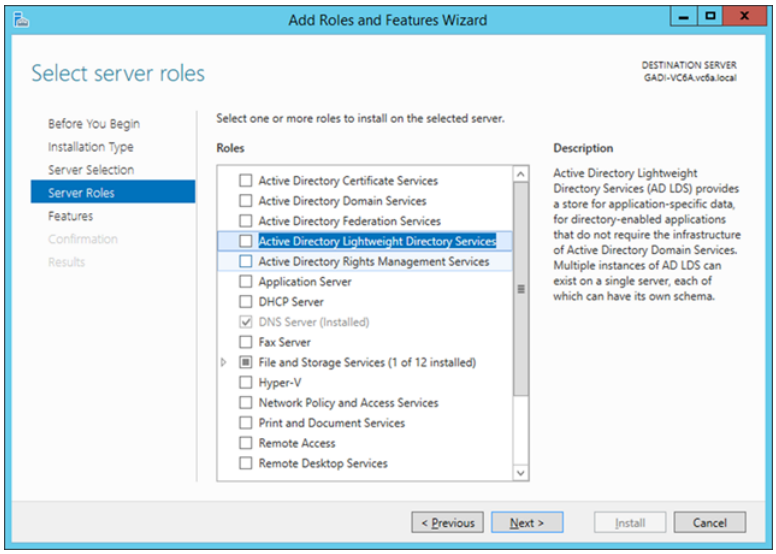
   Example:

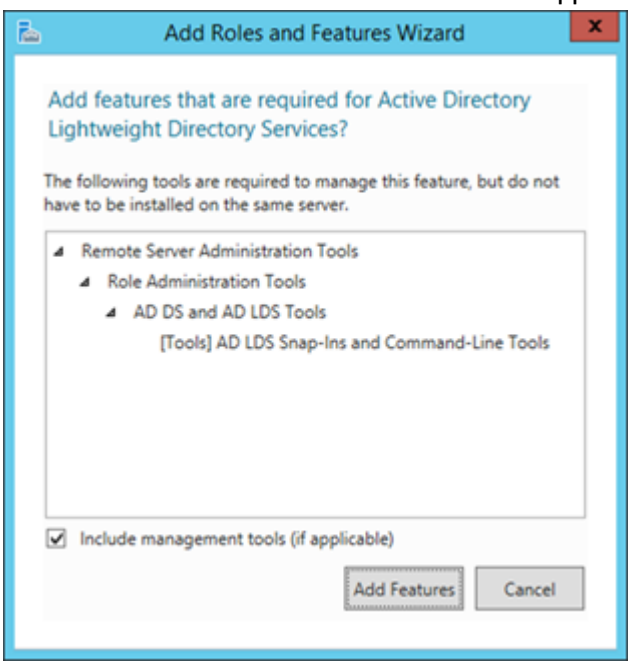
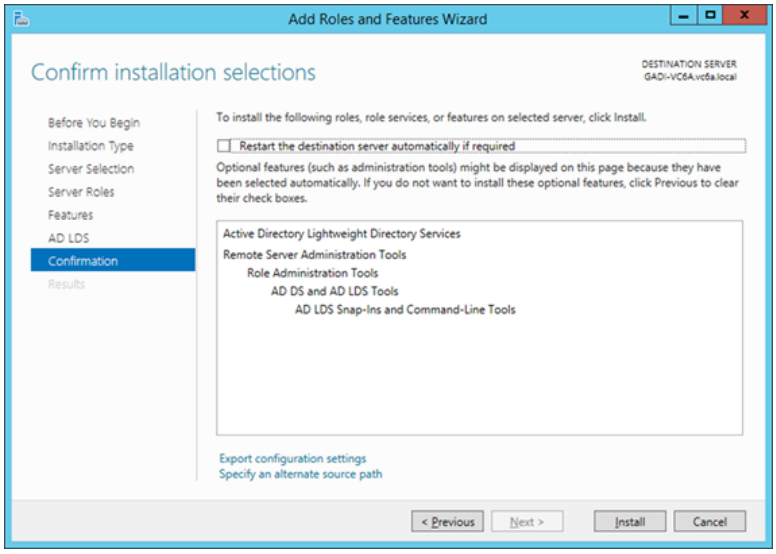
   ```
   192.168.1.1 example.ldaps.local
   ```

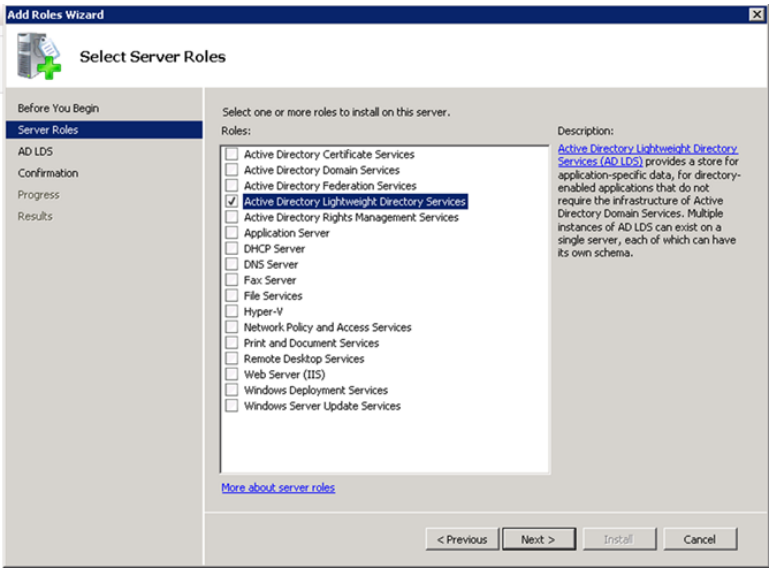
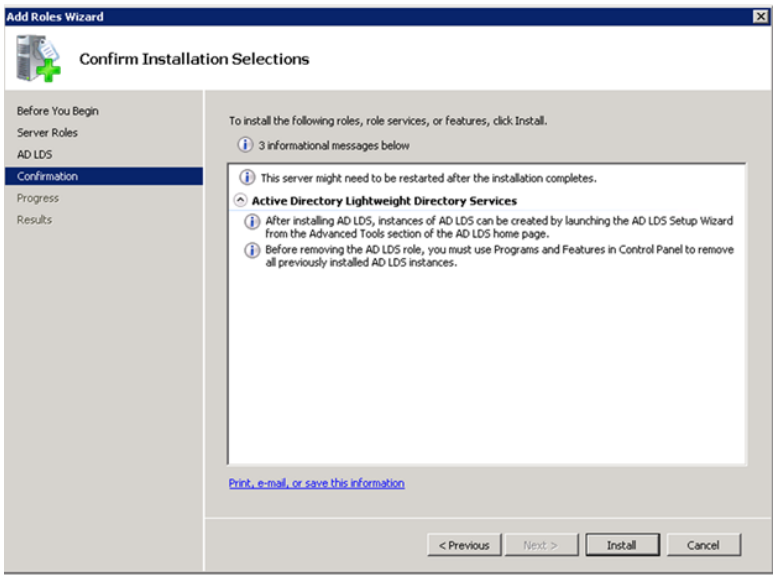
   The file looks similar to the following:

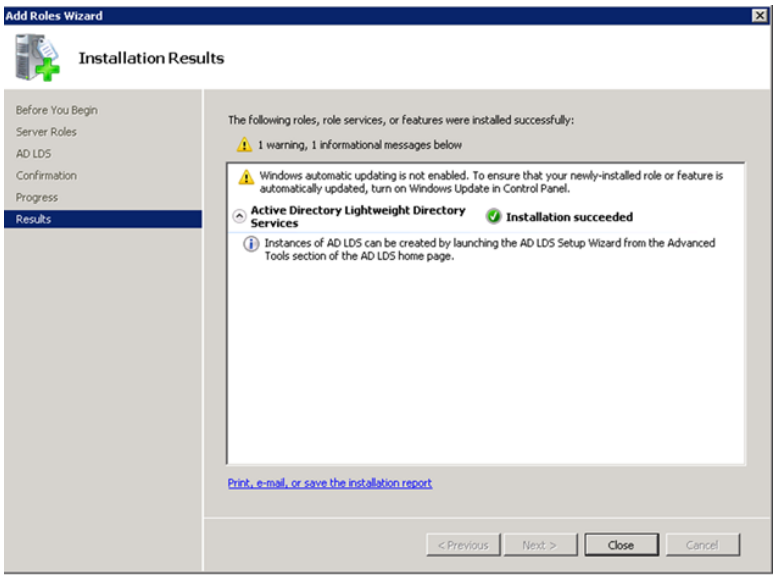


2. Depending on your version of Windows, verify that the `ldp.exe` command is present. If it is not present, perform one of the following procedures:

Windows version	Steps
Windows 2012R2	a. Select **Server Manager** > **Manage** > **Add Roles and Features Wizard**, and click **Next** three times until you see this window: 

Windows version	Steps
	b. Select the **Active Directory Lightweight Directory Services** check box. **Note** When you choose to install the Active Directory Lightweight Directory Services, it automatically selects and installs the .NET 3.5 Framework, unless it is already installed. The **Add Roles and Features Wizard** window appears:  c. Click **Add Features**, and then click **Next** three times, until the **Add Roles and Features Wizard** window appears:  d. Click **Install**.

Windows version	Steps
	e. When the installation is finished, click **Close**.
Windows 2008R2	a. Select **Server Manager** > **Roles** > **Add Roles** and click **Next**. The **Select Server Roles** window appears:  b. Select the **Active Directory Lightweight Directory Services** check box, and then click **Next** twice. **Note** When you choose to install the Active Directory Lightweight Directory Services, it automatically selects and installs the .NET 3.5 Framework, unless it is already installed. The **Confirm Installation Selections** window appears:  c. Click **Install**.

Windows version	Steps
	When the installation is finished, the **Installation Results** window appears:  d. Click **Close**.
Windows 7	Install `ldp.exe` on a client on which Windows 7 is installed: a. In any Internet browser, go to https://www.microsoft.com/en-IE/download/details.aspx?id=7887. b. Download the Remote Server Administration Tools for Windows® 7 with SP1. c. Install the package. The `ldp.exe` utility is now available on your system.

Running the ldp.exe utility

Run the Windows `ldp.exe` utility.

Procedure

1. Open a command line window.
2. At the command line enter:

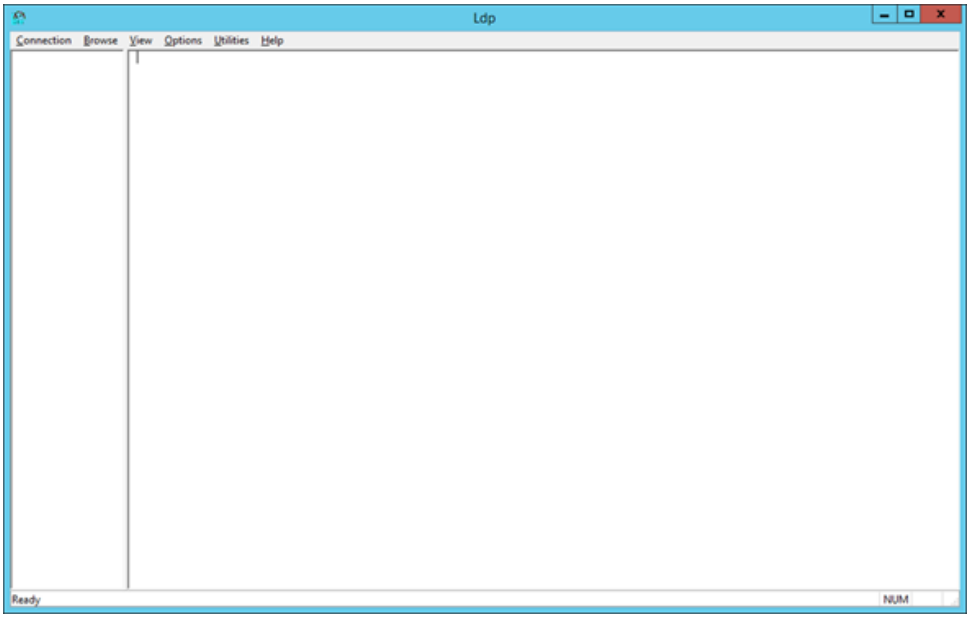
```
ldp
```

Note

In Windows Server 2012, launch the **Start** menu and enter `ldp` in the **Search** field.

3. Click `ldp.exe`.

   The **Ldp** window appears:



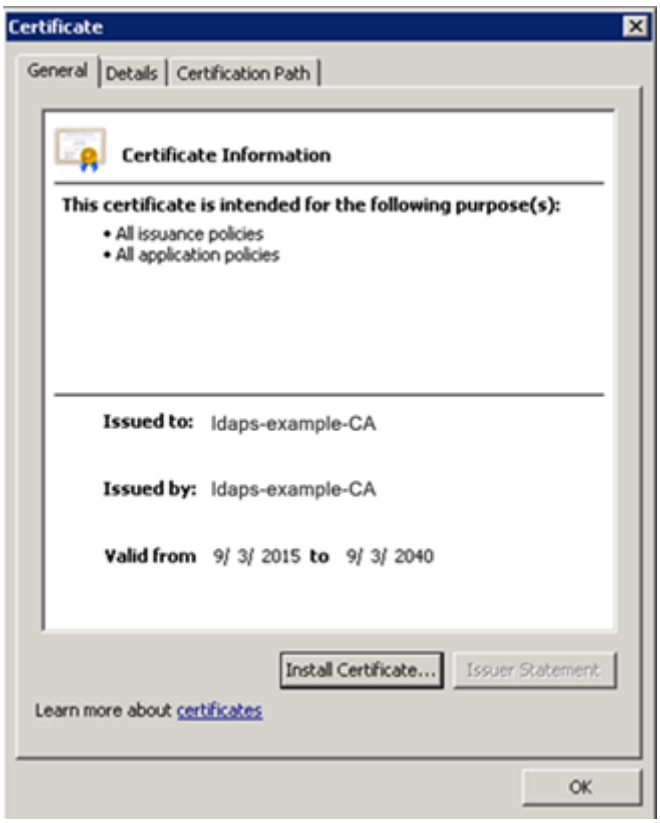
Importing the CA certificate in Windows Server 2012 or Windows 7

Import the CA certificate into the local certificate store.

Procedure

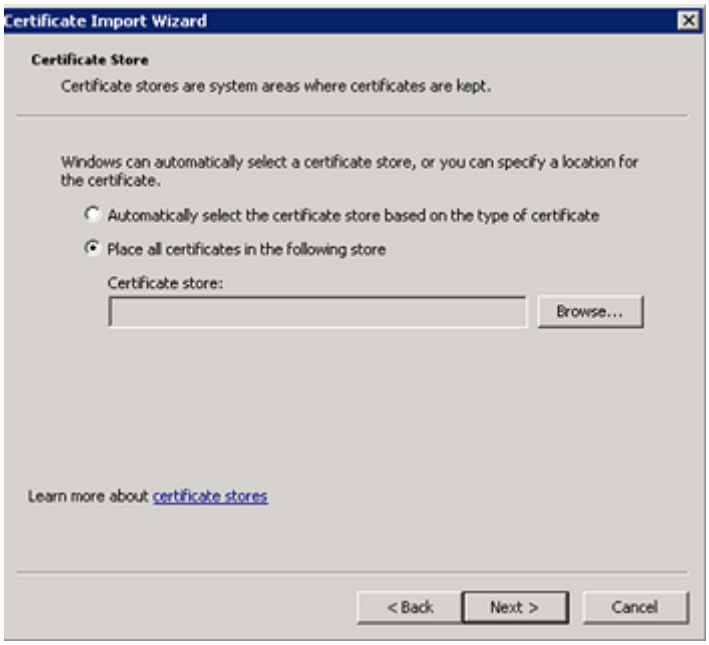
1. Copy the `scaleio.cer` file from the LDAP server to any location on your server.
2. Double-click the certificate.

   The **Certificate** window appears:



3. Click **Install Certificate**, and then **Next**.

   The **Certificate Import Wizard** window appears:



Note

On Windows 2012R2, after you click **Install Certificate**, an additional message box appears. In this case, select **Local Machine**.

4. Select **Place all certificates in the following store**, and then click **Browse**.

   The **Select Certificate Store** window appears:

5. Select **Trusted Root Certification Authorities**, and then click **OK**.
6. Click **Next**.
7. Click **Finish**.

   A confirmation message appears:

8. Click **OK**.

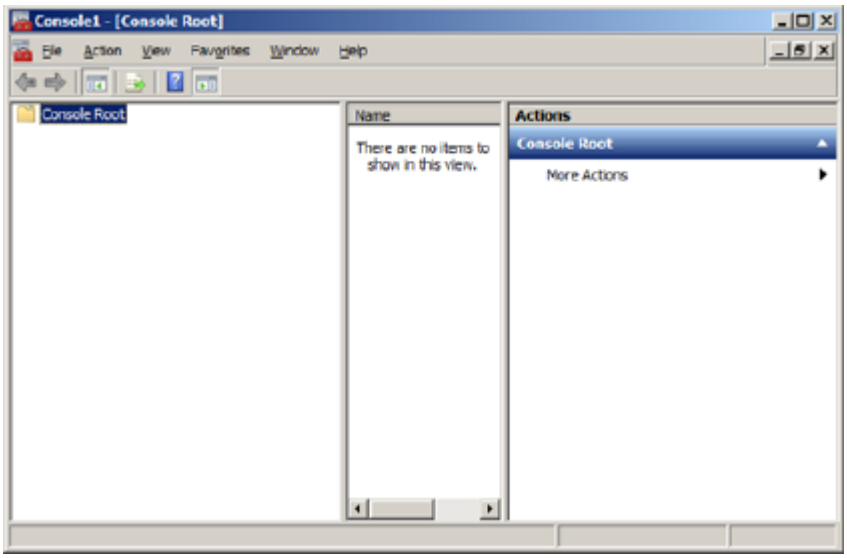
Importing the CA certificate in Windows 2008

Import the CA certificate into the local certificate store.

Procedure

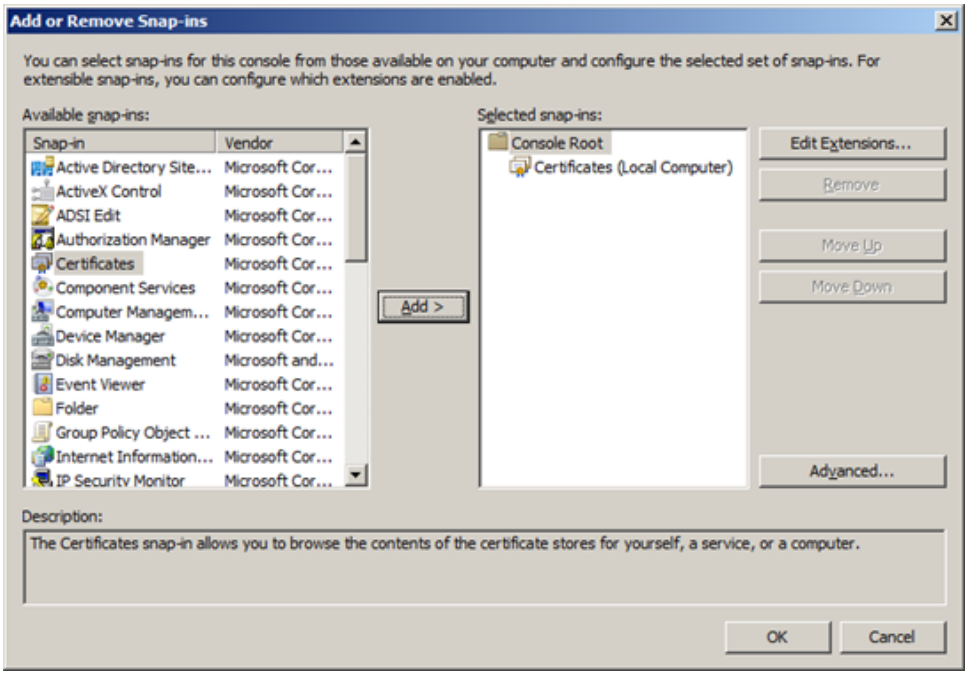
1. From the command line, run `mmc.exe`.

   The **Console1** window appears:



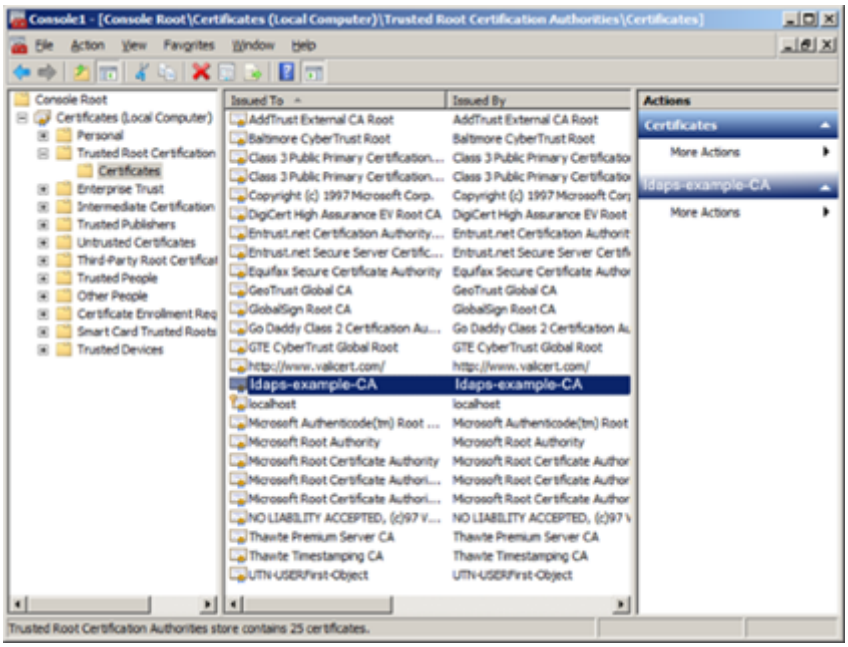
2. From the **File** menu, select **Add/Remove Snap-in**.
3. In the left pane, select **Certificate**, and then click **Add**.
4. Select the computer account, then click **Next** and **Finish**.

   The **Add or Remove Snap-ins** window appears:


Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Site...
Microsoft Cor...
ActiveX Control
Microsoft Cor...
ADSI Edit
Microsoft Cor...
Authorization Manager
Microsoft Cor...
Certificates
Microsoft Cor...
Component Services
Microsoft Cor...
Computer Managem...
Microsoft Cor...
Device Manager
Microsoft Cor...
Disk Management
Microsoft and...
Event Viewer
Microsoft Cor...
Folder
Microsoft Cor...
Group Policy Object ...
Microsoft Cor...
Internet Information...
Microsoft Cor...
IP Security Monitor
Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Certificates (Local Computer)
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel

5. Click **OK**.
6. In the left pane of the MMC window, expand **Certificate (Local Computer)** and then expand **Trusted Root Certification Authorities**.
7. Select **Certificate**.

   The **Console 1 [Console Root\Certificate...]** screen appears:



8. Verify that the LDAP certificate (for example, example@-DC-CA) appears in the right pane of the window.
9. If the LDAP certificate is not displayed, right-click **Certificate** and select **All Tacks** > **Import...**.
10. Click **Next**.
11. Click **Browse** and select the certificate file of the LDAP server.
12. Click **Next** twice, and then click **Finish**, followed by **OK**.

    The LDAP certificate appears in the right pane.

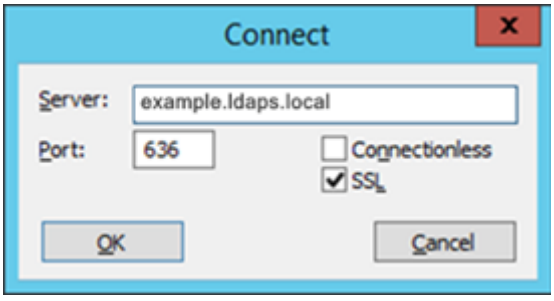
Testing secured LDAP node connectivity with ldp.exe

Test and verify secured LDAP node connectivity using the `ldp.exe` utility.

Procedure

1. Run `ldp.exe`.
2. From the **Connection** menu, select **Connect**.

   The **Connect** window appears:



3. Enter the required information:
   a. In the **Server** field., enter the LDAPS server FQDN.

      For example: example.ldaps.local

   b. Select the **SSL** option.

   c. In the **Port** field, change the port number to 636.
4. Click **OK**.

   The following information should appear in the `ldp.exe` utility window:

Note

If an error message appears, review the configuration.

Installation and configuration

After preparing the server for LDAP, install the MDM package and configure LDAP authentication:

1. Installing the MDM package or ScaleIO system on page 48
2. Configuring LDAP Authentication on page 48

Installing the MDM package or ScaleIO system

Install the MDM package, or the entire ScaleIO system.

For details, see the *ScaleIO Deployment Guide*.

Configuring LDAP Authentication

Run the following scli command to configure the LDAP authentication:

For example, to configure the sio_1 user:

```
scli --add_ldap_service --ldap_service_uri "ldaps://
example.ldaps.local" --ldap_base_dn "OU=OU1,DC=ldaps,DC=local"

scli --assign_ldap_groups_to_roles --ldap_service_id
<LDAP_SERVICE_ID_FROM_PREVIOUS_COMMAND> --administrator_role_dn
"CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local"
```

```
scli --set_user_authentication_method --
native_and_ldap_authentication

scli --login --username sio_1@ldaps.local --password --password  --
ldap_authentication
```

Preparation for non-secured LDAP

To prepare a non-secured LDAP environment, follow the procedures for LDAPS (secured), with the following exceptions:

Procedure

1. These pre-configuration procedures are unnecessary:
   - Creating a `cacerts`directory.
     For example, for Linux, skip the procedures “Creating a directory called “cacerts”.
   - Editing the `/etc/resolv.conf` file
     For example, for Linux, skip the procedures “Editing the /etc/resolv.conf file”.
   - Running the `cacertdir_rehash` script:
     For example, for Linux, skip the corresponding step in the procedures “Copying the Scaleio.cer file and running cacertdir_rehash”.
2. When configuring LDAP authentication, replace *ldaps://example.ldaps.local* with *ldap://server.example.com* (or replace it with an IP address).

CHAPTER 5

Configuring LDAP Authentication on the ScaleIO MDM

This chapter contains instructions for configuring LDAP authentication on the ScaleIO MDM. Topics include:

- Preparing for LDAP authentication 52
- Configuring LDAP in the ScaleIO system 52
- Using LDAP with ScaleIO 59

Preparing for LDAP authentication

Before configuring LDAP authentication on the ScaleIO MDM, ensure that you have prepared both the LDAPS server and the server on which the MDM is to be installed.

For instructions, see Preparation examples for various operating systems on page 25.

For information on adapting preparations for a non-secured LDAP environment, see Preparation for non-secured LDAP on page 49.

For details about the ScaleIO CLI commands, refer to *EMC ScaleIO CLI Reference Guide*.

Configuring LDAP in the ScaleIO system

The following topics explain how to configure LDAP for your system using the ScaleIO CLI:

- CLI basics on page 52
- Add the Service on page 53
- Group Assignment on page 55
- Query properties on page 57
- Query properties on page 57
- Logging in to the System on page 59

CLI basics

The ScaleIO CLI and SCLI commands enable you to perform all provision, maintain, and monitor tasks.

The CLI is installed as part of the MDM component and can be found in the following path:

- Linux and VMware: `scli`
- Windows: `C:\Program Files\emc\scaleio\MDM\bin`
- Xen: `siocli`

All CLI commands use the following format:

- Linux, VMware, and Windows:

```
scli [--mdm_ip <IP>] <command>
```

- Xen:

```
siocli [--mdm_ip <IP>] <command>
```

For more information, see *EMC ScaleIO CLI Reference Guide*.

Add the Service

Add the service to the MDM to be used for authentication. In return, the user receives the ID of the LDAP service.

Command

```
scli --add_ldap_service
```

Syntax

```
scli --add_ldap_service --ldap_service_uri <URI> --ldap_base_dn
<LDAP_DN>
[--ldap_service_name<LDAP_NAME>][--object_class_attribute <ATTR>]
[--user_id_attribute_name <NAME>] [--member_of_attribute_name
<NAME>]
[--disable_recursive_search]
```

The actual command syntax is operating-system dependent. For more information, see CLI basics on page 52.

Description/Notes

This command adds an LDAP service to the system. The service ID of the added LDAP will be returned.

Note

LDAP should be configured on all the MDMs in the system in order to support switch ownership scenarios.

Parameters

Parameter	Description
--ldap_service_uri	Where <LDAP_SCHEMA> defines the connection protocol: LDAPS - secure LDAP connection (recommended) LDAP - non-secure LDAP connection <PORT_NUMBER> - the LDAP service port (optional parameter; default is 636) This parameter must start with ldap:// or ldaps:// followed by the host name. No extra validation is performed at this stage. Example: LDAPS://my.ldaphost.com:636
--ldap_base_dn	Base Distinguished Name (DN) of users in the domain, and must be a valid DN containing the DC substring. For example, if a user corporate login is johnd@sxample.ldaps.local, the DC string would be DC=example, DC=ldaps, DC=local.

Parameter	Description
	Note On Active Directory Windows servers, you can use the dsquery tool to find LDAP Base DN information. To see available options, in the command line, type `dsquery /?`. On Linux, you can use `ldapsearch` from the command line (may need to be installed, if it is missing).
--ldap_service_name	LDAP service name
--object_class_attribute	The object class attribute that is used to identify a user; used in the search filter (default: user)
--user_id_attribute_name	The attribute name that defines the user id; used in the search filter (default: sAMAccountName)
--member_of_attribute_name	The attribute name that defines the contained group; used in the search filter (default: memberOf)
--disable_recursive_search	Disable recursive search

Example

```
scli --add_ldap_service --ldap_service_uri "ldap://
example.ldaps.local"
--ldap_base_dn "OU=SIO_OU_1,DC=ldaps,DC=local"
```

Where:

- `ldap://example.ldaps.local` is the host name of the authentication server.
- `OU=SIO_OU_1` is a specific organizational unit group defined in the Active Directory.
- `DC=ldaps, DC=local` are the Domain Component parts of the Base DN.

Additional commands

Related commands exist for renaming the LDAP service, and for removing it.

Rename the LDAP service

Command

```
scli --rename_ldap_service
```

Syntax

```
scli --rename_ldap_service (--ldap_service_id <LDAP_SERVICE_ID> | --
ldap_service_name <LDAP_SERVICE_NAME>) --new_name <NAME>
```

Description

This command renames the LDAP service in the ScaleIO system.

Parameters

Parameter	Description
--ldap_service_id	ID of LDAP service
--ldap_service_name	Name of LDAP service
--new_name <NAME>	New name to be assigned to the LDAP service

Example

```
scli --rename_ldap_service --ldap_service_id 0f33116700000000 --
new_name ldap_service1
```

The LDAP service name was changed successfully.

Remove the LDAP service

Command

```
scli --remove_ldap_service
```

Syntax

```
scli --remove_ldap_service (--ldap_service_id <LDAP_SERVICE_ID> | --
ldap_service_name <LDAP_SERVICE_NAME> | --remove_all )
```

Description
This command removes the LDAP service from the ScaleIO system.

Parameters

Parameter	Description
--ldap_service_id	ID of LDAP service
--ldap_service_name	Name of LDAP service
--remove_all	Remove all LDAP services

Example

```
scli --remove_ldap_service --ldap_service_id 0f33116700000000
```

The LDAP service was deleted successfully.

Group Assignment

Once the LDAP service is ready, the next step is to associate the Active Directory (AD) groups with the different roles offered by ScaleIO.

As described in User Roles on page 11, a segregation model is used for the roles in LDAP. This associates a set of commands with each role. Unlike the nested model, in which a more privileged role immediately grants access to the same set of authorized

commands to a less privileged role, in the case of LDAP one must add each role to grant access to the set of commands.

For example, in the local domain, when a user is defined as Administrator, that user may execute any command associated with the lesser privileged roles (Configurator and Monitor). So, an Administrator may add users due to the Administrator role, and in addition, may also perform configuration changes as the Configurator roles.

In LDAP, this is not the case. If a user is associated with a group that is mapped to the ScaleIO Administrator role, that user may perform user-related commands, but will not be allowed to make any configuration changes.

Note

All LDAP groups must be assigned the Monitor role if they want those LDAP users to be able to use the GUI/plug-in.

Associate an Active Directory group with a ScaleIO role

Command

```
scli --assign_ldap_groups_to_roles
```

Syntax

```
scli --assign_ldap_groups_to_roles (--ldap_service_id | --
ldap_service_name) [--administrator_role_dn] [--security_role_dn]
[--backend_config_role_dn] [--frontend_config_role_dn] [--
monitor_role_dn] [--allow_overwrite]
```

Description/Notes

This command maps LDAP groups to ScaleIO system roles. The LDAP service must be configured in advance. Once you have mapped the roles, you can assign users in the Active Directory to the relevant LDAP groups.

All LDAP groups must be assigned the Monitor role if they want those LDAP users to be able to use the GUI/plug-in.

Parameters

Parameter	Description
--ldap_service_id	ID of LDAP service
--ldap_service_name	Name of LDAP service
--administrator_role_dn	LDAP group that has users with administration privileges
--security_role_dn	LDAP group that has users with security privileges
--backend_config_role_dn	LDAP group that has users with backend configuration privileges
--frontend_config_role_dn	LDAP group that has users with frontend configuration privileges
--monitor_role_dn	LDAP group that has users with monitoring privileges
--allow_overwrite	Overwrites the role's LDAP group

Example

See Example of cross domain authentication on page 60.

Remove a group from a role assignment

Command

```
remove_ldap_group_from_role_assignment
```

Syntax

```
scli --remove_ldap_group_from_role_assignment (--ldap_service_id
<LDAP_SERVICE_ID> | --ldap_service_name <LDAP_SERVICE_NAME>) [--
administrator_role] [--security_role] [--backend_config_role] [--
frontend_config_role] [--monitor_role]
```

Description/Notes

This command removes LDAP groups from system role assignments.

Parameters

Parameter	Description
--ldap_service_id	ID of LDAP service. The service must already be configured.
--ldap_service_name	Name of LDAP service
--administrator_role	LDAP group that has users with administration privileges
--security_role	LDAP group that has users with security privileges
--backend_config_role	LDAP group that has users with backend configuration privileges
--frontend_config_role	LDAP group that has users with frontend configuration privileges
--monitor_role	LDAP group that has users with monitoring privileges

Example

```
scli --remove_ldap_group_from_role_assignment --ldap_service_id
0f33387700000000 --administrator_role
```

Assignment of roles to LDAP groups has been successfully removed.

Query properties

The query command allows you to view the properties defined for the LDAP services and groups.

Command

```
scli --query_user_authentication_properties
```

Example

See the example in Example of cross domain authentication on page 60.

Authentication Method

Once the LDAP service is set, and groups are assigned, specify the authentication method with which ScaleIO will authenticate the users. The users may be restricted to only the local domain or the LDAP server only, or both types may be allowed. This decision should be made at the discretion of the system administrator, and is usually dictated by the security policy of the organization.

Command

```
set_user_authentication_method
```

The command accepts one of these options:

- *ldap_authentication*
- *native_authentication*
- *native_and_ldap_authentication*

Once the authentication method is set, it cannot be changed easily. To change it, one must use the Reset Administrator procedure (see Resetting the Administrator on page 16).

Syntax

```
scli --set_user_authentication_method (--ldap_authentication | --
native_authentication | --native_and_ldap_authentication) [--
i_am_sure]
```

Description/Notes

This command sets the user authentication method for the system. Use this command with caution, because it is complex to roll back this operation.

Parameters

Parameter	Description
--ldap_authentication	LDAP based authentication method, where users are managed in LDAP compliant server. In order to switch to this authentication method, LDAP service parameters should be configured.
--native_authentication	Native authentication method, where users are managed locally in the system.
--native_and_ldap_authentication	A hybrid authentication method. Both LDAP and Native users may log into the system after it is set.
--i_am_sure	Preemptive approval.

Example

See the example in Example of cross domain authentication on page 60.

Logging in to the System

Once the system parameters are set, you may log in to the system according to the defined method.

Command

```
scli --login
```

When logging in locally, the command must include a user name and password. When using LDAP, the command should also include the LDAP domain it is using, and the LDAP authentication parameter, as in the following examples:

Example: local login, native authentication

```
scli --log in --username JohnDoe --password <password>
```

Example: LDAP login

```
scli --login --username JohnDoe@example.ldaps.local --password
<password>   ldap_authentication
```

Using LDAP with ScaleIO

LDAP users function differently than local users in ScaleIO.

When a local user is associated with a role, that user immediately inherits the capabilities of less privileged roles. For example, a local user with Administrator privileges will also be able to execute Configurator commands.

For an LDAP user, this is not the case. An LDAP user defined as an Administrator is limited to Administrator operations, such as adding users (see Command Authorization on page 17), but is not able to invoke any Configurator commands. You can overcome this limitation one of two ways:

- Assign an LDAP group to several ScaleIO roles.
- Assign an LDAP group to each ScaleIO role.

The following examples in Example of LDAP use with ScaleIO on page 59 show how to use each method.

Note

This section refers to LDAP configuration of the ScaleIO MDM. To configure LDAP on the ScaleIO Gateway, see Configuring LDAP Authentication on the ScaleIO Gateway on page 63.

Example of LDAP use with ScaleIO

This example shows how to configure LDAP so that the user John.Doe will be a Frontend Configurator as well as Monitor of the system.

Local Domain

Assign John.Doe (a local user) to the Frontend_Config role.

Because Monitor is nested in Frontend Configurator, John.Doe has all the desired privileges.

LDAP domain—LDAP group to multiple ScaleIO roles

Create and associate LDAP groups with multiple ScaleIO roles. You can do this for all roles by creating parallel groups in LDAP.

1. In LDAP, create the following LDAP group:
   - Frontend_Configurator_LDAP_Group
2. Assign John.Doe@example.ldaps.local to the above LDAP group.
3. In ScaleIO, associate Frontend_Configurator_LDAP_Group to both the Frontend_Config role and the Monitor role. In this way, Frontend_Configurator_LDAP_Group has the same privileges as the local Frontend Configurator role, and therefore will have the desired privileges.

LDAP domain—LDAP group to one ScaleIO role

Associate each LDAP group to one ScaleIO role:

1. In LDAP, create these LDAP groups:
   - Frontend_Configurator_LDAP_Group
   - Monitor_LDAP_Group
2. Assign John.Doe@ example.ldaps.local (an LDAP user) to both LDAP groups.
3. In ScaleIO, associate Frontend_Configurator_LDAP_Group to the Frontend_Config role, and assign Monitor_LDAP_Group to the Monitor role.

John.Doe@example.ldaps.local will have all the desired privileges.

Cross domain authentication

When there are two (or more) LDAP servers with a trusted relationship, a user from one server (user_ldap_server) can be associated with a group (scaleio_group) that is configured in the second server (group_ldap_server). The group in the second server is associated with a role in the ScaleIO system.

For ScaleIO to allow this user to log in, perform the following steps:

Procedure

1. Add the user_ldap_server as an LDAP service in ScaleIO.
2. Assign the scaleio_group (that belongs to the group_ldap_server) to ScaleIO, and associate it with the desired role.

Results

From now on, any user from the user_ldap_server can log in to the ScaleIO system with the role associated with scaleio_group that belongs to group_ldap_server.

Example of cross domain authentication

This example demonstrates the configuration activities that are performed in a ScaleIO system.

The example assumes that a user is a defined user in user_ldap. In addition, there is a group called scaleio_monitor_group defined in group_ldap.
The following steps show how to enable access to the ScaleIO systems for users in the user_ldap server (e.g., John Doe) who are part of the scaleio_monitor_group defined in group_ldap.

Procedure

1. Add user_ldap as an LDAP service:

```
[root~]$ scli --add_ldap_service --ldap_service_name
example_ldap --ldap_service_uri ldap://user_ldap.example.com
--ldap_base_dn "CN=Users,DC=user_ldap,DC=example,DC=com"
```

   Output similar to the following should appear. At the prompt, enter 'y':

```
LDAP uri defined with unsecured protocol. Press 'y' and then
Enter to confirm.y
Successfully added an LDAP service. Object ID 0b83f1c400000000
with Name: example_ldap, URI: ldap:// user_ldap.example.com and
base DN: CN=Users,DC=user_ldap,DC=example,DC=com
```

2. Assign the scaleio_monitor_group group to the Monitor role:

```
[root~]$ scli --assign_ldap_groups_to_roles --
ldap_service_name example_ldap --monitor_role_dn
"CN=scaleio_monitor_group,OU=scaleio_ou,DC=group_ldap,DC=examp
le,DC=com"
```

   The following output should appear:

```
Assignment of roles to LDAP groups completed successfully
```

3. Check the settings:

```
[root~]$ scli --query_user_authentication_properties
```

   Output similar to the following should appear:

```
------------------------------------------------------------
System has 1 configured LDAP services
------------------------------------------------------------
LDAP service ID: 0b83f1c400000000
LDAP service name: example_ldap
LDAP service URI: ldap://user_ldap.example.com
Users base DN: cn=users,dc=user_ldap,dc=example,dc=com
LDAP service has 1 configured groups.
           Role: Monitor
Group DN:
CN=scaleio_monitor_group,OU=scaleio_ou,DC=group_ldap,DC=example,
DC=com
------------------------------------------------------------
```

4. Set the authentication method:

```
[root~]$ scli --set_user_authentication_method --
ldap_authentication
```

   The following output should appear:

```
Authentication method changed successfully
```

5. Log in using the desired user name:

```
[root~]$ scli --login  --username John.Doe@ldap.example.com --
ldap_authentication
```

Output similar to the following should appear:

```
Enter password:
Logged in. User role is Monitor. System ID is 31bf07056dd2f5d7
```

CHAPTER 6

Configuring LDAP Authentication on the ScaleIO Gateway

This chapter explains how to configure LDAP authentication on the ScaleIO Gateway. Topics include:

Note

This chapter is not applicable to ScaleIO Ready Node systems.

- Preliminary configurations 64
- Configuring the ScaleIO gateway 64
- Editing the gateway.properties file 66

Preliminary configurations

Before configuring LDAP authentication on the ScaleIO Gateway, you are required to perform the following tasks:

- Verify that the `openldap` package is installed.
- Create a directory called cacerts.
- Edit the `/etc/resolv.conf` file.
- Add the LDAPS server IP address, IFWDN, and hostname to the `/etc/hosts` file.
- Copy the `Scaleio.cer` file and run `cacertdir_rehash`.

Note

For more information on these procedures, see the procedures in Preparation examples for various operating systems on page 25 for the specific operating system on which the ScaleIO Gateway is installed.

- Use SioGWTool in command line to add the LDAP configuration to the LockBox. The LockBox can be created beforehand, but you can also create a default LockBox when you run the command to add the LDAP configuration. SioGWTool is located at:
  - Linux:

    ```
    /opt/emc/scaleio/gateway/bin/SioGWTool.sh
    ```

  - Windows:

    ```
    C:\Program Files\EMC\ScaleIO\Gateway\bin\SioGWTool.bat
    ```

By default, login can be performed locally (with username admin) or via the LDAP server. It is also possible to configure the Gateway so that authentication can only be performed via the LDAP server.

Configuring the ScaleIO gateway

Configure the gateway in a ScaleIO system.

Procedure

1. Configure LDAP/LDAPS connectivity, as described in Configuring LDAP Authentication on the ScaleIO MDM on page 51.
2. For authentication via LDAP server only (local logging in will be disabled), using a text editor, edit the `gatewayUser.properties` file. (For detailed instructions, follow this procedure.)

   Change the property

   `gateway-admin.disable.local.login=false`

   to

   `gateway-admin.disable.local.login= true.`

3. Add the LDAP parameters to the Gateway:

```
SioGWTool --set_ldap_properties --server_url <URL_address> --
base_dn <base_DN> --group_name <group_name> --
create_default_lockbox
```

Note

If the default lockbox already exists, omit the `--create_default_lockbox` option.

For example:

- On Linux:

```
SioGWTool.sh --set_ldap_properties --server_url ldaps://
example.ldaps.local --base_dn "DC=ldaps,DC=local" --
group_name "CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local" --
create_default_lockbox
```

- On Windows:

```
SioGWTool.bat --set_ldap_properties --server_url ldaps://
example.ldaps.local --base_dn "DC=ldaps,DC=local" --
group_name "CN=SIO_GRP_1,OU=OU1,DC=ldaps,DC=local" --
create_default_lockbox
```

4. For a secured connection with the LDAPS server, add the LDAPS server's Trusted/Root certificate to the Gateway's `truststore.jks` file, using the following Java Keytool command, and then restart the Gateway:

```
keytool -import -trustcacerts -alias [unique_alias] -file
[path_to_the_certificate_file] -keystore
[path_to_certificates_folder]/truststore.jks
```

Note

If you add `--storepass changeit` to the command, confirmation using user credentials will not be required. For example:

```
./keytool -import -trustcacerts -alias test -file "/tmp/scaleio.cer"
--keystore "/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/
certificates/truststore.jks" --storepass changeit
```

In RHEL 6, the keytool location is: `/usr/java/jre1.8.0_40/bin`. For more information about using Keytool, default paths and typical commands, see "Using Keytool to add certificates to external components" in the *ScaleIO User Guide*.

5. To verify that the certificate was imported successfully, run the following command, and make sure that the LDAPS server's Trusted/Root certificate was imported into the Gateway's `truststore.jks` file:

```
keytool -list -v -keystore [path_to_certificates_folder]/
truststore.jks -alias [unique_alias] -storepass changeit
```

For example:

```
keytool -list -v -keystore "/opt/emc/scaleio/gateway/webapps/
ROOT/WEB-INF/classes/certificates/truststore.jks" -alias test
-storepass changeit
```

The Gateway's truststore is at the following location:

- Linux:

```
/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes/
certificates/truststore.jks
```

- Windows:

```
C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF
\classes\certificates\truststore.jks
```

Editing the gateway.properties file

Edit the `gateway.properties` file.

Procedure

1. Using a text editor, open the `gatewayUser.properties` file that is located in the following directory on the Installation Manager/Gateway server:

Gateway installed on	Location of gatewayUser.properties file
Linux	`/opt/emc/scaleio/gateway/webapps/ROOT/WEB-INF/classes`
Windows	`C:\Program Files\EMC\ScaleIO\Gateway\webapps\ROOT\WEB-INF\classes\`

2. Edit the file as required.
3. Save and close the file.
4. Restart the scaleio-gateway service:
   - Linux:
     Type the command `service scaleio-gateway restart`
   - Windows:
     Restart the EMC ScaleIO Gateway service.

5. When the configuration is complete, you may log in to the Gateway using LDAP user credentials.

   For example:

```
user: sio_1@ldaps.local, password: password
```

CHAPTER 7

LDAP facts

This chapter contains the following topics:

- AD configuration propagation 70
- Changing Group to Role Association 70

AD configuration propagation

Every change in the Active Directory (AD) needs to propagate to all AD nodes.

Depending on the cluster configuration, the propagation process may take some time. It usually takes around 20 minutes, but could take up to a few hours.

Changing Group to Role Association

After changing the groups to role associations for the LDAP service used in the current login process, log in again to bring the changes into effect.

For information, see Group Assignment on page 55).