16

WebLogic Server Security

Objectives

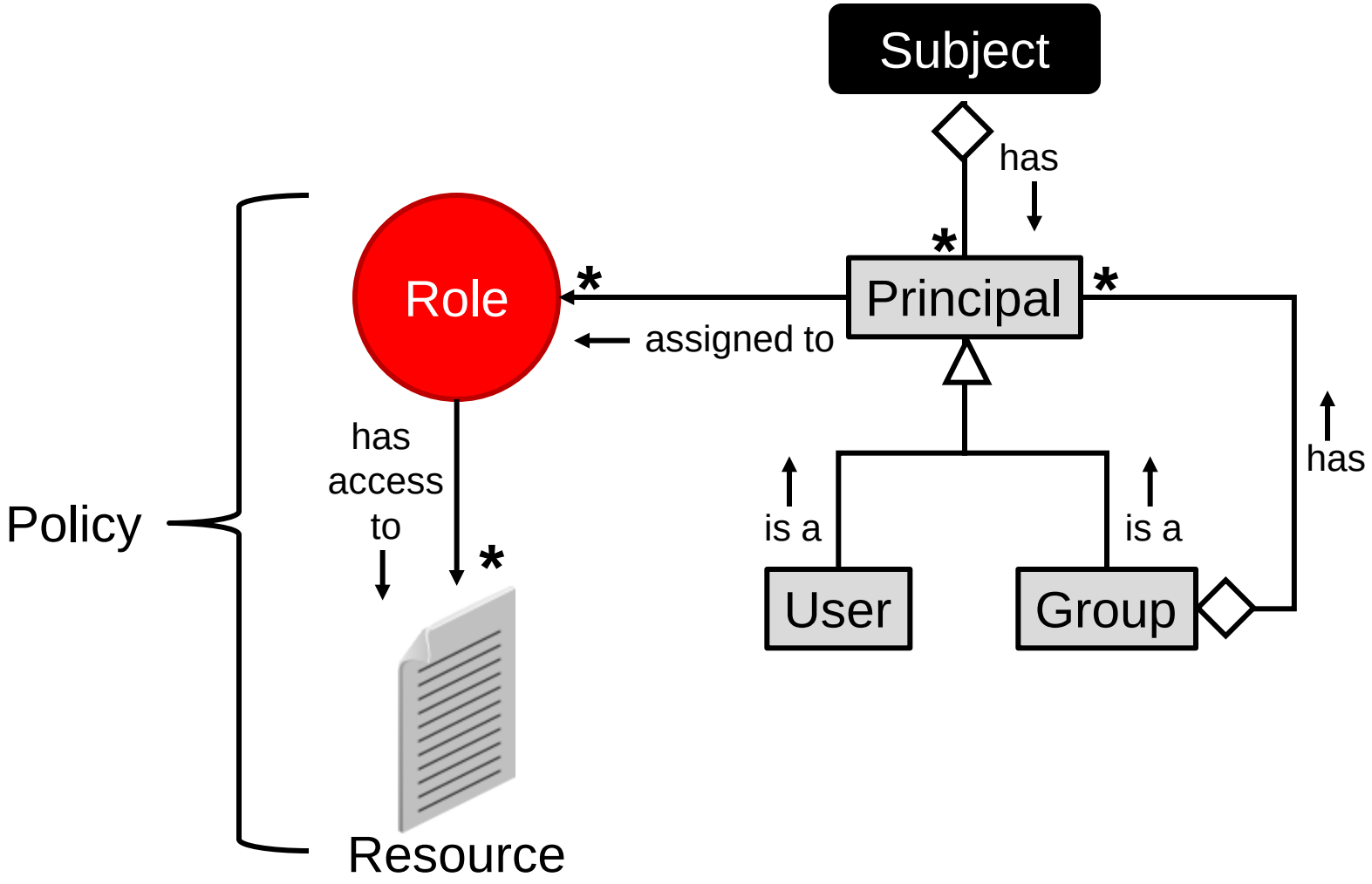
After completing this lesson, you should be able to:

- Describe the basics of the WebLogic Server security architecture
- Describe basic LDAP concepts
- Configure an external LDAP authentication provider for WebLogic Server

Some Security Terms

- *Subject*: The user (or service) accessing the system
  - A subject has one (or more) *principals*
- *Principal*: The unique identity of a subject, assigned after authentication
  - Usually a username or a group name
- *User*: An individual (or program) accessing the application
- *Credentials*: Usually username or password
- *Group*: A collection of users and/or other groups
- *Role*: A type of user
  - Principals can be assigned roles to say what kind of user they represent
- *Policy*: A security rule, usually an association of a resource to one or more roles

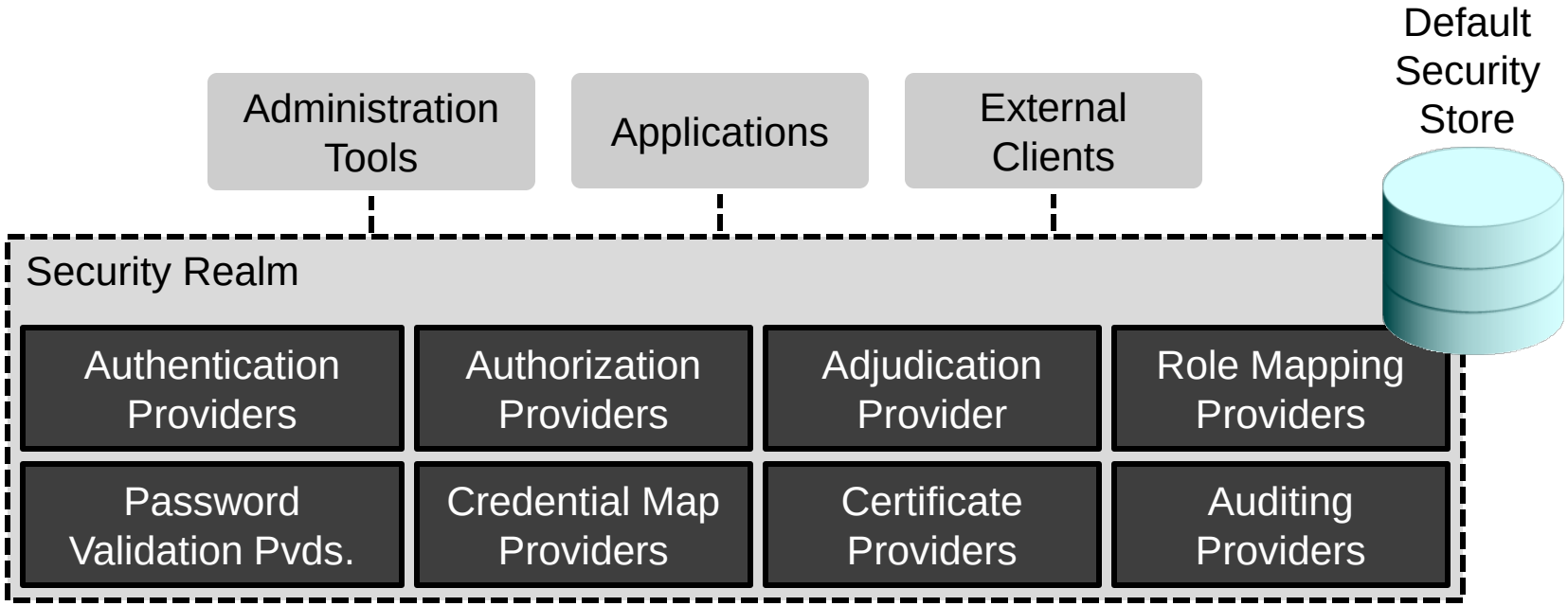
Some Security Terms: Graphically



WebLogic Server Security Realm

A WebLogic Server security realm:

- Handles security logic and decisions for a domain
- Consists of a series of pluggable security providers
- Applies to all servers in a domain



What the Providers Do

- **Authentication:** Who are you? Prove it.
  - Can optionally use an Identity Assertion Provider, which takes a token from outside of WebLogic Server, validates it, and, if valid, maps the token to a username.
- **Authorization:** Are you allowed to use this resource?
  - Uses the Role Mapping provider
- **Adjudication:** The multiple authorization providers do not agree. Can the user have the resource?
- **Role Mapping:** What type of user are you?
  - For example: `manager`, `salesperson`, `administrator`
- **Password Validation:** Does the new or modified password meet the password rules?

What the Providers Do

- **Credential Mapping:** Maps a user authenticated to WebLogic Server to a set of credentials for another system, so that the user can access that other system
- **Certificate Providers:** Keeps a list of trusted digital certificates and validates those certificates
- **Auditing:** For certain user tasks, tracks who did what and when

Security Stores

A persistent store is assigned to a security realm to persist assets such as:

- Users and groups
- Roles
- Policies
- Credential maps
- Certificates

Some providers use the default security store while others use an external system.

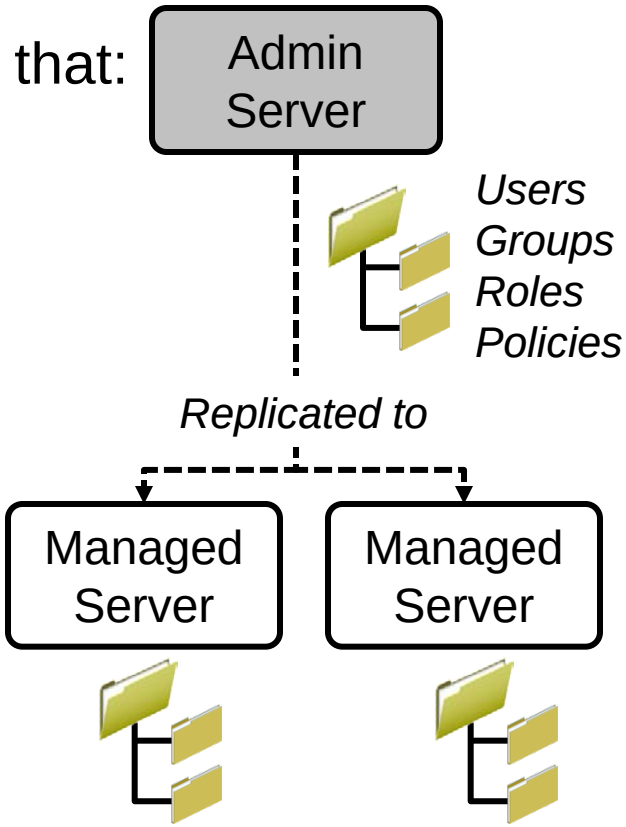
Default Security Store Implementation

- The WebLogic default:
  - An embedded LDAP server running on the admin server and replicated to the managed servers
- Or, you can configure the RDBMS security store:
  1. In the admin console, select the realm. Then select **Configuration** > **RDBMS Security Store**.
  2. Select **RDBMS Security Store Enabled** and fill in the required fields.
     - The schema files are located at `<WL_HOME>/server/lib`.

Default Security Configuration

A new domain includes a default realm that:

- Includes default providers:
  - Default authenticator
  - Default identity asserter
  - XACML* role mapper
  - XACML* authorization provider
  - Default password validator
  - Default credential mapper
  - Default certificate path provider
    - Validates certificate chains
- Uses the embedded LDAP security store



* eXtensible Access Control Markup Language: An XML-based security policy language

Security Customization Approaches

- Create an entirely new security realm and add (at least) the required providers.
  - After the new security realm is configured, make it the active security realm.
- Add, remove, and configure providers in the default realm, called `myrealm`.
- Have developers create custom security providers and add them to either the default realm or a custom security realm.

Most realm modifications require a domain restart.

Authentication Providers

Authentication providers are organized into two categories:

- *Authenticators:*
  - Establish the user's identity given some credentials (like username and password)
  - Can associate multiple principals with a single user, such as groups
- *Identity asserters:*
  - Validate tokens claiming a user has already been authenticated
  - Allow WebLogic Server to participate in single sign-on (SSO) solutions
  - Can map the token to a local user and use authenticators to look up that user's principals

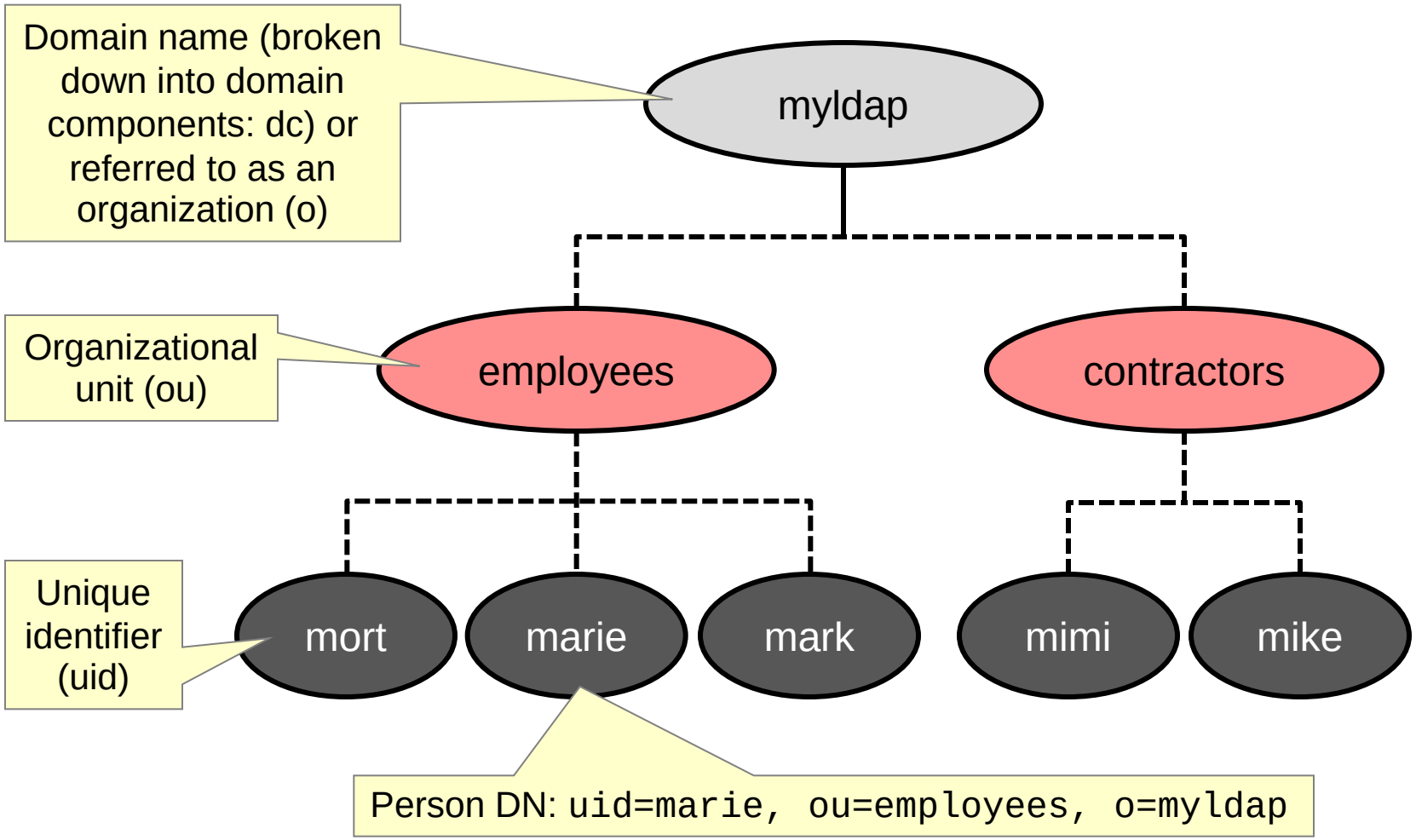
Available Authentication Providers

- Available authenticators include:
  - Default (Internal LDAP)
  - LDAP (generic and vendor-specific)
  - Database (multiple DBMS providers)
  - Windows NT
  - SAML (Security Assertion Markup Language)
- Available identity asserters include:
  - Default
  - LDAP X509
  - SAML
  - Negotiate (SPNEGO)

Lightweight Directory Access Protocol (LDAP)

- LDAP:
  - Is a TCP/IP protocol
  - Provides a hierarchical lookup and search service
  - Models information as a tree of entries, whose attributes are defined by a schema or “object class”
  - Defines default schemas for common entries like people and groups
  - Supports SSL
- Entries:
  - Identify their locations in the tree by using a *distinguished name* (DN)
  - Can be referrals that link to other LDAP servers

LDAP Structure



LDAP Search Operations

Searching for LDAP entries involves:

1. The base DN from which to start searching
2. A search filter that specifies the:
   - Search criteria in terms of attribute values
   - The type or “object class” of the desired entries
3. An indication whether or not the search should include any child entries

LDAP Query Basics

- = (equal)
  - Example: `(uid=tjp)`
- & (logical and)
  - Example: `(&(uid=tjp)(sn=Parker))`
- | (logical or)
  - Example: `(|(uid=tjpark)(uid=tjp))`
- ! (logical not)
  - Example: `(!(sn=Parker))`
- * (wildcard)

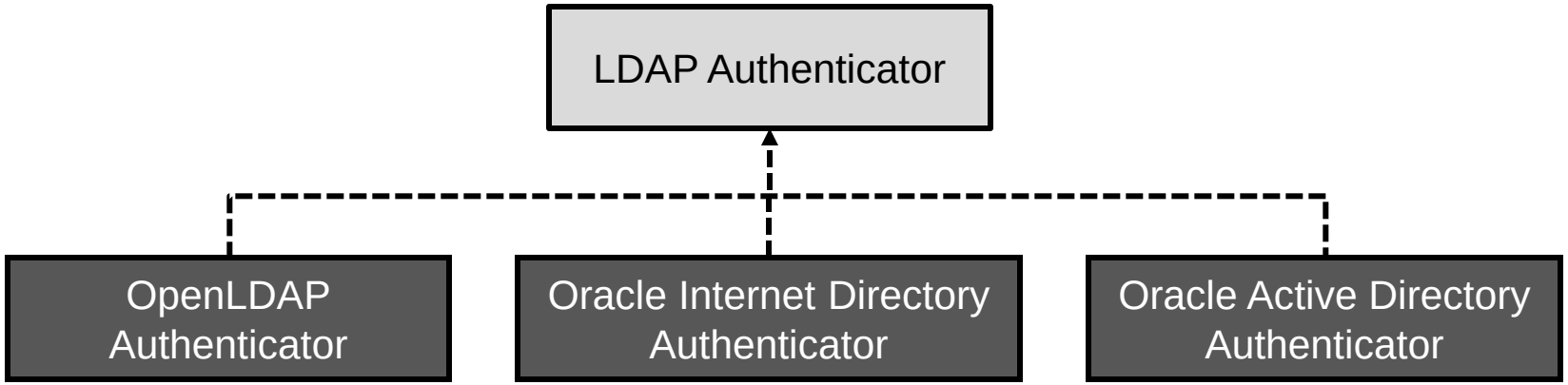
Here is an LDAP search filter that finds all person entries whose user ID begins with “t,” while ignoring those whose surname starts with “Th”:

```
(&(&(uid=t*)(!(sn=Th*)))(objectclass=person))
```

LDAP Authentication Providers

WebLogic Server includes:

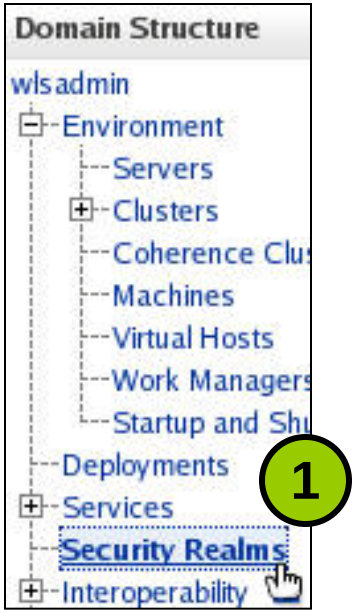
- A base LDAP authenticator that can be configured to support any compliant vendor
- Vendor-specific LDAP authenticators, whose attributes are set to vendor-specific defaults for convenience



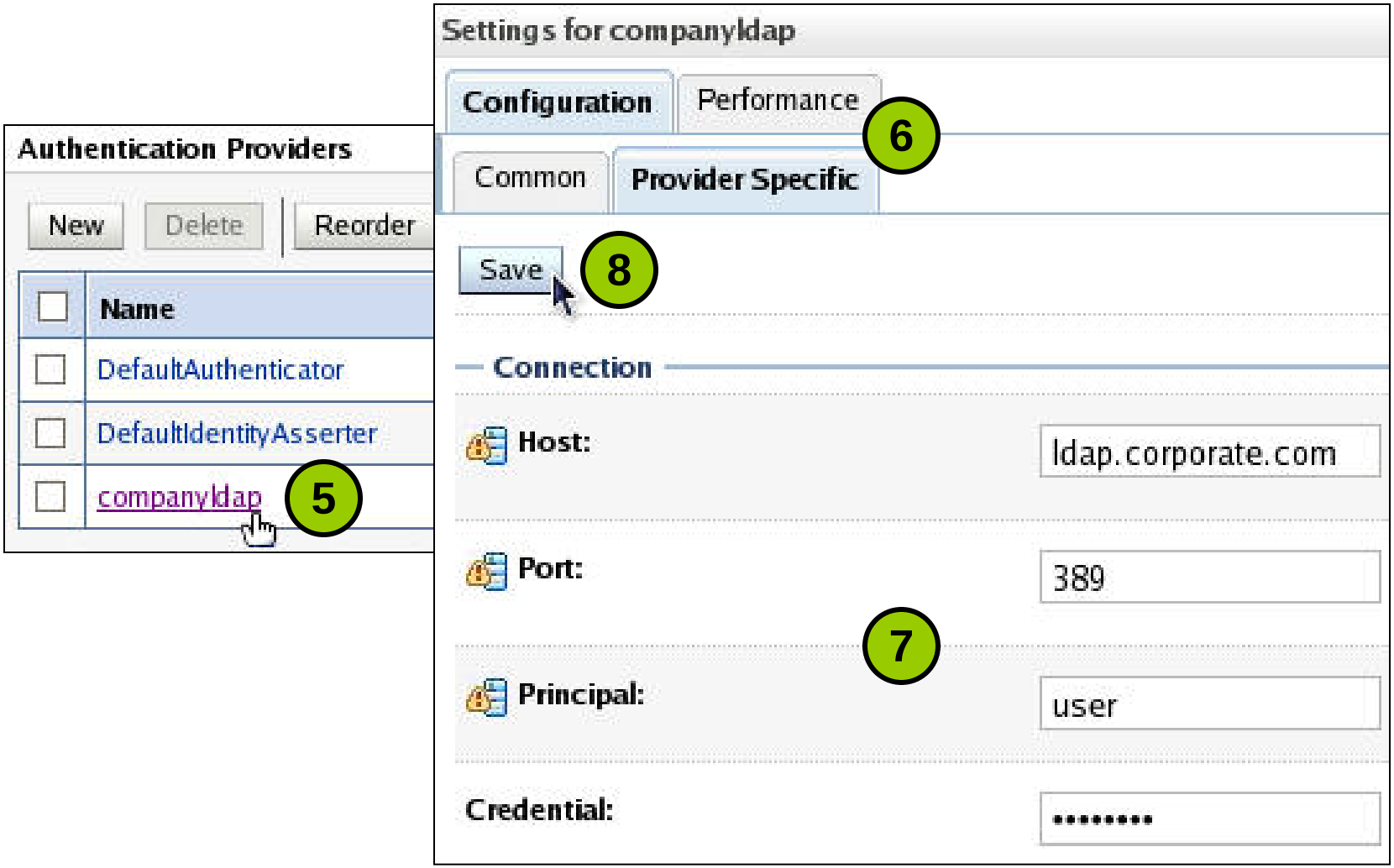
Available LDAP Authentication Providers

- The available LDAP authentication providers include:
  - LDAP Authenticator (generic)
  - Oracle Internet Directory Authenticator
  - Oracle Virtual Directory Authenticator
  - iPlanet Authenticator
  - Active Directory Authenticator
  - Novell Authenticator
  - OpenLDAP Authenticator
- These providers:
  - Can be used to change passwords of existing users
  - Cannot be used to create, update, or delete users and groups

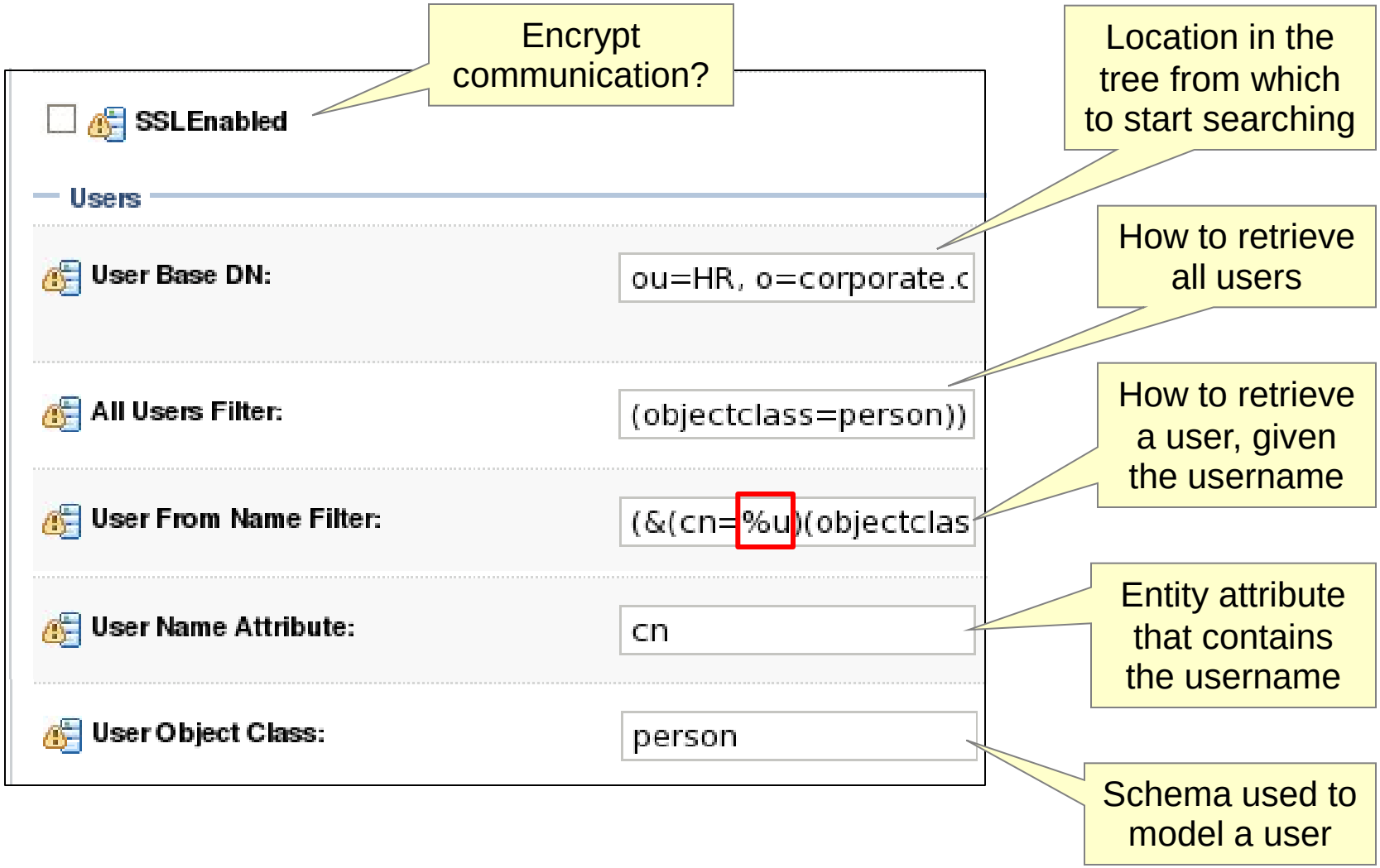
Creating a New LDAP Authentication Provider



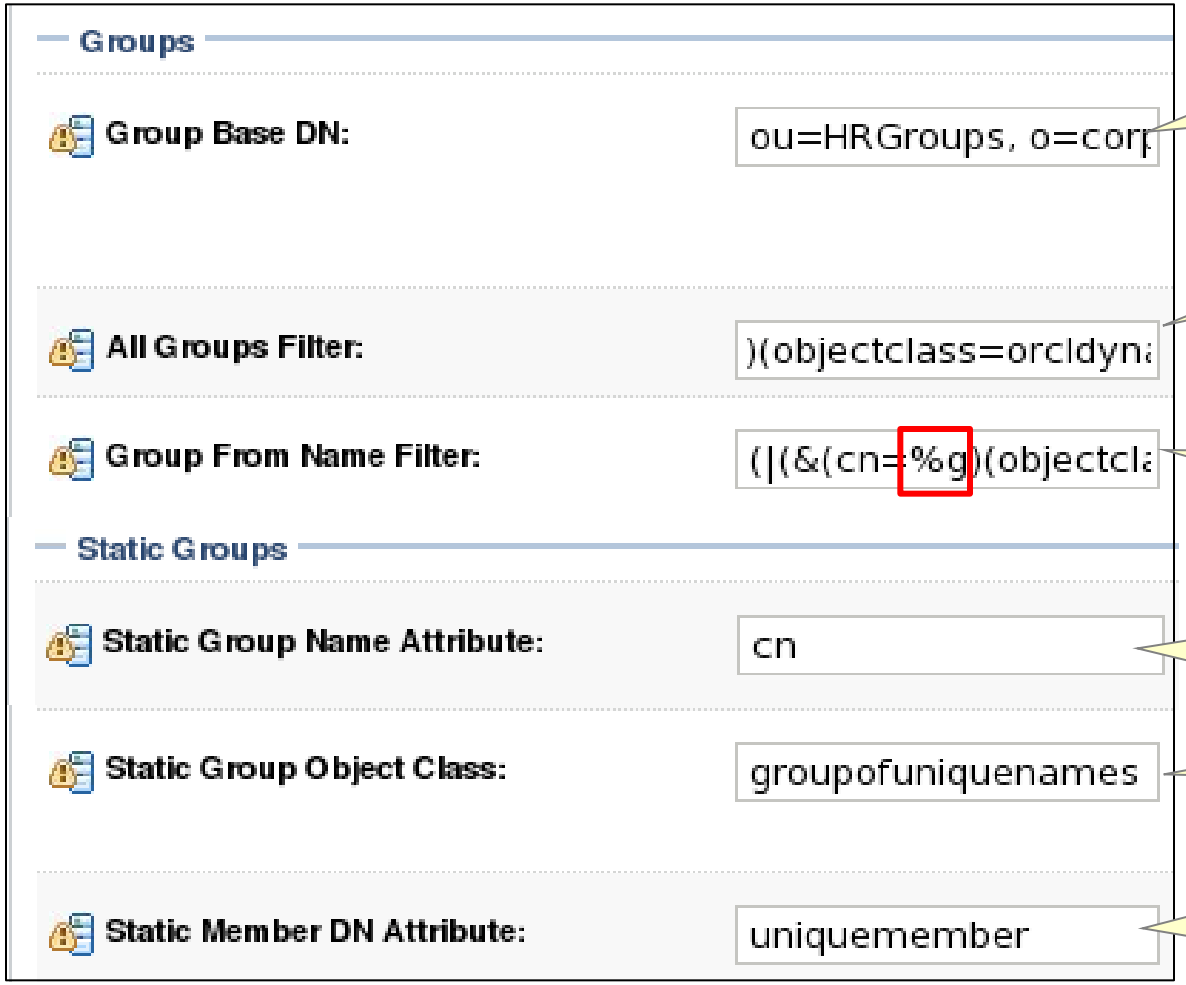
Configuring the LDAP Provider: Connection



Configuring the LDAP Provider: Users



Configuring the LDAP Provider: Groups



Location in the tree from which to start searching

How to retrieve all groups

How to retrieve a group, given its name

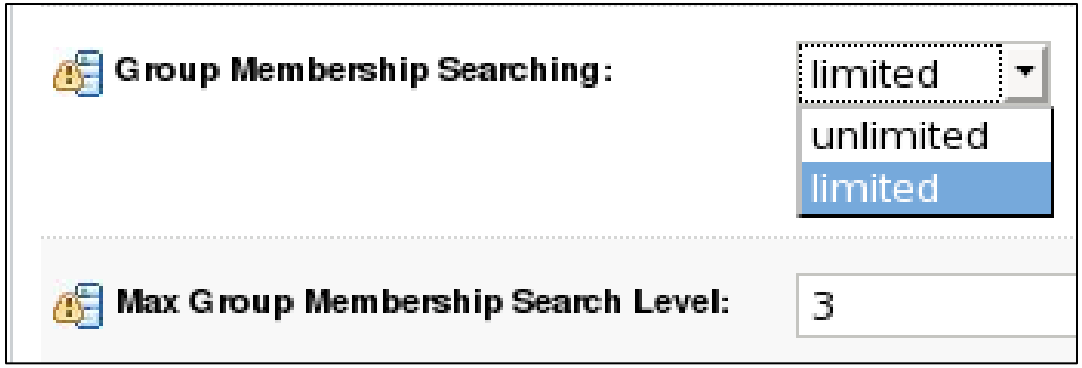
Entity attribute that contains group name

Schema used to model a group

Entity attribute that contains members

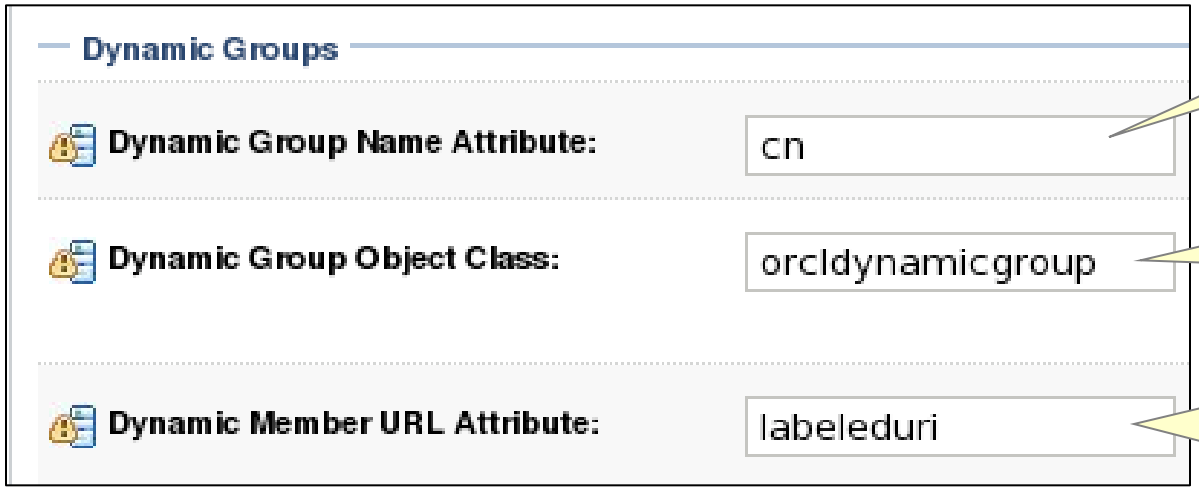
Configuring the LDAP Provider: Subgroups

- Groups can include other groups.
- To improve performance, you can limit the depth that the provider will search for subgroups.



Configuring the LDAP Provider: Dynamic Groups

- Instead of a list of users, dynamic groups contain a list of search filters, each of which returns zero or more users.
- Member search filters are expressed as URLs.



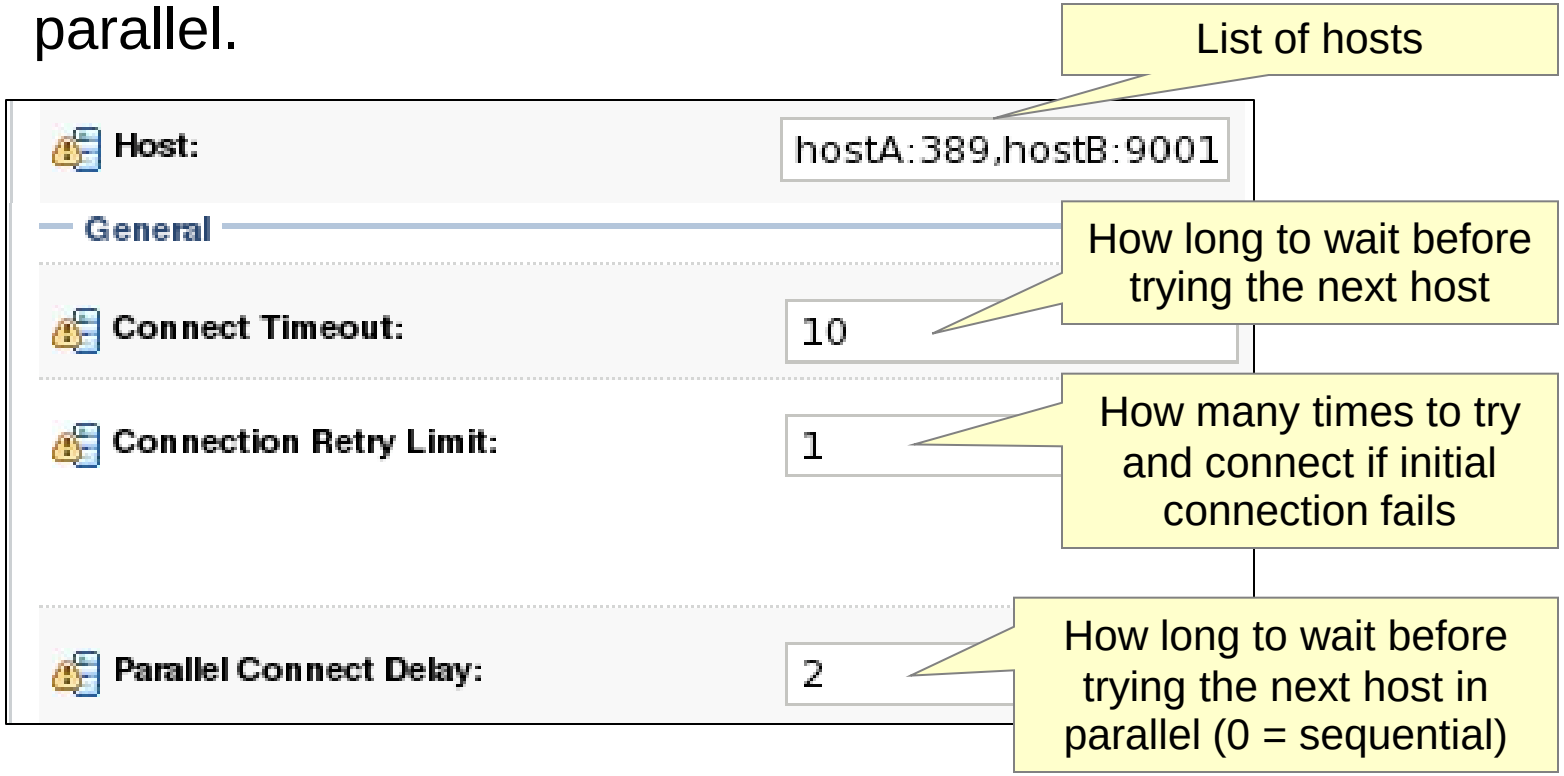
Entity attribute that contains the group name

Schema used to model a dynamic group

Entity attribute that contains member search filters

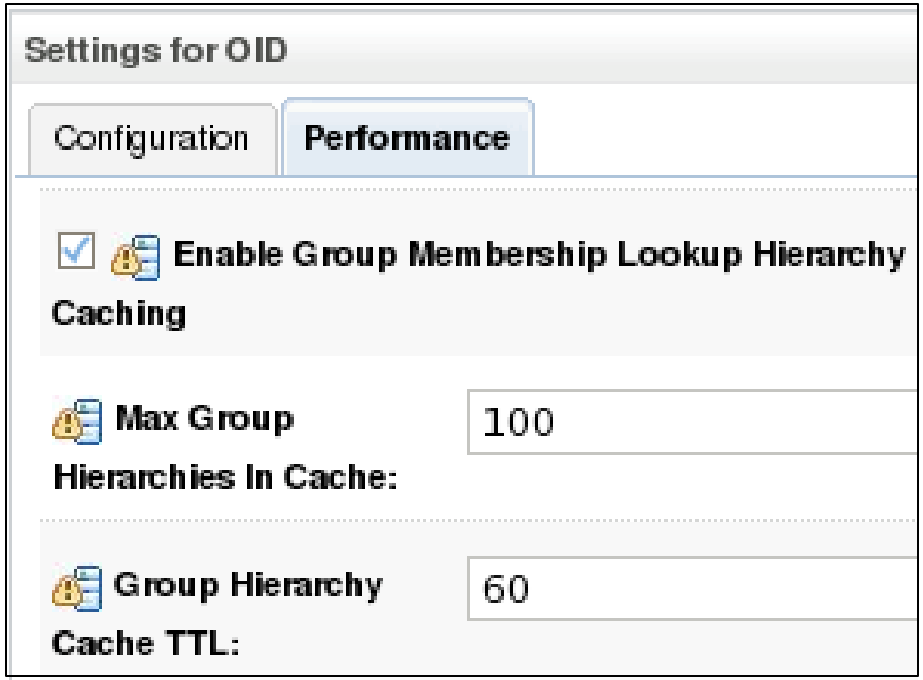
LDAP Failover

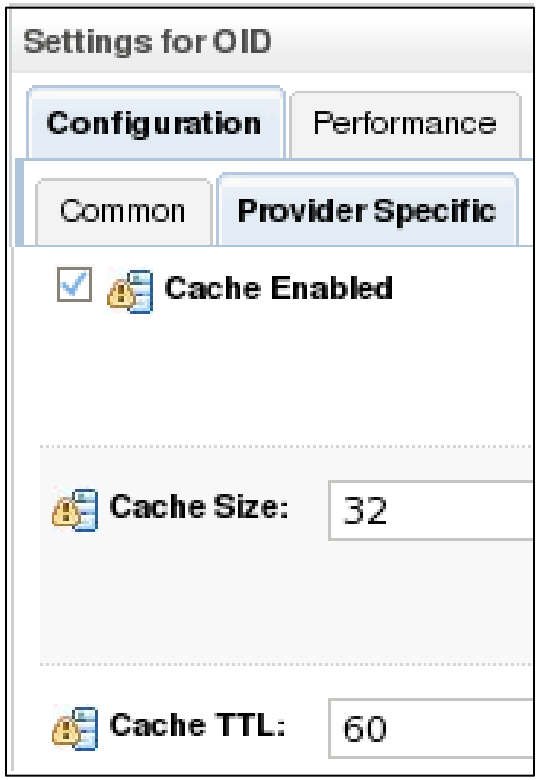
- The **Host** attribute supports a list of candidate servers for high availability.
- Connection attempts can be made sequentially or in parallel.



LDAP Caching

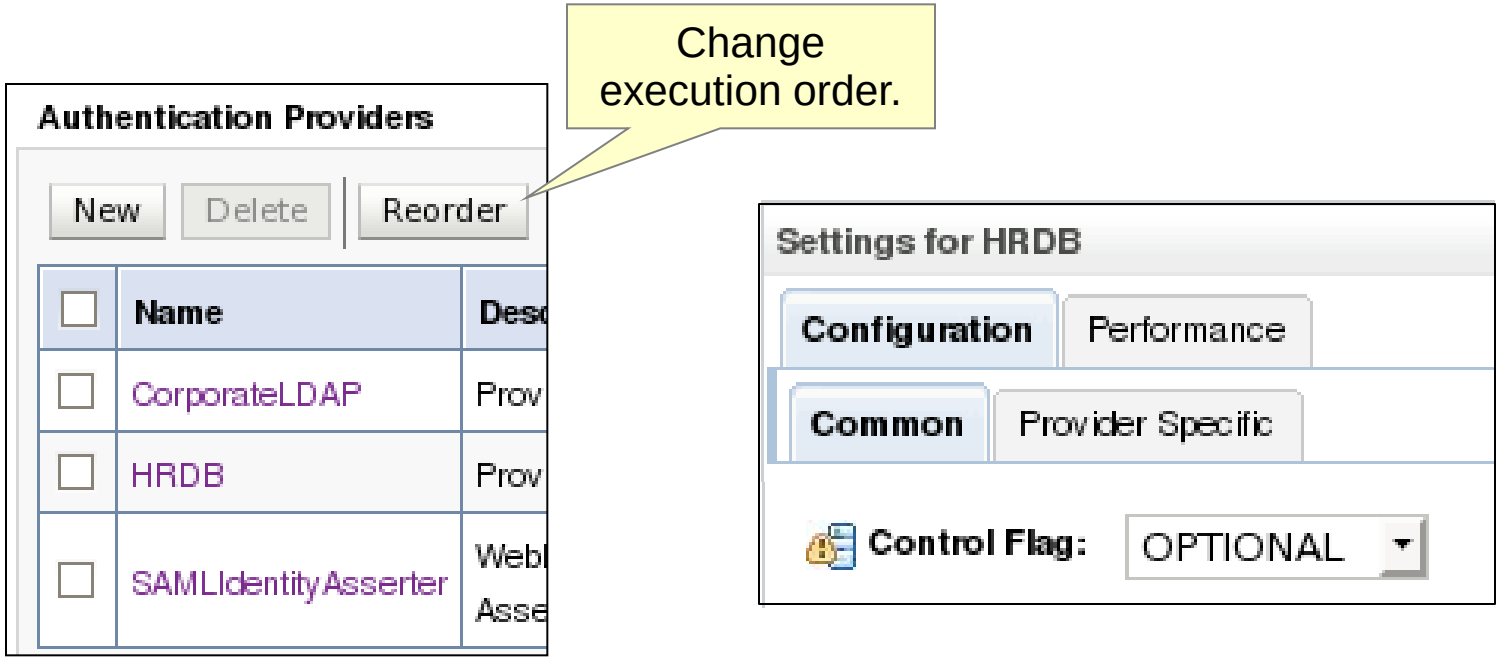
- All authenticators can cache a group's member list.
- LDAP Authenticators can also cache individual entries.





Multiple Authentication Providers

- A single security realm can support multiple authentication providers.
- For authenticators, *control flags* determine the processing logic as each provider is executed.



Control Flags

Flag	Explanation	Success Action	Failure Action
REQUIRED	Must succeed	Execute next provider	Execute next provider, but outcome is: FAIL
REQUISITE	Must succeed	Execute next provider	Return control to application with: FAIL
SUFFICIENT	Not required to succeed	Return control to application with: SUCCESS	Execute next provider
OPTIONAL	Not required to succeed	Execute next provider	Execute next provider

Administration Groups

At least one authentication provider must exist that associates users with groups that have WebLogic Server administrative rights.

Group	Default Capability (via roles and policis)
Administrators	Full administrative access to the domain and its applications
Operators	View domain configuration, start and stop servers
Deployers	View domain configuration, deploy, undeploy, and update applications
Monitors	View domain configuration
AppTesters	Access applications running in admin mode (servicing administration requests) through the admin port

Often the default authentication provider retains the administrative users, groups, roles and policies; another authentication provider is added for “regular” users, groups, roles and policies.

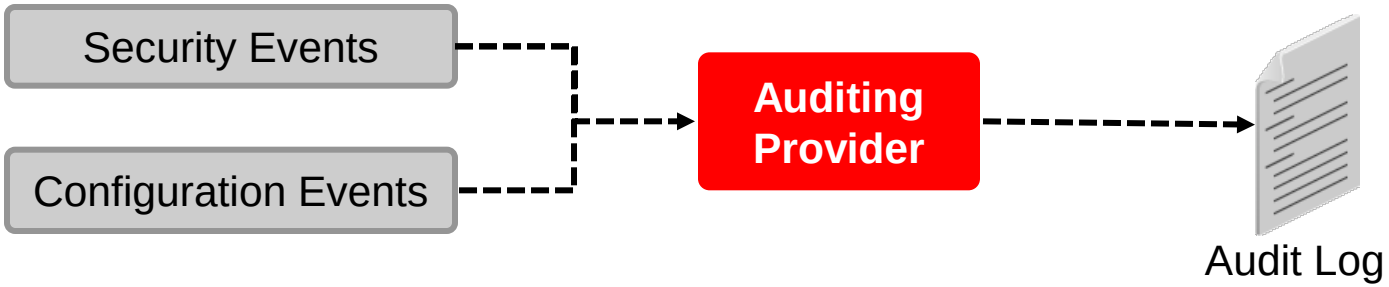
Troubleshooting Authentication

- If you think users are doing things that they should not do, configure an auditing provider.
  - The default auditing provider can be quickly configured.
- Use the server logs.
  - Enable security realm debug flags for more detailed log messages.
- Check the external LDAP authentication provider configuration attributes.
- Use any debug capabilities of the external LDAP Server software.

Auditing Provider

The WebLogic auditing provider:

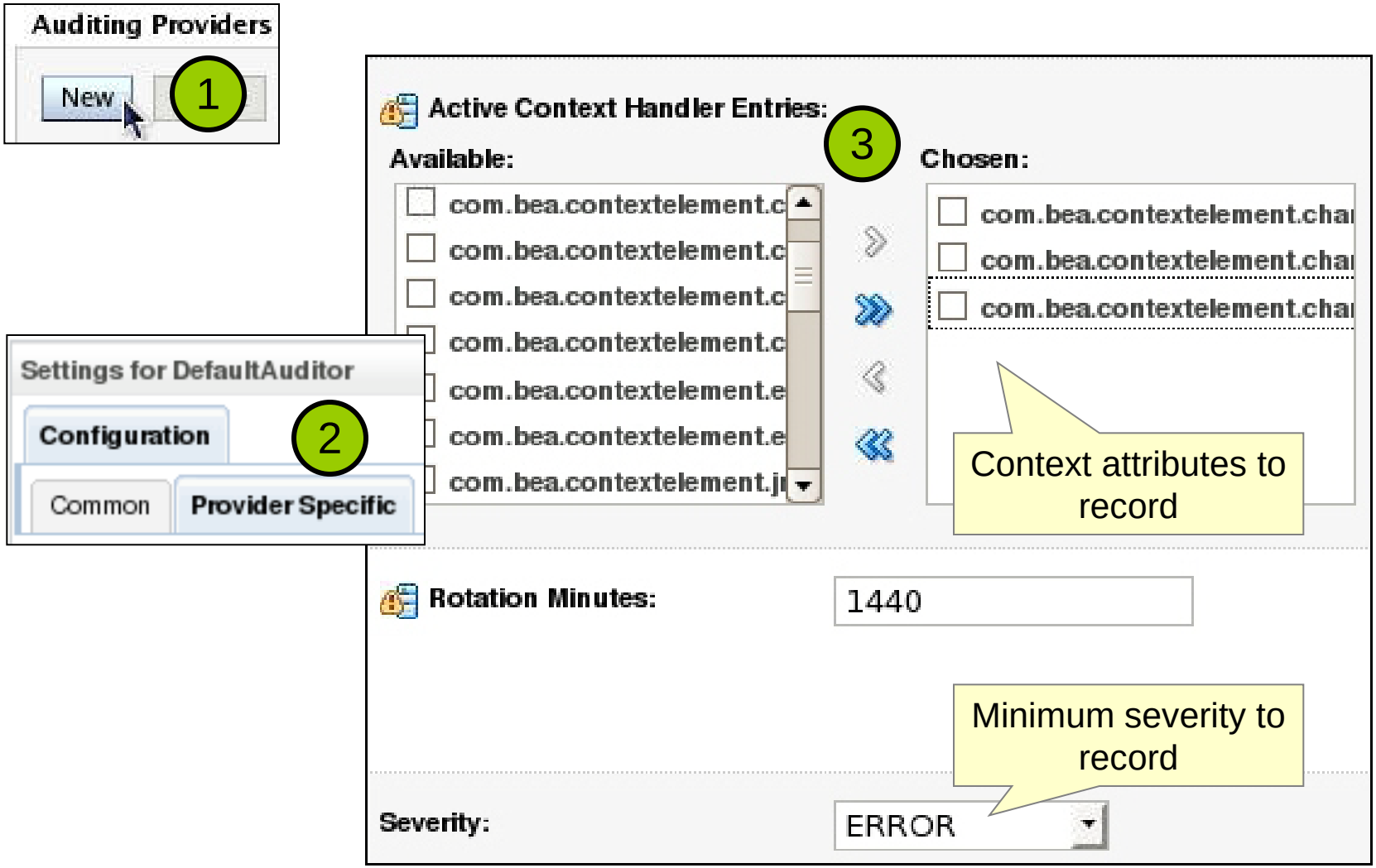
- Creates a detailed record of all security changes and decisions within a domain in each server's `logs` directory to a file named `DefaultAuditRecorder.log`.
- Can also create a record of all domain configuration changes
- Is not enabled by default



Security Audit Events

- Typical security events:
  - An authentication or identity assertion is attempted.
  - A new role or policy is created.
  - A user account is locked out or is unlocked.
- Security events have the following characteristics:
  - Name
  - Severity (`WARNING`, `ERROR`, `SUCCESS`, and so on)
  - Zero or more “context attributes:”
    - Protocol, port, address
    - HTTP headers
    - EJB method parameters
    - SAML tokens

Configuring the Auditing Provider



Security Realm Debug Flags

Flag	Description
DebugSecurityRealm	Trace the initialization of the realm's providers and the loading of initial data from the default store.
DebugSecurityAtn	Trace the authentication and management of users and groups.
DebugSecurityRoleMap	Trace role policy evaluations and results.
DebugSecurityAtz	Trace authorization policy evaluations and access decisions.
DebugSecurityAdjudicator	Trace final authorization decisions.
DebugSecurityUserLockout	Trace the locking and unlocking of user accounts based on the number of invalid login attempts.
DebugSecuritySAML*	Trace the processing and/or generation of SAML tokens.

Multiple SAML security flags

Common LDAP Issues

Typical causes include:

- The wrong base DN, object class, or attribute has been set for users or groups.
- A configured search filter is syntactically valid, but it is semantically incorrect.
  - So, it fails to retrieve the intended users or groups.
- An insufficient “maximum level for nested group memberships” has been set.
  - So, not all group members are found, which means some users are not mapped to their proper roles.
- WebLogic Server does not trust the LDAP server’s SSL certificate (and they are set to communicate over SSL).

Quiz

The WebLogic Server default security realm uses this as its security provider store by default:

a. Oracle Database
b. Embedded LDAP Server
c. Derby Database
d. OpenLDAP Server
e. Any Database

Quiz

With LDAP, what does DN stand for?

a. Directory Network
b. Dynamic Name
c. Distinguished Name
d. Directory Name

Quiz

Which of the following is NOT an available authentication provider control flag?

a. SUFFICIENT
b. REQUISITE
c. OPTIONAL
d. ALWAYS
e. REQUIRED

Summary

In this lesson, you should have learned how to:

- Describe the basics of the WebLogic Server security architecture
- Describe basic LDAP concepts
- Configure an external LDAP authentication provider for WebLogic Server

Practice 16-1 Overview: Configuring an Authentication Provider

This practice covers the following topics:

- Initializing Apache DS LDAP
- Setting DS LDAP as one of the authentication providers
- Setting the appropriate control flags
- Testing the new authentication provider