Enhanced Security Using LDAP Authentication

Webinar - November 8, 2017 at 11:00 am PST / 2:00 pm EST (UTC-8)

Adamo Tonete - Senior Technical Services Engineer

Agenda

- Security 101;
- Default Roles;
- Creating a user;
- What is LDAP;
- Packages needed;
- LDAP + PSMDB - Creating users with LDAP;
- Live demo;
- Q&A.

**PSMDB stands for Percona Server for MongoDB*

Security 101

Minimum security requirements;

Except for some use cases, *listen ip* must only listen to local network;

Use at least a keyfile in a replica-set;

Create an administrative user and create one user per client/application, with the minimum access needed to work with the database.

Authorization vs Authentication

While authentication **proves who you are**, the authorization checks what **can be done under a specific account**.

The LDAP integration will only authenticate the user and will not perform any authorization.

Default Roles

read	readWrite	dbAdmin	dbOwner
userAdmin	clusterAdmin	clusterMonitor	clusterManager
hostManager	backup	restore	readAnyDatabase
readWriteAnyDatabase	userAdminAnyDatabase	dbAdminAnyDatabase	root
__system			

Creating the administrator user;

After installing the database, create an administrative user with:

```
use admin
db.createUser({user :'admin', pwd: '123',
roles : ["root"]})
```

Creating a read-only user

In order to create a read-only user, we will need to specify one pre existing role, such as:

```
use admin
db.createUser({user :'admin', pwd: 'mypass',
roles : ["readAnyDatabase"]})
```

The admin database

The admin database stores information from all the users and their roles. We can issue queries against this database in order to read its information.

The following slide has an example of how user information is stored on the system.users collection in the admin database.

The admin database

```
db.system.users.find().pretty()
{
	"_id" : "admin.admin",
	"user" : "admin",
	"db" : "admin",
	"credentials" : {
		"SCRAM-SHA-1" : {
			"iterationCount" : 10000,
			"salt" : "ZuACyMJlu/s0dJpFzsp70Q==",
			"storedKey" : "zwFmdoqRCVfirWBbR1Ow1wg+HHk=",
			"serverKey" : "nqXAVQxV/qCWtoh5R/g5X+Fz99A="
		}
	},
	"roles" : [
		{
			"role" : "root",
			"db" : "admin"
		}
	]
}
```

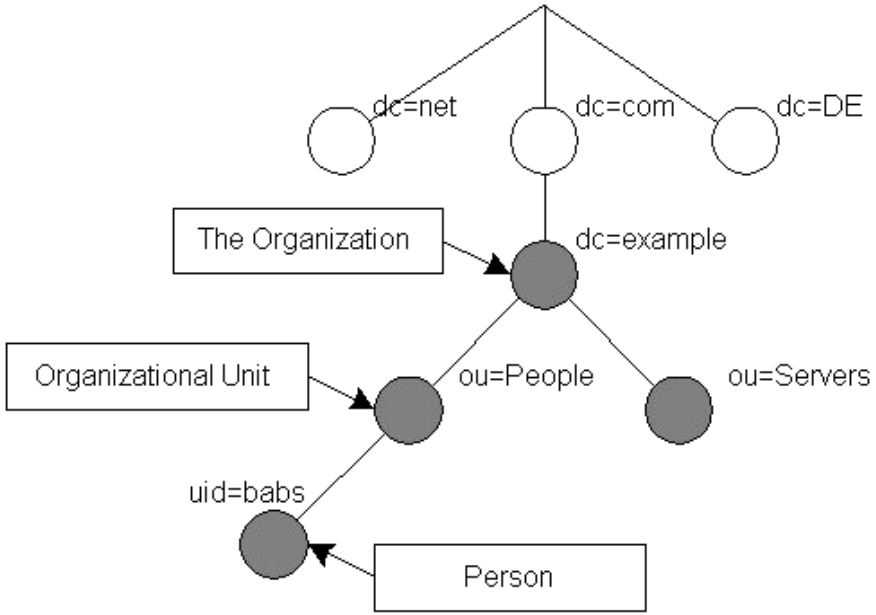
What is LDAP?

LDAP stands for lightweight directory access protocol;
A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server so as to validate users.[4]

Microsoft has their own domain service, which is called Active Directory.

We are going to use OpenLDAP for this demo (freeware)

What is LDAP - domain tree



http://www.openldap.org/doc/admin22/intro.html

What packages do I need?

Slapd - Daemon LDAP process;
ldap-utils - Utility package to manipulate data on LDAP;
sasl2-bin cyrus ldap utility to connect to the LDAP server;
phpldapadmin - web interface to manipulate and visualize ldap users and configure domains.

How to create an LDAP user on PSMDB?

```
> db.getSiblingDB("$external").createUser({
user : 'support',
roles: [ {role : "read", db: 'percona'} ]
})
Successfully added user: {
  "user" : "support",
  "roles" : [
    {
      "role" : "read",
      "db" : "percona"
    }
  ]
}
```

How to authenticate on PSMDB with LDAP?

```
db.getSiblingDB("$external").auth(
{
  mechanism: "PLAIN",
  user: 'support',
  pwd: '123',
  digestPassword: false
}
)
```

Live Demo;

- Ubuntu server 16.04
- Percona Server for MongoDB 3.4.x

Review;

- PSMDB needs sas2-bin library configured to communicate to the ldap server;
- Authentication must be enabled and plain text mechanism must be enabled;
- LDAP users will be authenticated externally but the authorization still being handled by mongodb.
- https://www.percona.com/blog/2017/11/06/mongodb-security-using-ldap-authentication/ for more info.

Questions?

Database Performance Matters