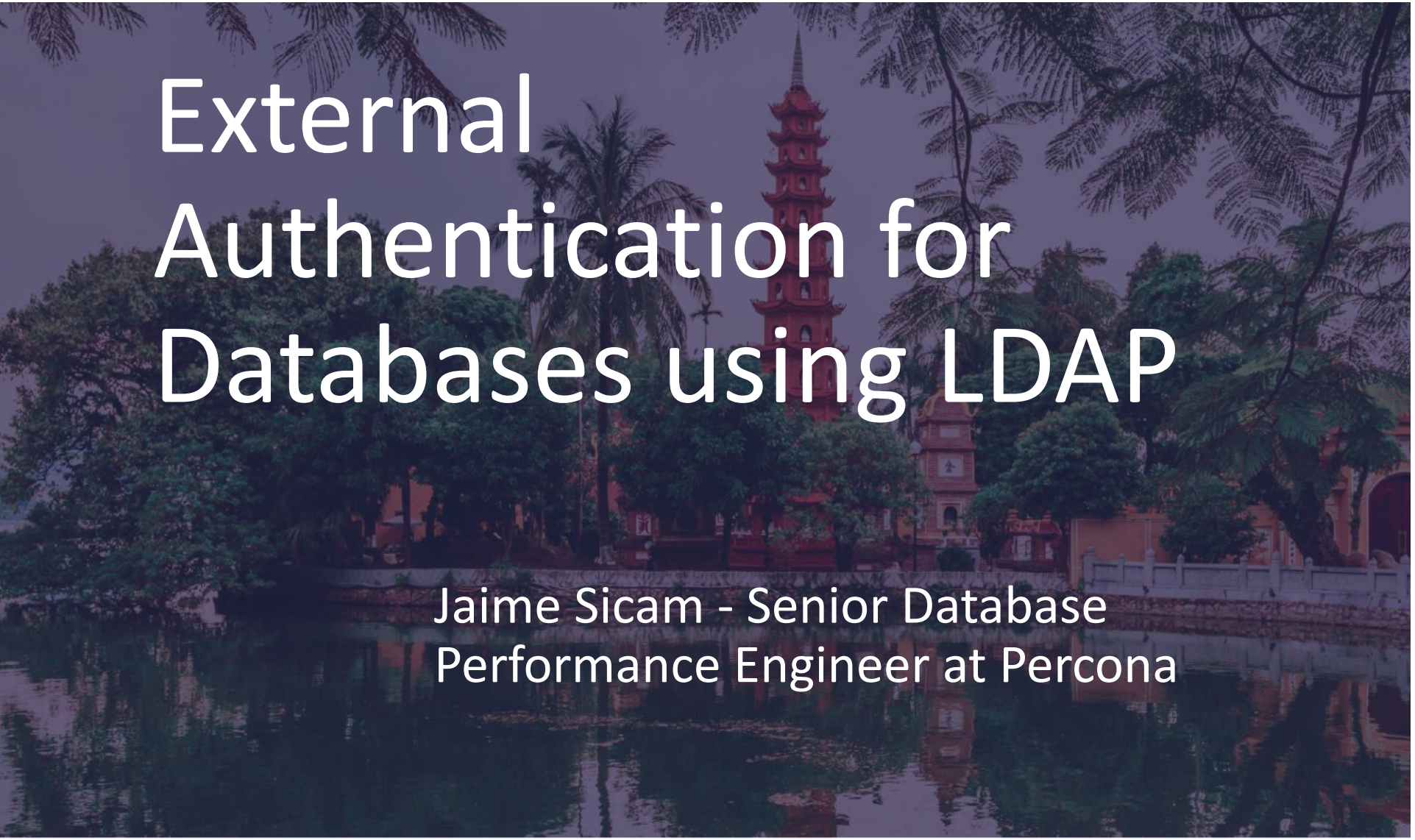
External Authentication for Databases using LDAP



Jaime Sicam - Senior Database Performance Engineer at Percona

Hanoi, Vietnam 2024

PERCONA UNIVERSITY

Open Source Databases Meetup

In partnership with BNH Better and Higher

About Me

- **Senior Database Performance Engineer at Percona**
- **APAC support team (Vietnam, India, Australia, Philippines)**
- **Based in Metro Manila, Philippines**

Managing Users in Databases

- **Every Database software have their own built-in feature for managing users and groups**
- **It becomes a challenge to maintain it across multiple servers**

External Authentication

- **3rd-party system that can check if a user can authenticate or not**
- **Provides centralized information and management of users and groups**
- **Can be used to identify what a user can do based on its membership**
- **Supported in MySQL, MongoDB, and PostgreSQL**

External authentication is an Enterprise Feature!

PostgreSQL is an exception

PERCONA

Percona Server is bundled with Enterprise features

- **Key servers for Encryption at rest**
- **Additional storage engines**
- **Hot backups**
- **Audit logging**
- **External authentication**

LDAP

- **Lightweight Directory Access Protocol**
- **A standard protocol for managing directory services of typically users, groups and devices**
- **Many applications use LDAP for lookups**
- **OpenLDAP, Active Directory, RedHat Directory Server and Samba implement LDAP protocol to access its data**

External Authentication with LDAP

- **MySQL - https://docs.percona.com/percona-server/8.0/ldap-authentication.html**
- **MongoDB - https://docs.percona.com/percona-server-for-mongodb/7.0/ldap-setup.html**
- **PostgreSQL - https://www.postgresql.org/docs/current/auth-ldap.html**

Essential LDAP knowhow for external authentication

- **Connecting to LDAP**
- **Using ldapsearch to enumerate users and groups**
- **Test with Samba**

PERCONA

Adding user accounts in Samba

- **samba-tool user add THE_USERNAME THE_PASSWORD**
  - Eg. samba-tool user add jaime password_of_jaime

PERCONA

Adding group accounts in Samba

- **samba-tool group add THE_GROUP**
  - Eg. samba-tool group add support

PERCONA

Adding user as a member in a group

- **samba-tool group addmembers THE_GROUP THE_USER**
  - Eg. samba-tool group addmembers support jaime

PERCONA

Need help with samba-tool

- **--help can help you out**
- **samba-tool --help**
- **samba-tool user add --help**
- **samba-tool group --help**
- **samba-tool user show --help**

Using samba

- **samba-tool user show devuser01**

```
root@7ab3ff1f1374:/# samba-tool user show devuser01
dn: CN=Dev User01,CN=Users,DC=test,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Dev User01
sn: User01
givenName: Dev
instanceType: 4
whenCreated: 20240417144225.0Z
whenChanged: 20240417144225.0Z
displayName: Dev User01
uSNCreated: 4027
name: Dev User01
objectGUID: 36a4e61c-f04e-4fb6-a9b4-7d68be4ab442
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 0
primaryGroupID: 513
objectSid: S-1-5-21-3177632221-3994852741-1873823975-1106
accountExpires: 9223372036854775807
logonCount: 0
sAMAccountName: devuser01
sAMAccountType: 805306368
userPrincipalName: devuser01@test.com
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=test,DC=com
mail: devuser01@test.com
pwdLastSet: 133578385452815920
userAccountControl: 512
uSNChanged: 4029
memberOf: CN=developers,CN=Users,DC=test,DC=com
distinguishedName: CN=Dev User01,CN=Users,DC=test,DC=com
```

- **samba-tool group show developers**

```
root@7ab3ff1f1374:/# samba-tool group show developers
dn: CN=developers,CN=Users,DC=test,DC=com
objectClass: top
objectClass: group
cn: developers
instanceType: 4
whenCreated: 20240417144226.0Z
uSNCreated: 4039
name: developers
objectGUID: d88dfa0f-383a-43a8-b6af-cb0396e89386
objectSid: S-1-5-21-3177632221-3994852741-1873823975-1110
sAMAccountName: developers
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=test,DC=com
whenChanged: 20240417144227.0Z
member: CN=Dev User01,CN=Users,DC=test,DC=com
member: CN=Dev3 User03,CN=Users,DC=test,DC=com
member: CN=Dev2 User02,CN=Users,DC=test,DC=com
uSNChanged: 4043
distinguishedName: CN=developers,CN=Users,DC=test,DC=com
```


PERCONA

LDAP searches

- **ldapsearch -x -H ldap://ldap.example.com -D "administrator@example.com" -b "CN=Users,DC=example,DC=com" -w PerconaLDAPTest2024 "(cn=Dev User01)"**
- **ldapsearch -x -H ldap://ldap.example.com -D "CN=Administrator,CN=Users,DC=example,DC=com" -b "CN=Users,DC=example,DC=com" -w PerconaLDAPTest2024 "(cn=developers)"**

Quick Demonstration

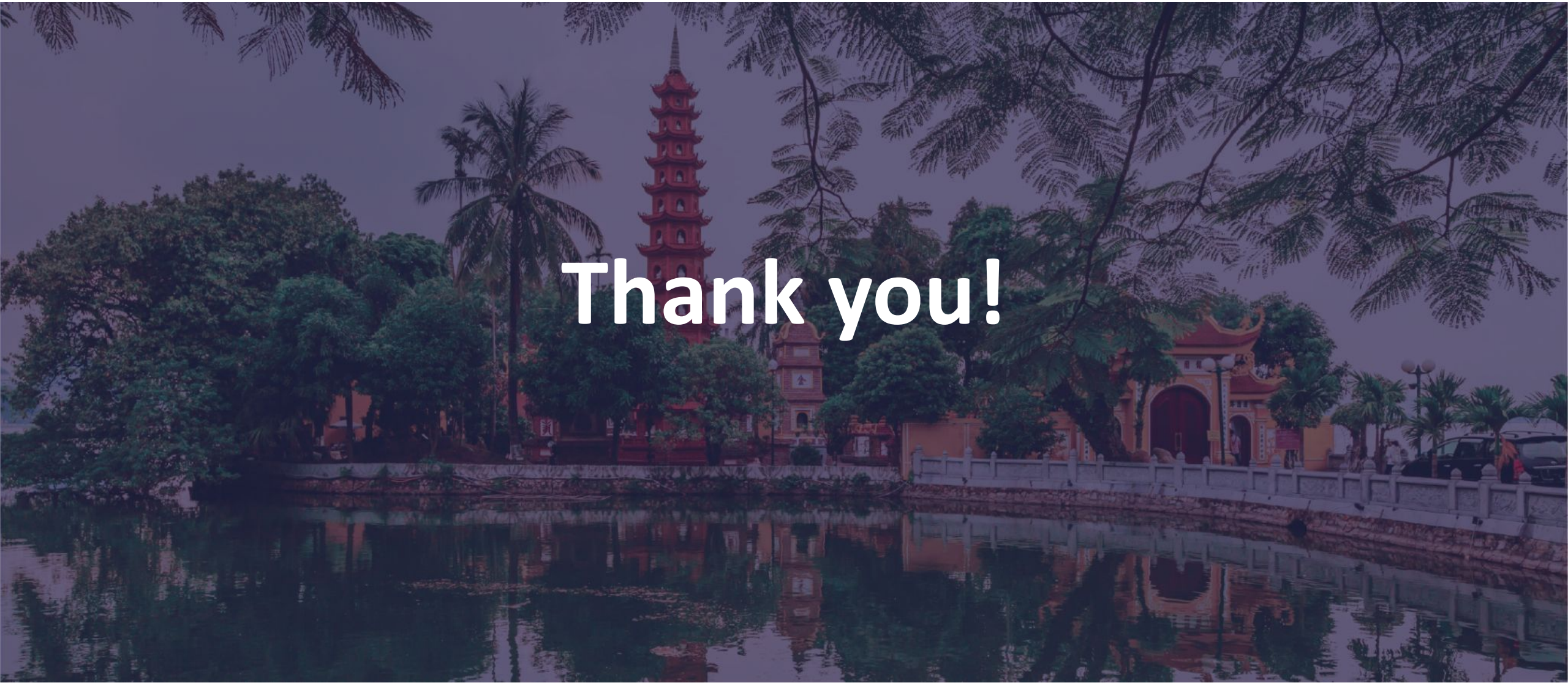
- **Show configuration of LDAP authentication in MySQL, MongoDB and PostgreSQL**
- **Add LDAP user and group**
- **Login with the same user in all of these databases servers**

Hanoi, Vietnam 2024

PERCONA UNIVERSITY

Open Source Databases Meetup

In partnership with BNH Better and Higher



In partnership with BNH Better and Higher