LDAP/AD Integration for DevTest

Surya Anil Kumar Suravarapu

February 2017

Legal Statement

Agenda

User Authentication and Authorization

Authentication / Authorization in DevTest

Challenges with ACL

Solution

LDAP / AD Integration with DevTest

Why do we need this?

How does this work?

How do we configure this?

Demo

Q & A

ca
technologies

User Authentication and Authorization

- Authentication
  - Validate who is who

- Authorization
  - Verify access or performance of an action

- Prevents unauthorized access / usage

- Important aspects of DevTest

Authentication / Authorization in DevTest

Role based Access Control - ACL

ACL
- Users
- Roles

Roles have permissions
- Defined for various action / activities
- Ex: VSE Service Deployment, Stage Test etc.

Enabled by default from DevTest 8.0
- Optional for older versions

Settings → Access Control

ACL Data is stored in DB
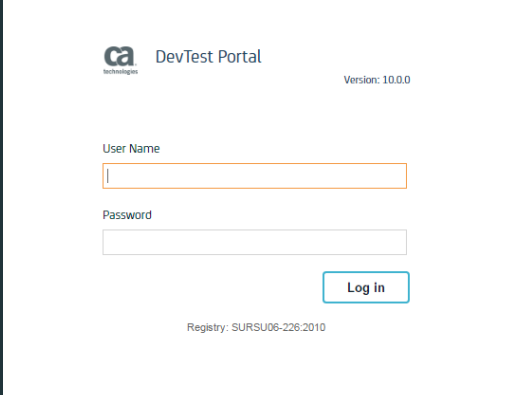
technologies

Challenges with ACL

Separate passwords	Maintenance of passwords • Especially in large organizations
Manual addition of users	User maintenance

ca DevTest Portal

Version: 10.0.0

User Name

Password

Log in

Registry: SURSU06-226:2010

ca
technologies

Solution

- Integration with an existing authentication mechanism

- Should work in conjunction with ACL

- Centralized management of users / passwords

Existing System

DevTest ACL

ca
technologies
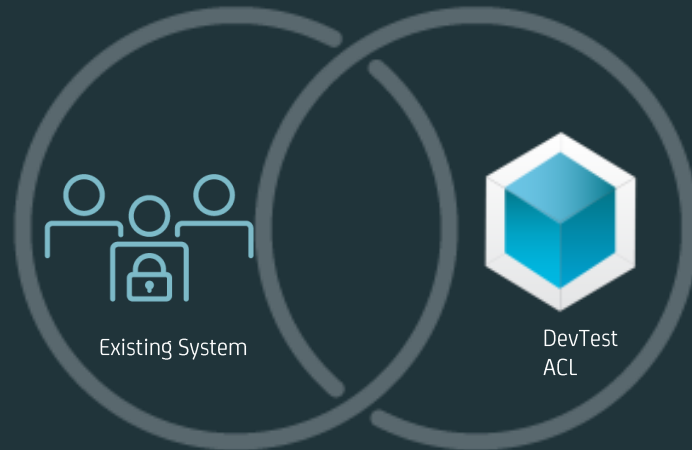
LDAP / AD Integration with DevTest

- Integration with an LDAP or Active Directory based system.

- Enables LDAP administrator to manage users and their passwords
  - User passwords can no longer be managed through ACL.

- Will ensure integration into an already existing user management system.
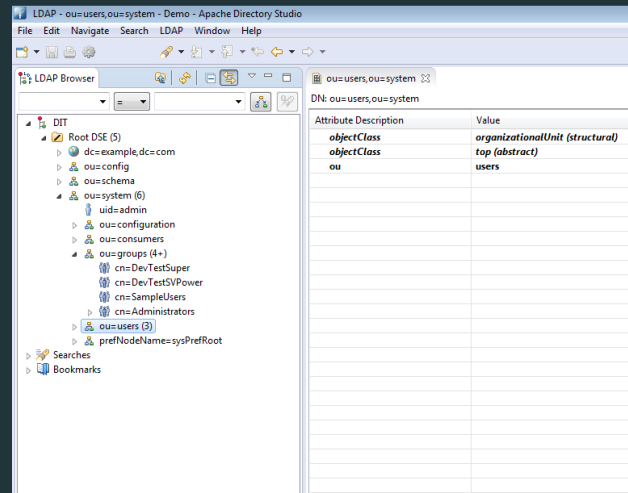
Why do we need this?

- Helps take advantage of existing user management system

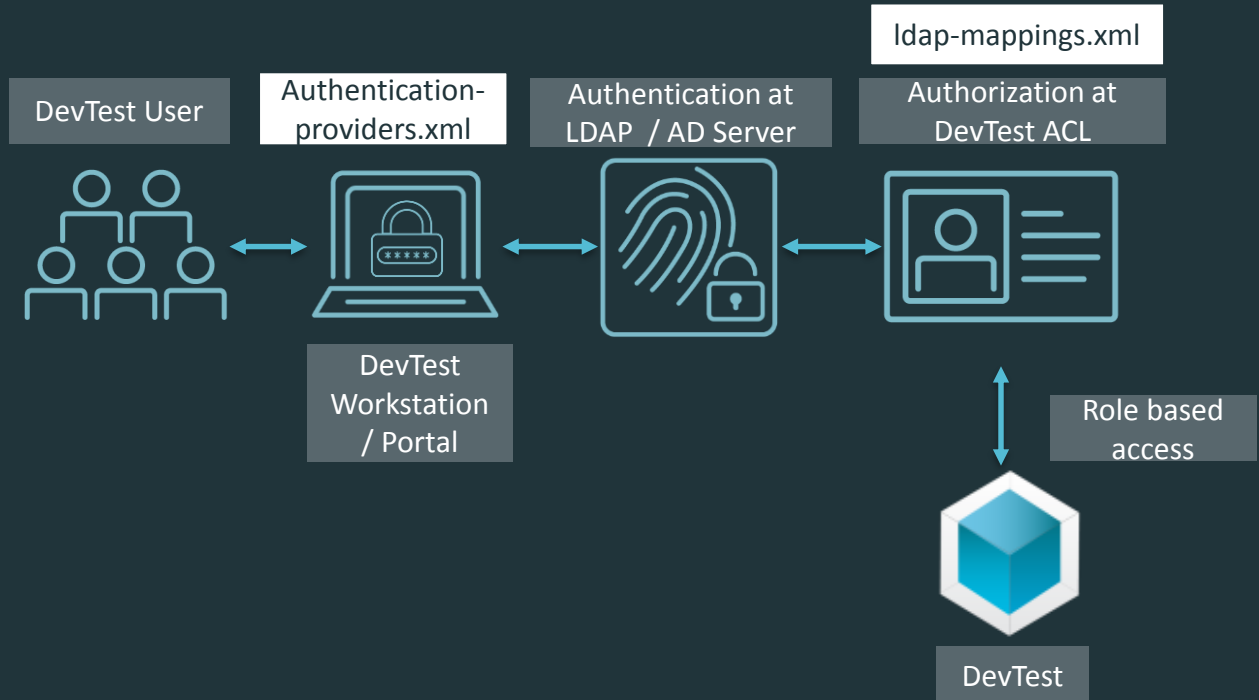- Use the same LDAP / AD passwords for DevTest
  - ACL admin no longer needs to maintain passwords

- Easier to configure and manage users for large organizations
  - Auto add for users into DevTest ACL
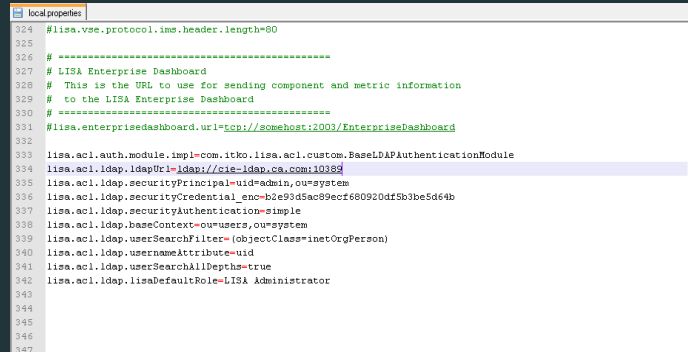
ca
technologies

How does this work?

DevTest User

Authentication-providers.xml

Authentication at LDAP / AD Server

ldap-mappings.xml

Authorization at DevTest ACL

DevTest Workstation / Portal

Role based access

DevTest

How do we configure this?

- Local.properties
  - Older method

- Properties configured
  - Ldap url
  - Ldap user and credentials
  - Base Context and user search filter
  - DefaultRole

- Remove or comment
  - lisa.acl.auth.enabled property


```
local.properties
324  #lisa.vse.protocol.ims.header.length=80
325
326  # ===========================================
327  # LISA Enterprise Dashboard
328  #  This is the URL to use for sending component and metric information
329  #  to the LISA Enterprise Dashboard
330  # ===========================================
331  #lisa.enterprisedashboard.url=tcp://somehost:2003/EnterpriseDashboard
332
333  lisa.acl.auth.module.impl=com.itko.lisa.acl.custom.BaseLDAPAuthenticationModule
334  lisa.acl.ldap.ldapUrl=ldap://cie-ldap.ca.com:10389
335  lisa.acl.ldap.securityPrincipal=uid=admin,ou=system
336  lisa.acl.ldap.securityCredential_enc=b2e93d5ac89ecf680920df5b3be5d64b
337  lisa.acl.ldap.securityAuthentication=simple
338  lisa.acl.ldap.baseContext=ou=users,ou=system
339  lisa.acl.ldap.userSearchFilter=(objectClass=inetOrgPerson)
340  lisa.acl.ldap.usernameAttribute=uid
341  lisa.acl.ldap.userSearchAllDepths=true
342  lisa.acl.ldap.lisaDefaultRole=LISA Administrator
343
344
345
346
347
```

How do we configure this?

- Authentication-providers.xml
  - Configuration of LDAP involves configuring LDAP settings
  - Providers – LDAP, Active Directory, Custom

- Ldap-mappings.xml
  - LDAP groups can be mapped against DevTest ACL user roles
  - Multiple LDAP groups can be mapped to single role

ca
technologies

Demo

ca technologies

Surya Anil Kumar Suravarapu

Sr. Engineering Services Architect

SuryaAnilKumar.Suravarapu@ca.com

@suravarapu

slideshare.net/SuryaAnilKumarSurava

linkedin.com/in/surya-suravarapu

ca.com