

LDAP/AD Integration for DevTest

Surya Anil Kumar Suravarapu

February 2017

Legal Statement

© 2017 CA. All rights reserved. CA confidential & proprietary information. For CA, CA Partner and CA Customer use only. No unauthorized use, copying or distribution. All names of individuals or of companies referenced herein are fictitious names used for instructional purposes only. Any similarity to any real persons or businesses is purely coincidental. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. These Materials are for your informational purposes only, and do not form any type of warranty. The use of any software or product referenced in the Materials is governed by the end user's applicable license agreement. CA is the manufacturer of these Materials. Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-19(c)(1)-(2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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

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

The image displays three screenshots of the DevTest Portal interface. The top screenshot shows the 'Users' management page, listing users such as 'admin', 'capower', 'devtest', 'guest', 'supower', 'sysadmin', and 'tpower'. The middle screenshot shows the 'Roles' management page, listing roles like 'Super User', 'DevTest Administrator', 'Test Administrator', 'System Administration', 'CAI Power', 'SV Power', 'Test Power', 'Runtime', 'Test Runner', 'Test Observer', and 'Load Tester'. The bottom screenshot shows the 'Role Information - SV Power' page, displaying details for the 'SV Power' role, including its description, effective user types, and a list of permissions and assignments.

Challenges with ACL

Separate passwords

Maintenance of passwords

- Especially in large organizations

Manual addition of users

User maintenance

ca technologies DevTest Portal Version: 10.0.0

User Name

Password

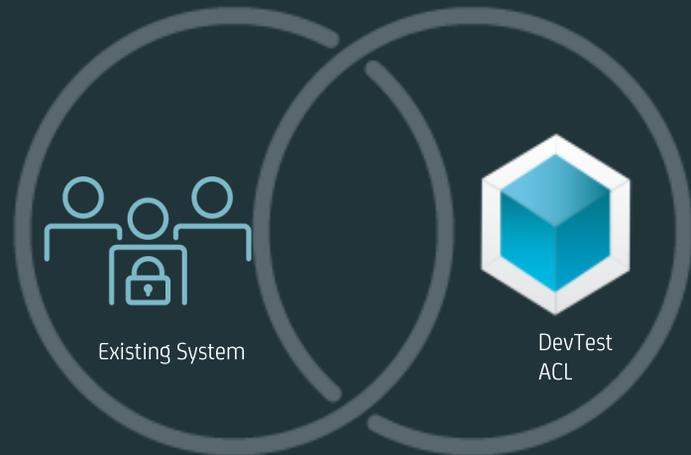
[Log in](#)

Registry: SURSU06-226:2010

<http://swagger.io>

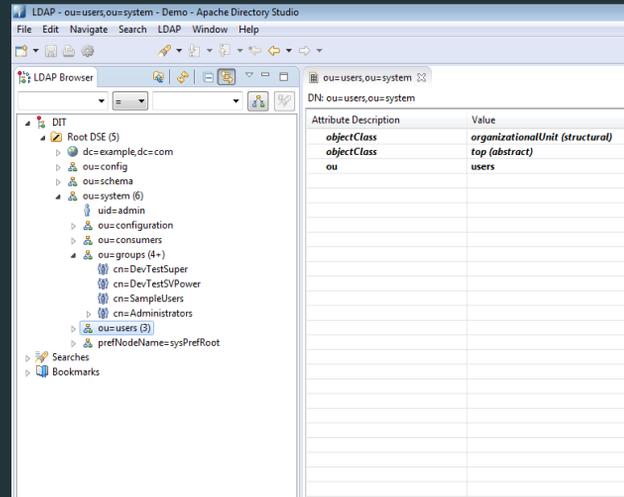
Solution

- Integration with an existing authentication mechanism
- Should work in conjunction with ACL
- Centralized management of users / passwords



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.

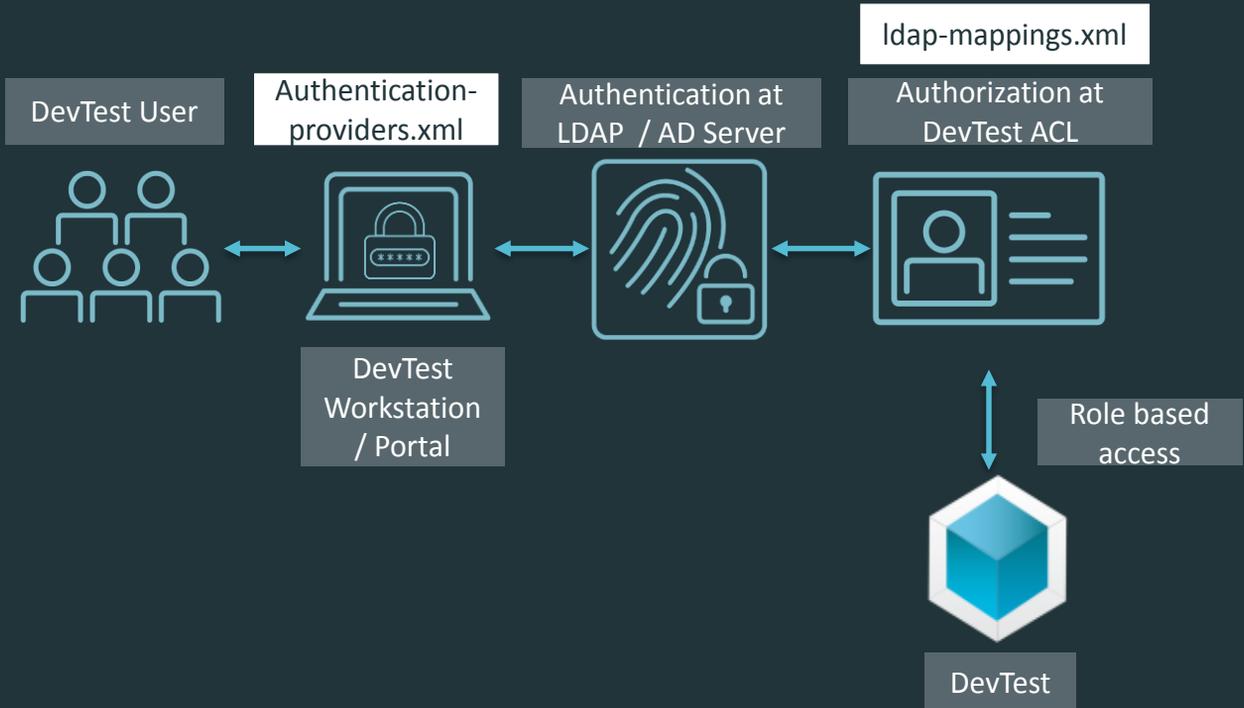


Why do we need this?

- 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



How does this work?



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=90
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=http://somehost:2003/EnterpriseDashboard
332
333 lisa.acl.auth.module.impl=com.itko.lisa.acl.custom.BaseLDAPAuthenticationModule
334 lisa.acl.ldap.ldapUri=ldap://cic-ldap.ca.com:10389
335 lisa.acl.ldap.securityPrincipal=uid=admin,ou=system
336 lisa.acl.ldap.securityCredential_enc=b2e93d5ac89ec2680920df5b3be5d64b
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

```
authentication-providers.xml
100 <authentication-provider
101   name="ITRO Authentication Module"
102   type="Legacy"
103   enabled="true"
104   defaultRole="Guest"/>
105
106 -->
107 <authentication-provider
108   name="Corp. Active Directory Server"
109   autoAddUsers="true"
110   authenticationOnly="false"
111   enabled="true"
112   type="LDAP"
113   defaultRole="SV Power"
114   executeOnapplicable="true"
115   <url>ldap://cic-ldap.ca.com:10382</url>
116   <user-dn>uid=admin,ou=system</user-dn>
117   <user-password>(crj)13ec2589b1b2f0e637a8de4a37ffc0472182c821b3bba4c94c7e42c324724d436ad2a52194e</user-password>
118   <user-dn-pattern>uid=0,ou=users,ou=system</user-dn-pattern>
119   <user-search-base>ou=users,ou=system</user-search-base>
120   <user-search-filter>(amp;(objectClass=inetOrgPerson)(uid=0))</user-search-filter>
121   <group-search-base>ou=groups,ou=system</group-search-base>
122   <group-search-filter>(member=0)</group-search-filter>
123   <authenticateOnApplicable>
124     </authenticateOnApplicable>
125 </authentication-provider>
126
```

```
ldap-mappings.xml
35 and SV Power roles assigned. Finally the "cn=users,ou=groups,dc=example,dc=com"
36 members are assigned the Test Observer role.
37 -->
38
39 <mapping role="Super User">
40   <groupDN>cn=DevTestAdmin,ou=groups,ou=system</groupDN>
41 </mapping>
42 <mapping role="DevTest Administrator">
43   <groupDN>cn=DevTestUser,ou=groups,ou=system</groupDN>
44 </mapping>
45 <mapping role="Test Administrator">
46 </mapping>
47 <mapping role="System Administration">
48 </mapping>
49 <mapping role="PE Power">
50 </mapping>
51 <mapping role="SV Power">
52 </mapping>
53 <mapping role="Test Power">
54 </mapping>
55 <mapping role="Runtime">
56 </mapping>
57 <mapping role="Test Runner">
58 </mapping>
59 <mapping role="Test Observer">
60 </mapping>
61 <mapping role="Load Tester">
62 </mapping>
63 <mapping role="User">
```



Demo





Surya Anil Kumar Suravarapu

Sr. Engineering Services Architect

SuryaAnilKumar.Suravarapu@ca.com

 [@suravarapu](https://twitter.com/suravarapu)

 slideshare.net/SuryaAnilKumarSurava

 linkedin.com/in/surya-suravarapu

ca.com