Customer

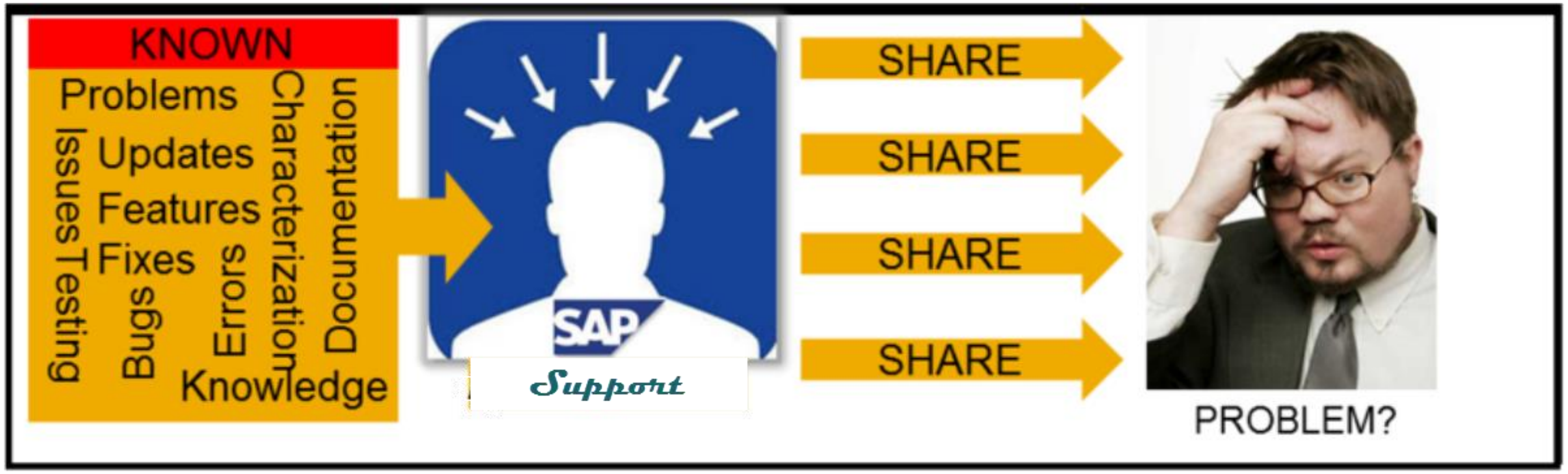
Customer Coffee Corner for SAP IQ – LDAP & SAP IQ

SAP Product Support
May, 2017

Agenda

- **Objectives**
- **LDAP user authentication**
- **FAQs**
- **LDAP testing short demo**
- **Closing remarks**
- **Open discussion**

Objectives



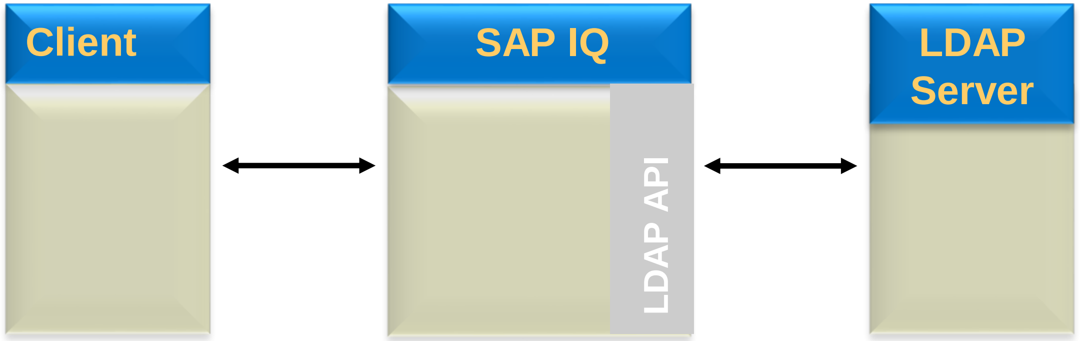
- **Proactive outreach based on feedbacks**

- **Target audience – IQ DBAs Novice/Beginner**

- **Awareness about key infrastructure process, which may help in better planning and execution avoiding “how to” IQ incidents.**

LDAP user authentication

- **What is LDAPUA ?**
  It is Lightweight Directory Access Protocol (LDAP) based user authentication.



- Users are authenticated by binding to LDAP server
- Enable customers to hook into existing enterprise infrastructures for managing users and passwords
- Enable central management of password complexity policies

LDAP user authentication – Steps to enable

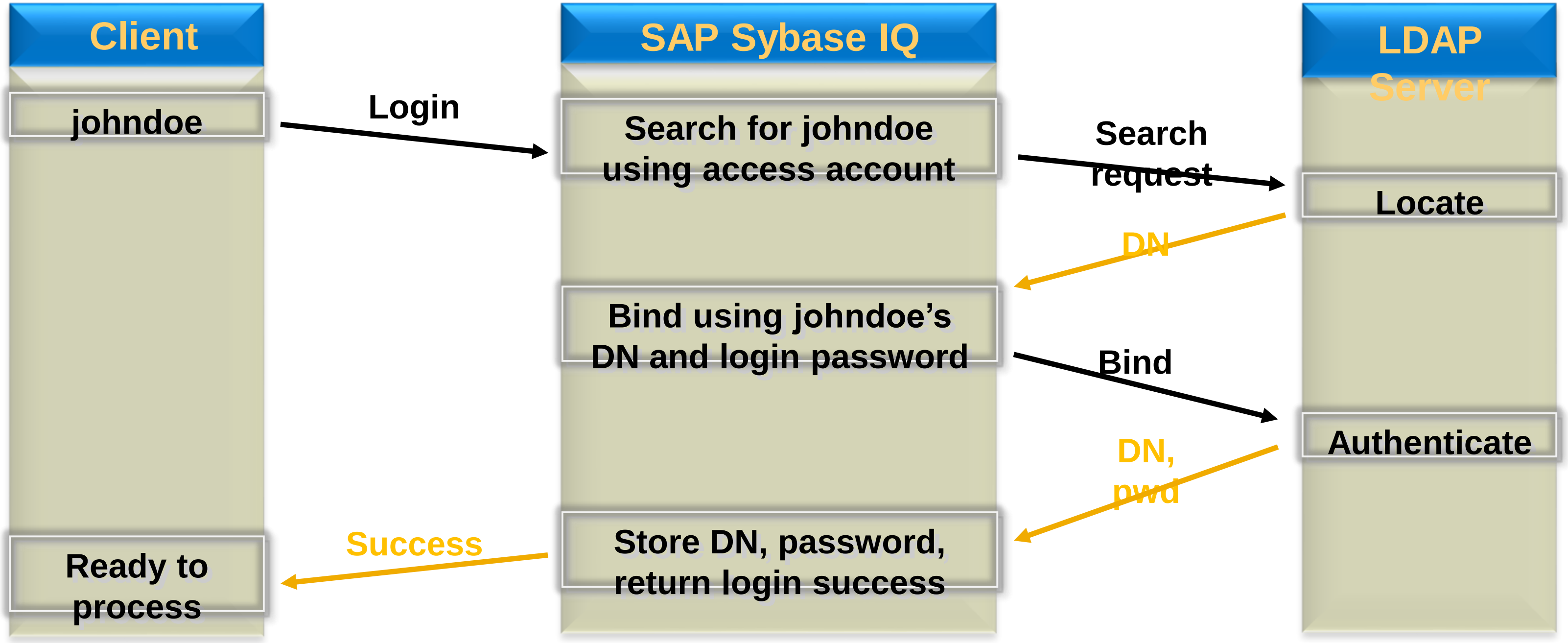
- **What are the steps to enable LDAPUA ?**
  Documentation Enabling LDAP User Authentication
  Working sample Configuring ldap connection in IQ

- **What is LDAP server configuration object ?**
  Despite its name, the LDAP server is a configuration object that resides on the SAP IQ server, rather than an actual server. Its sole function is to provide a connection to a physical LDAP server to allow LDAP user authentication.
  Any configuration of the LDAP server configuration object applies only to the SAP IQ side of the LDAP user authentication equation. LDAP server configuration object configuration settings are never written to the physical LDAP server.

- **What are the steps in creating LDAP server configuration object ?**
  - Identify the values for the applicable SEARCH DN attributes to be defined for the new LDAP server configuration object.
  - Identify the values for the applicable LDAPUA server attributes for the new LDAP server configuration object.
  - Execute the *CREATE LDAP SERVER* command, specifying the applicable attributes and clauses.

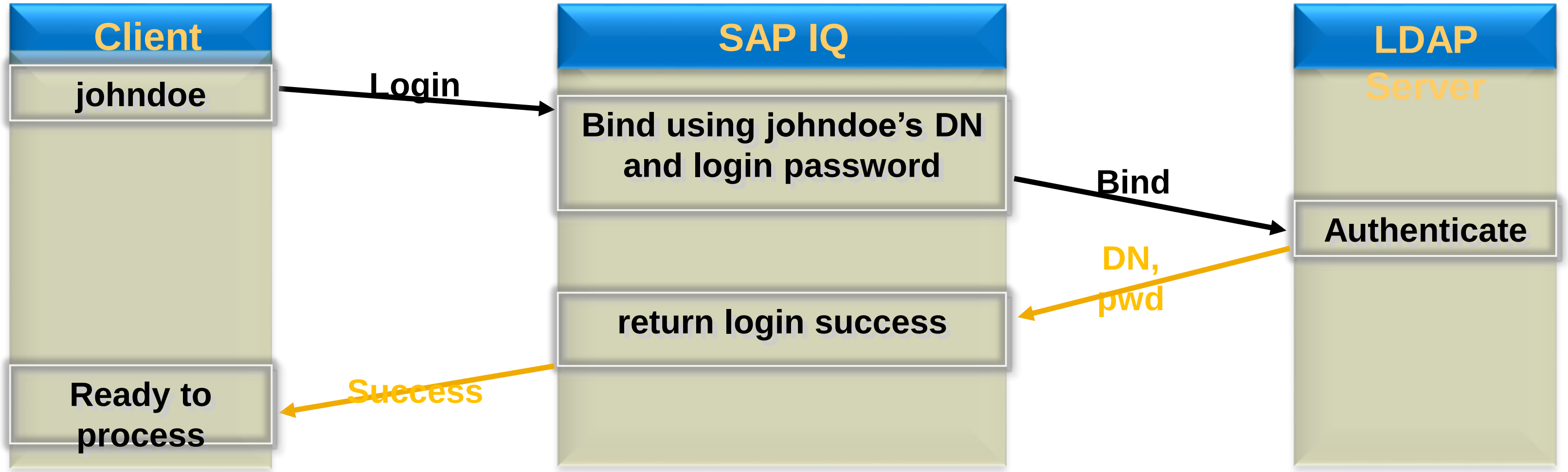
- **What is LDAP server configuration object URL ?**
  The URL identifies the host (by name or by IP address), port number, and search to be performed when executing a secure distinguished name (DN) lookup to the LDAP server.
  Syntax and parameters - ldapurl::=ldap://host:[port]/[node]?[attributes]? [base | one | sub]? [filter]

LDAP user authentication – First connect


Client
johndoe
Ready to process
Login
Success
SAP Sybase IQ
Search for johndoe using access account
Bind using johndoe's DN and login password
Store DN, password, return login success
Search request
DN
Bind
DN, pwd
LDAP Server
Locate
Authenticate

- Administrator defines LDAP URLs, specifies access account to LDAP server, and other options
- On first connection for a user, SAP Sybase IQ server searches the LDAP server for the distinguished name (DN) of the user
- SAP Sybase IQ Server binds to LDAP Server with user's DN and password to authenticate user
- On successful authentication DN and password for a user are cached in SYSUSER.

LDAP user authentication – Subsequent connects



- Cached Distinguished Name avoids repeated LDAP searches.
- Cached password allows users to connect when LDAP Servers are down.
- Efficient design for frequent, short-lived connections

LDAP user authentication – Next connect after LDAP pwd change

- Upon successful authentication with LDAP SERVER, if the specified password differs from that stored in system table ISYSUSER, the encrypted password is updated in ISYSUSER in column password.

- In the case of catastrophic failure of an LDAP SERVER or when resource limits prevent LDAPUA from working and when configuration permits, users may still authenticate with their most recently cached password using Standard authentication login_mode.

- Passwords do not change frequently so updates to ISYSUSER occur infrequently, but occur at the time of connection.

- There is a window between password cache from LDAP User Authentication and checkpoint, and *either* old or new password may continue to work. This happens because checkpoint writes to disk happen asynchronously.

Use manual checkpoint OR “alter user ldap_user_name refresh dn” commands OR have user connect connect couple of times using new ldap password

LDAP user authentication – Next connect after LDAP pwd change

Useful *AS IS* event code for refreshing USER DN periodically

```
 FOR LDAPDNLOOP AS LDAPDNCURSOR DYNAMIC SCROLL CURSOR FOR
    SELECT USER_NAME AS @LDAP_USER_NAME
    FROM SYSUSER WHERE USER_DN IS NOT NULL AND DATE(LAST_LOGIN_TIME) <>
(CURRENT DATE)
   DO
     EXECUTE IMMEDIATE 'ALTER USER ' || @LDAP_USER_NAME || ' REFRESH DN;';
   END FOR;
ALTER LDAP SERVER "aa" with refresh;
ALTER LDAP SERVER "bb" with refresh;
END;
```

LDAP user authentication – Reference ..

- **IQ startup configuration flags** (Location – Inside dbname.cfg file in directory where dbname.db resides)
  - -al - Extends LOGIN_MODE for LDAPUA only to a select 5 users using Standard authentication.
  - -hX – Undocumented verbose diagnostic tracing of LDAPUA is placed in specified file.

- **Key IQ stored procedures (** Use ># ‘file’ which makes output readable and loadable **)**
  - sa_get_ldapserver_status - shows current status of the LDAP server configuration object.
  - sa_get_user_status – Shows current state of all users.

- **Key IQ views (** Use ># ‘file’ which makes output readable and loadable **)**
  - SYSLDAPSERVER - shows attributes for the LDAP server..

- **Key LDAP server commands**
  - DROP LDAP Server
  - CREATE LDAP Server
  - ALTER LDAP Server
  - VALIDATE LDAP Server
  - CREATE LOGIN POLICY

FAQs

- Where can I find standard for LDAP URL format ? LDAP URL Standard

- Which common LDAP vendors are supported ? Active Directory (AD), Tivoli, SunONE Oracle DS, and OpenLDAP

- Do I need license to use LDAPUA ?

  LDAP authentication is part of IQ's Advanced Security option.
  If the customer purchases Adaptive Server Platform (bundles IQ, ASE, and RepServer - you can buy core licenses of any subset of these), then the advanced security option for IQ is included.

- What different types of external authorization IQ support ? LDAPUA , Kerberos , PAM

- Is there any difference between login_mode value ‘Standard,LDAPUA’ and ‘LDAPUA,Standard ?

  No. LDAP authentication is attempted before Standard authentication when both are permitted by login_mode and login policy settings.

- How to use secured LDAP ? Enabling secured LDAP

FAQs

- If DN (Distinguished Name) lookup is failing, which external tools can be used to determine potential problem with DN construction ?

  ldapsearch – Command line linux tool
  Jexplorer - general purpose LDAP client that can be used to search, read and edit any standard LDAP directory, or any directory service with an LDAP or DSML interface.
  ** You may need permissions or work with together with ldap admin.

- Can I use multiple ldap servers for different user groups?

  Yes. Create different login policies using different LDAP servers for authentication.

- Can IQ handle High Availability user authentication with multiple LDAP servers ?

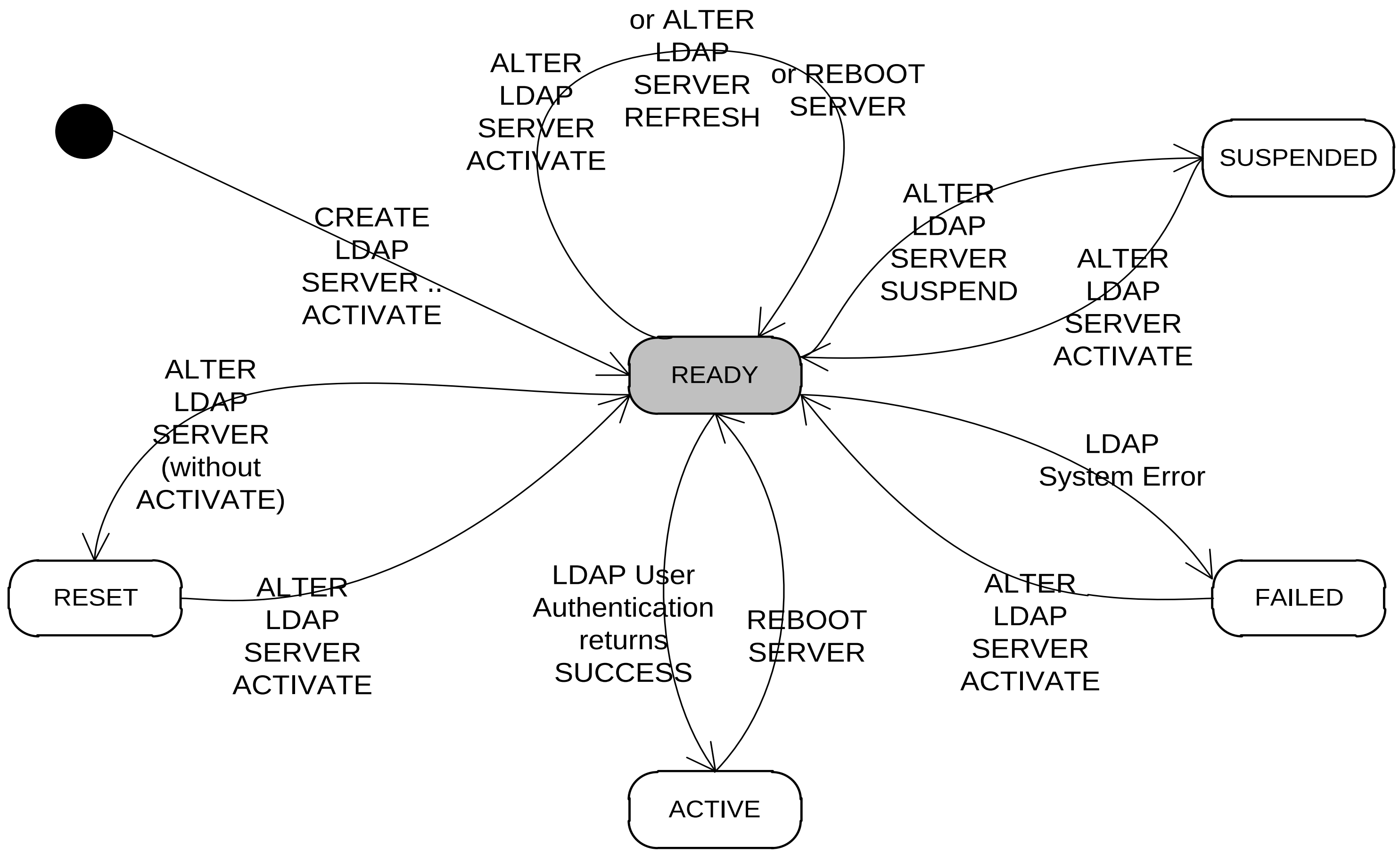
  Yes. login policy may specify a primary/secondary LDAP server pair
  Automatic failover from primary to secondary when primary LDAP Server is down
  Automatic or manual failback to primary when primary activates again

- . Can login policy control authentication mode standard/LDAPUA?

  No. Database option login_mode controls authentication mode combinations.

FAQs

- How LDAP server states transition ?



or ALTER LDAP SERVER REFRESH
ALTER LDAP SERVER ACTIVATE
or REBOOT SERVER
SUSPENDED
CREATE LDAP SERVER .. ACTIVATE
ALTER LDAP SERVER SUSPEND
ALTER LDAP SERVER ACTIVATE
READY
ALTER LDAP SERVER (without ACTIVATE)
LDAP System Error
RESET
ALTER LDAP SERVER ACTIVATE
LDAP User Authentication returns SUCCESS
REBOOT SERVER
ALTER LDAP SERVER ACTIVATE
FAILED
ACTIVE

LDAP testing short demo

– Demo Transcript study

  - Working sql sequence

  - Error scenarios with –hX trace snippet –

    BAD Distinguished name DN
    BAD LDAP URL node
    BAD LDAP URL filter

KBA’s - specific to today’s topic

1911807 Errors when trying to login using LDAP

1934407 IQ 16.0 support for Kerberos / LDAP authentication (Active Directory)

1938510 How to setup LDAP (Active Directory) for Sybase Control Center (SCC) user authentication. -- SAP IQ

2140693 The specified distinguished name '%1' does not match the search result '%2' -SAP IQ

2163441 The search on LDAP server completed with no matching results - SAP IQ

2269928 Why enduser gets error [Could not load dynamic library 'libsybaseldap64.so'] and why there are several versioned ldap libraries ?

KBA’s - product specific

2309381 – Customer Virtual Coffee corner for ASE, IQ, Replication Server, Software Developers Kit …
2137179 – Customer Coffee Corner for SAP IQ – Americas

1910965 IQ 15.x / 16 - Restore of an IQ database from a backup failed with Msg 13720
1984346 How to monitor memory usage and CPU per connection - SAP IQ
2013615 Installation SCC java.lang.UnsatisfiedLinkError: no dbjodbc11 in java.library.path:SAP IQ
2026768 How to migrate an user and password into a new system.
2088457 An IQ secondary server gets unresponsive while running heavy DMLs and doing a checkpoint.
2114371 Cannot add a partition or subpartition to table - SAP IQ
2125122 Certifications on Red Hat Linux 7 and Oracle Solaris 11 - SAP IQ 16.x
2126584 An incorrect result returned when using HPDJ - SAP IQ
2142537 How to identify connections and queries involved in high temp space usage - SAP IQ
2192748 All IQ large memory has been used while running a load table - SAP IQ
2198121 When is the end of life support date for SAP IQ15x / IQ 16x : IQ

Closing Remarks

- What’s next ?

- Please provide your feedback to IQ VCC coordinators on
  - Did you learn something new/useful ?
  - Did this outreach help understanding IQ and LDAP ?

Any Questions ?

Thank you