

Building Powerful LDAP Configurations

Jon Sue-Ho
Support Specialist



Agenda

A Word on Coexistence - LDAP with both InterSystems IRIS and Caché/Ensemble

A Story of Excessive Success

Quick Overview of LDAP and LDAP Configs

Cool New Things

- Multiple Domains (more users from more orgs)
- Authorization Group and Instance IDs (more granular security)

Demo



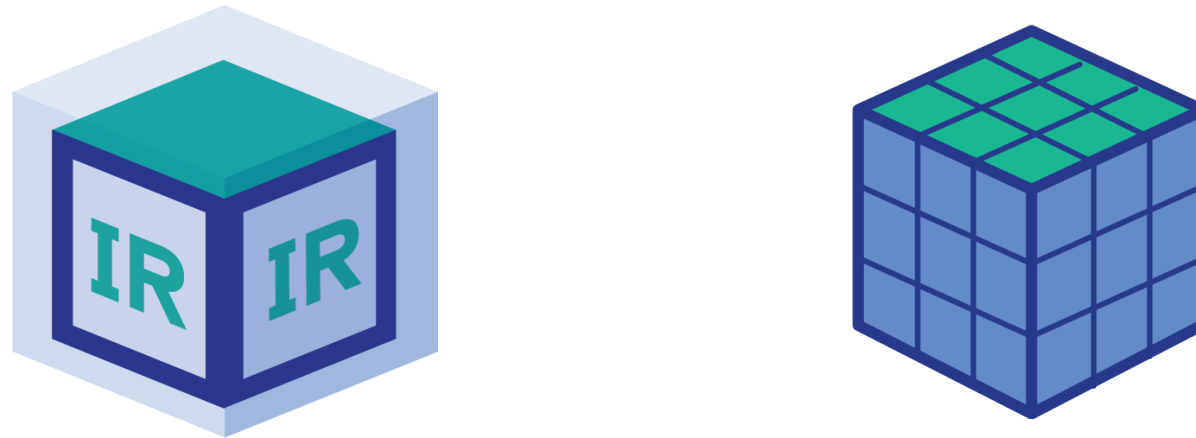
Coexistence

You may want/need mixed environments with InterSystems IRIS and Caché/Ensemble

Certain technology will be kept compatible between them for future releases

LDAP will be one of those technologies, so LDAP functionality in future InterSystems IRIS releases will also be available in future Caché/Ensemble releases

A common method for authentication between the different types of instances!



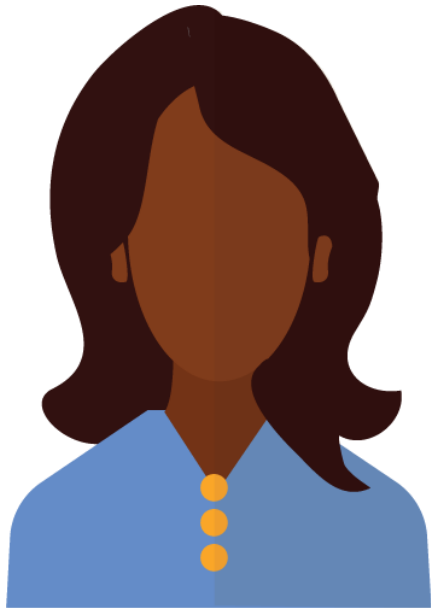
A Story of Excessive Success

Why you need LDAP

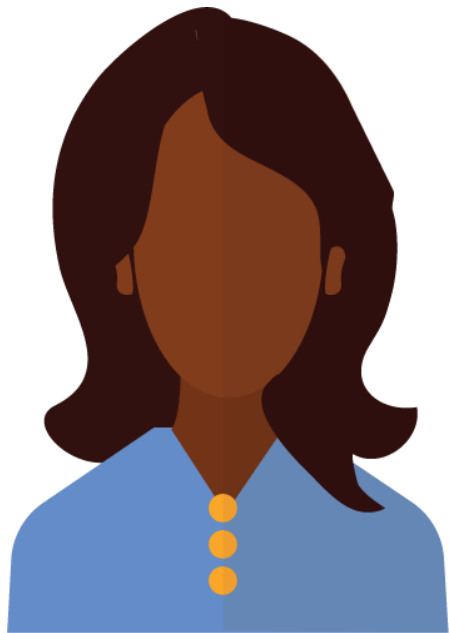












Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

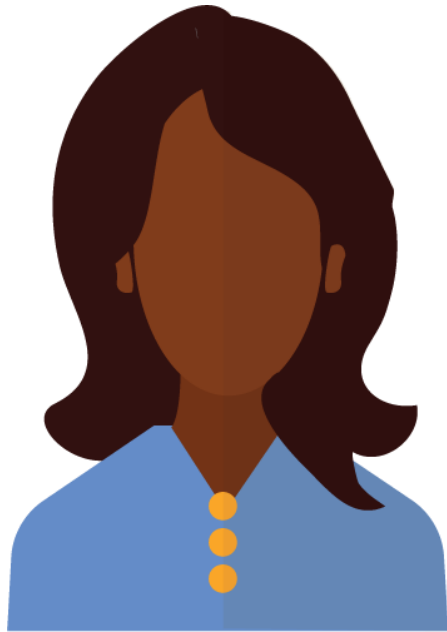
Available		Selected
----- Select One or More -----		----- Select One or More -----
%All		
%DB_%DEFAULT		
%DB_ENSLIB		
%DB_IRISAUDIT		
%DB_IRISLIB		
%DB_IRISLOCALDATA		
%DB_IRISSYS		
%DB_IRISTEMP		
%DB_USER		
%Developer		
%EnsRole_Administrator		
%EnsRole_AlertAdministrator		
%EnsRole_AlertOperator		
%EnsRole_Developer		

[Assign](#)

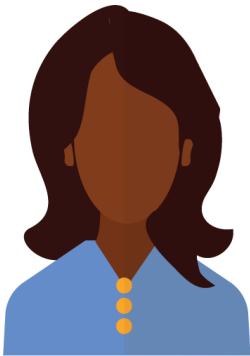
[Assign with Grant Option](#)

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.









Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Select One or More

Available

Selected

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Select One or More

Available

Selected

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Select One or More

Available

Selected

Assign

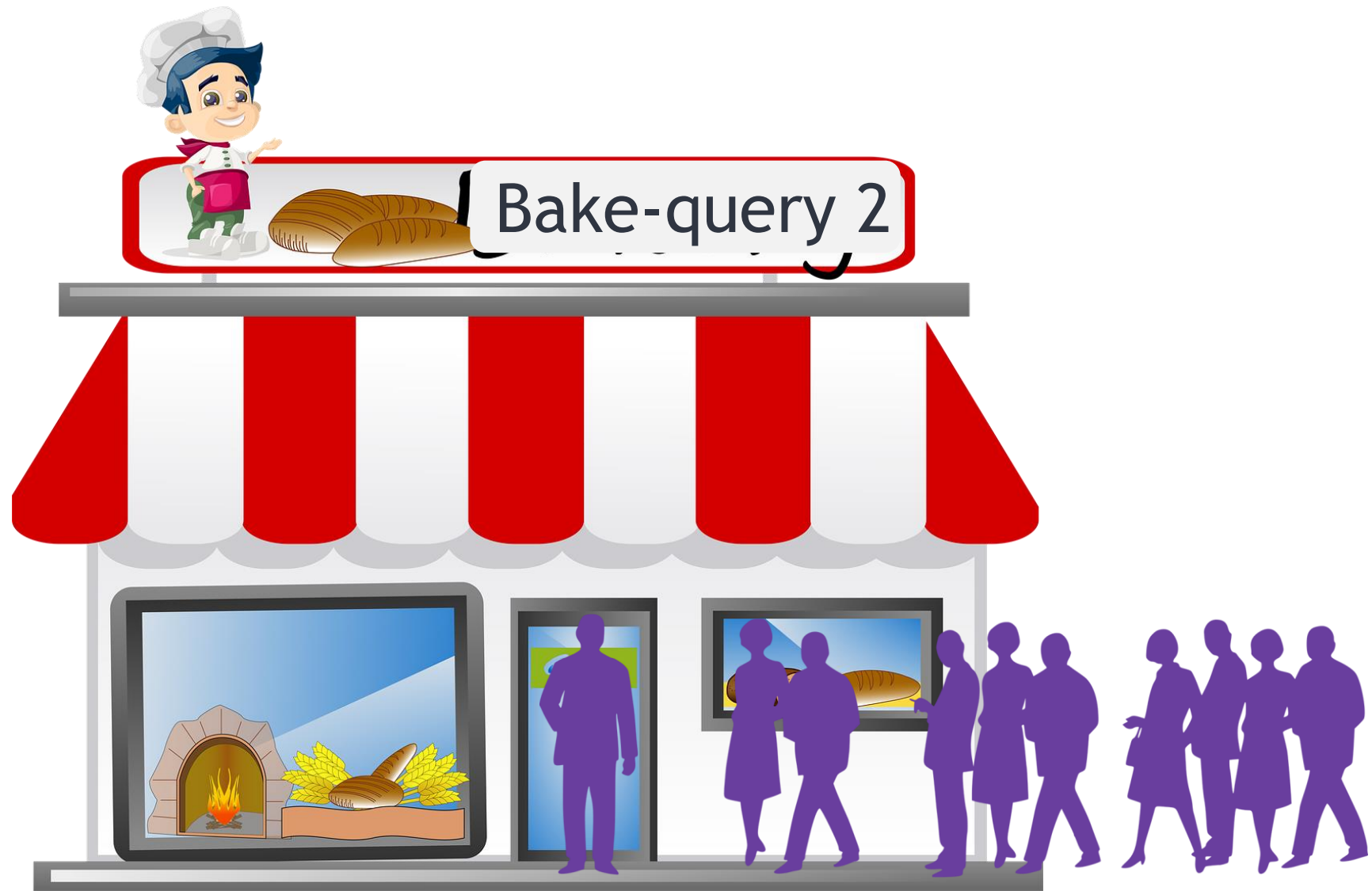
Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

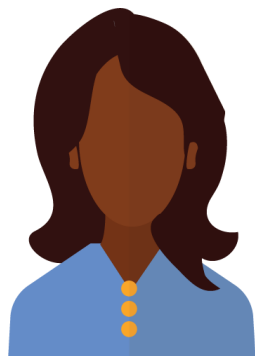












Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

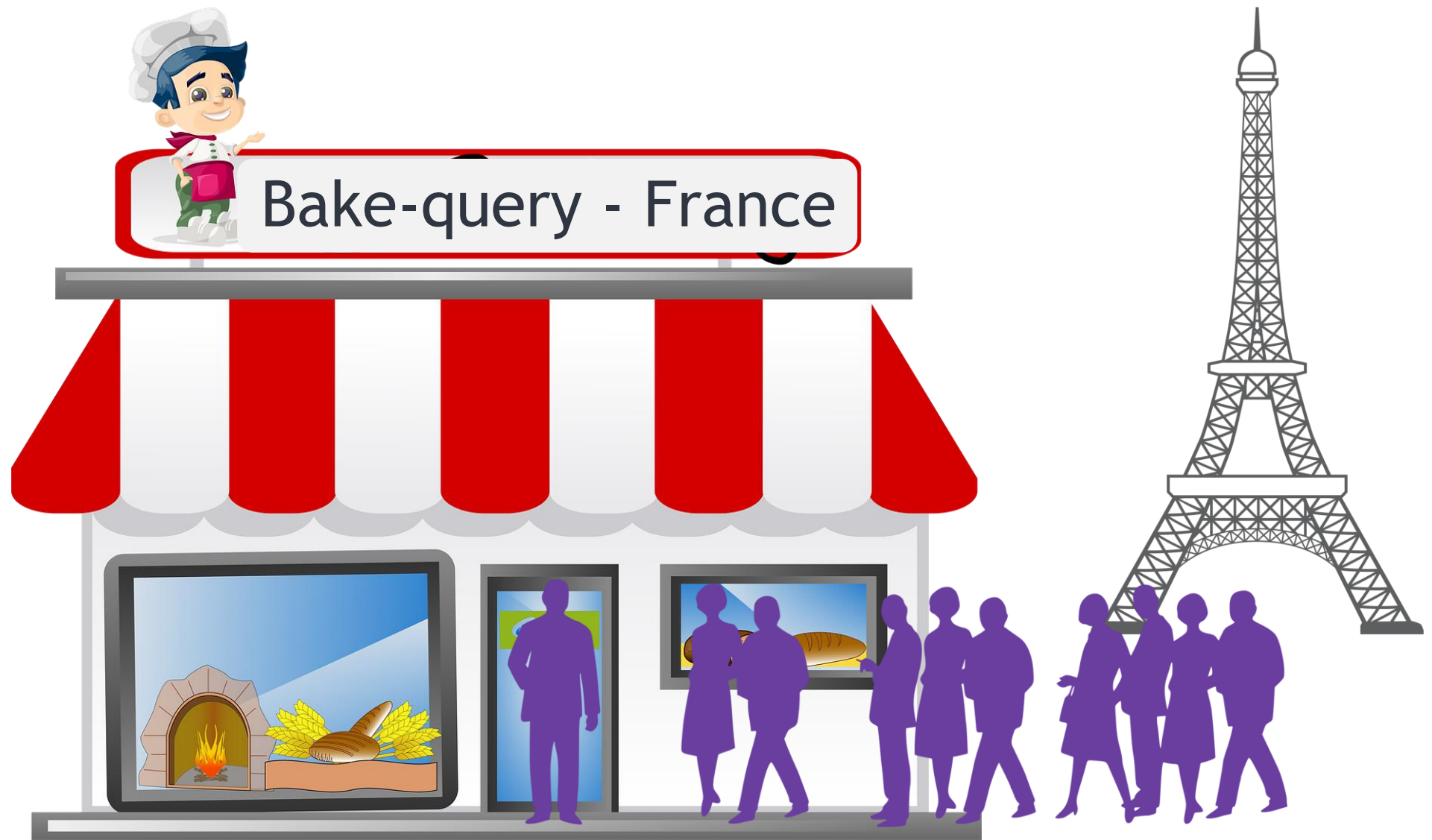
Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.











Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available

Select One or More

- %All
- %DB_%DEFAULT
- %DB_ENSLIB
- %DB_IRISAUDIT
- %DB_IRISLIB
- %DB_IRISLOCALDATA
- %DB_IRISSYS
- %DB_IRISTEMP
- %DB_USER
- %Developer
- %EnsRole_Administrator
- %EnsRole_AlertAdministrator
- %EnsRole_AlertOperator
- %EnsRole_Developer

Selected

Select One or More

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available

Select One or More

- %All
- %DB_%DEFAULT
- %DB_ENSLIB
- %DB_IRISAUDIT
- %DB_IRISLIB
- %DB_IRISLOCALDATA
- %DB_IRISSYS
- %DB_IRISTEMP
- %DB_USER
- %Developer
- %EnsRole_Administrator
- %EnsRole_AlertAdministrator
- %EnsRole_AlertOperator
- %EnsRole_Developer

Selected

Select One or More

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available

Select One or More

- %All
- %DB_%DEFAULT
- %DB_ENSLIB
- %DB_IRISAUDIT
- %DB_IRISLIB
- %DB_IRISLOCALDATA
- %DB_IRISSYS
- %DB_IRISTEMP
- %DB_USER
- %Developer
- %EnsRole_Administrator
- %EnsRole_AlertAdministrator
- %EnsRole_AlertOperator
- %EnsRole_Developer

Selected

Select One or More

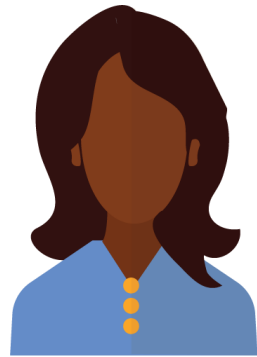
Assign

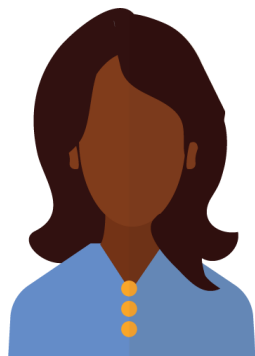
Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.









Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

Name New User
Required

Full Name

Comment

Password Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag/Routine

Email Address

Mobile Phone Service Provider Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available	Selected
Select One or More	Select One or More
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	

Assign

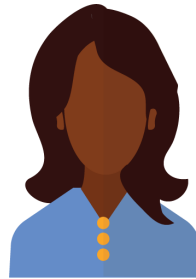
Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.





2



Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag*Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

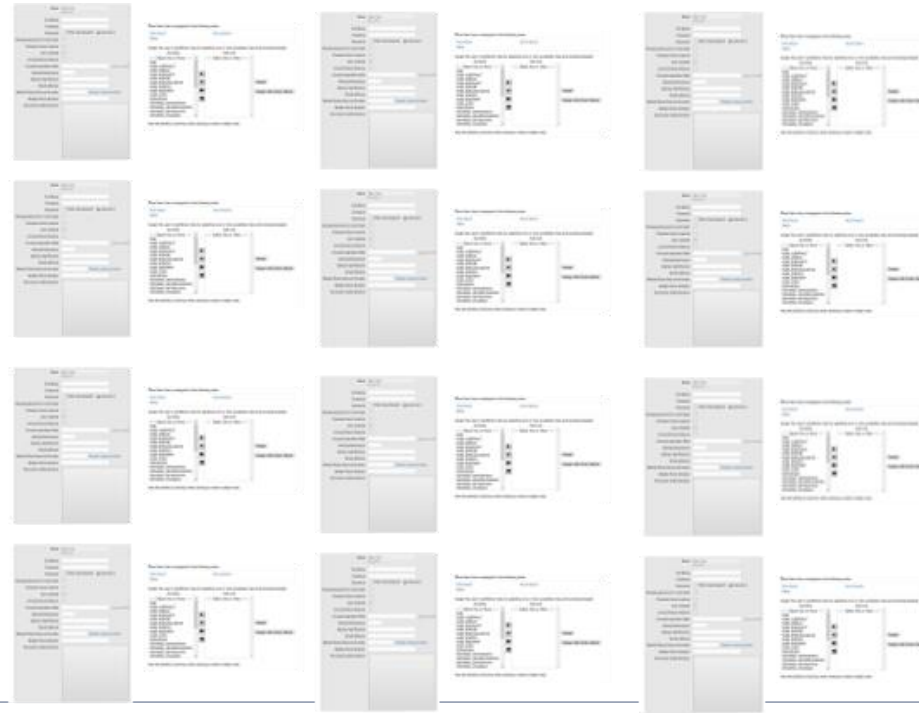
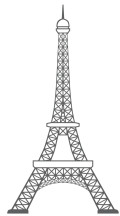
Available	Selected
----- Select One or More -----	----- Select One or More -----
%All %DB_%DEFAULT %DB_ENSLIB %DB_IRISAUDIT %DB_IRISLIB %DB_IRISLOCALDATA %DB_IRISSYS %DB_IRISTEMP %DB_USER %Developer %EnsRole_Administrator %EnsRole_AlertAdministrator %EnsRole_AlertOperator %EnsRole_Developer	
	Assign Assign with Grant Option

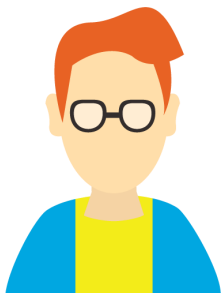
Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.





2



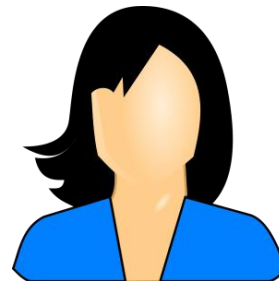
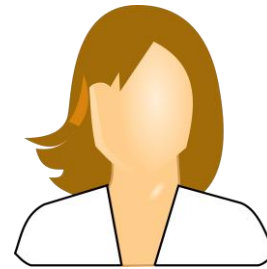








Windy Hair Consultants



NameNew User
Required.

Full Name

Comment

Password

Enter new password

Leave as is

Change password on next login

Password never expires

User enabled

Account Never Expires

Account expiration Date

(yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider

Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available

Selected

----- Select One or More -----

%All
%DB_%DEFAULT
%DB_ENSLIB
%DB_IRISAUDIT
%DB_IRISLIB
%DB_IRISLOCALDATA
%DB_IRISSYS
%DB_IRISTEMP
%DB_USER
%Developer
%EnsRole_Administrator
%EnsRole_AlertAdministrator
%EnsRole_AlertOperator
%EnsRole_Developer

----- Select One or More -----

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.



Test Kitchen



Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available		Selected
----- Select One or More -----		----- Select One or More -----
%All		
%DB_%DEFAULT		
%DB_ENSLIB		
%DB_IRISAUDIT		
%DB_IRISLIB		
%DB_IRISLOCALDATA		
%DB_IRISSYS		
%DB_IRISTEMP		
%DB_USER		
%Developer		
%EnsRole_Administrator		
%EnsRole_AlertAdministrator		
%EnsRole_AlertOperator		
%EnsRole_Developer		

Assign

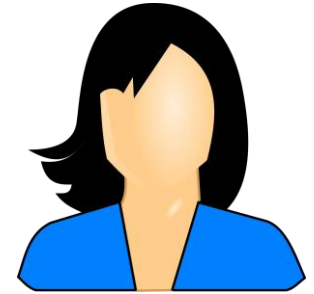
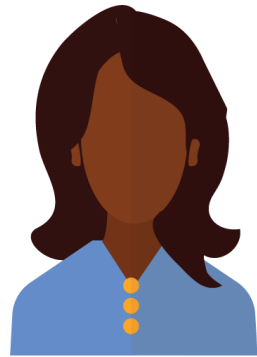
Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.



Analytics Instance

Look for holes in
business performance



NameNew User
Required.

Full Name

Comment

Password

Enter new password

Leave as is

Change password on next login

Password never expires

User enabled

Account Never Expires

Account expiration Date

(yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider

Create a new provider

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available

Selected

----- Select One or More -----

%All
%DB_%DEFAULT
%DB_ENSLIB
%DB_IRISAUDIT
%DB_IRISLIB
%DB_IRISLOCALDATA
%DB_IRISSYS
%DB_IRISTEMP
%DB_USER
%Developer
%EnsRole_Administrator
%EnsRole_AlertAdministrator
%EnsRole_AlertOperator
%EnsRole_Developer

----- Select One or More -----

Assign

Assign with Grant Option

Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.



Appetizers



Appetizers

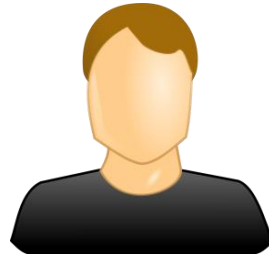
ECP App Server



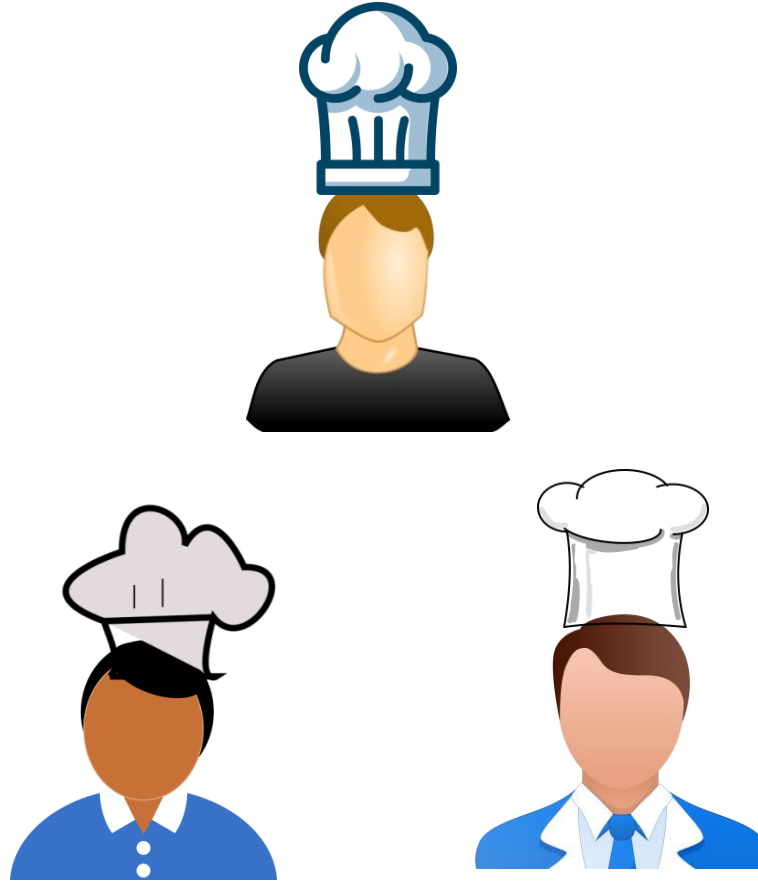
ECP App Server



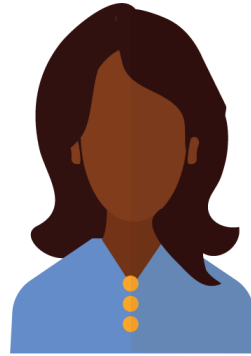
Waiters from an outside firm



Balding Waiters from an outside firm



App Servers



Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

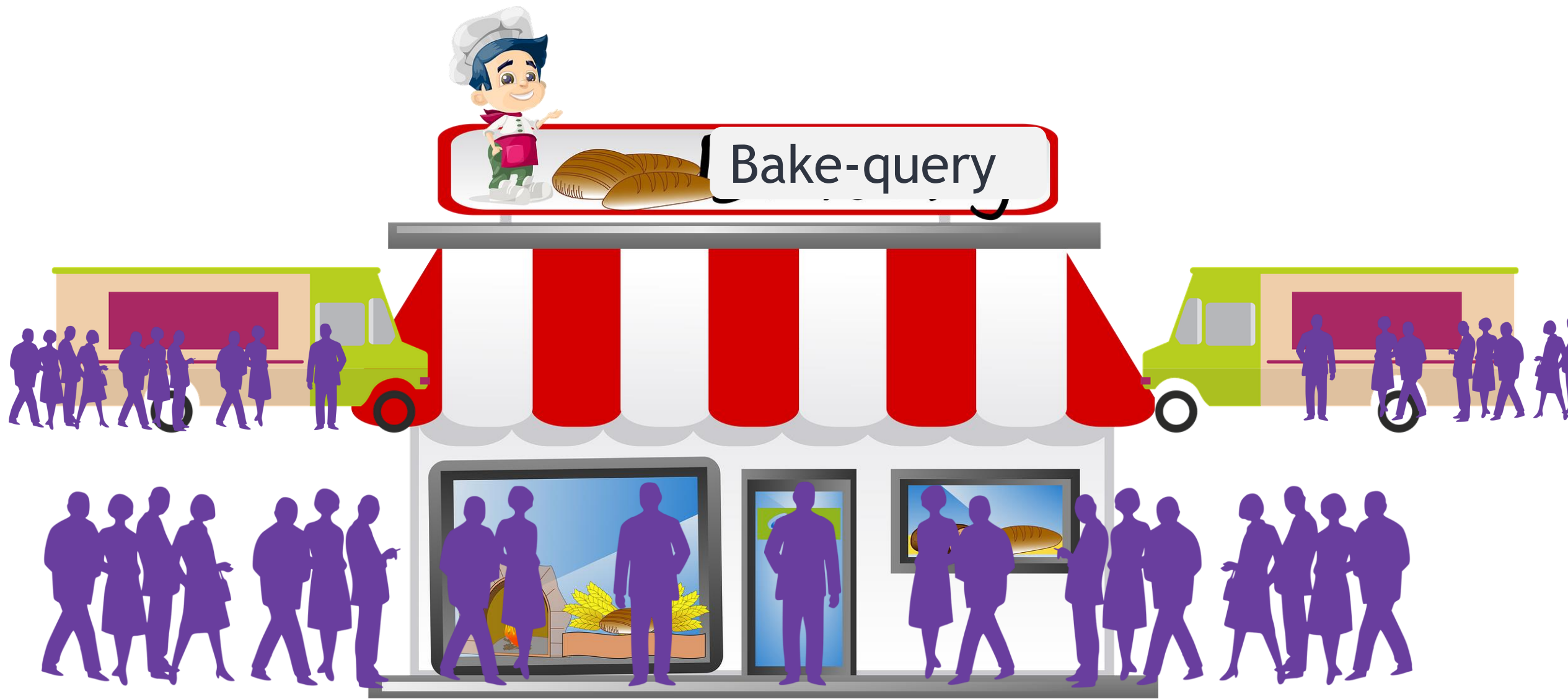
Available		Selected
----- Select One or More -----		----- Select One or More -----
%All		
%DB_%DEFAULT		
%DB_ENSLIB		
%DB_IRISAUDIT		
%DB_IRISLIB		
%DB_IRISLOCALDATA		
%DB_IRISSYS		
%DB_IRISTEMP		
%DB_USER		
%Developer		
%EnsRole_Administrator		
%EnsRole_AlertAdministrator		
%EnsRole_AlertOperator		
%EnsRole_Developer		

Assign

Assign with Grant Option

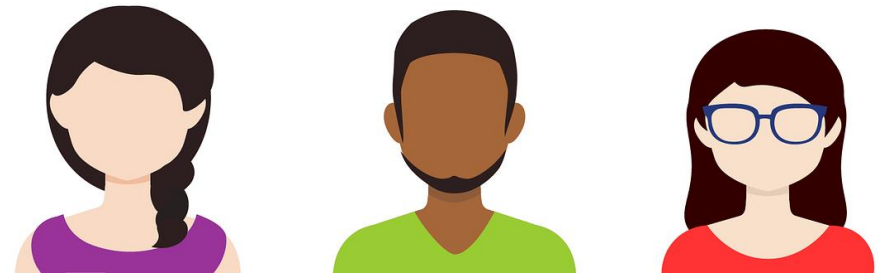
Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.













Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

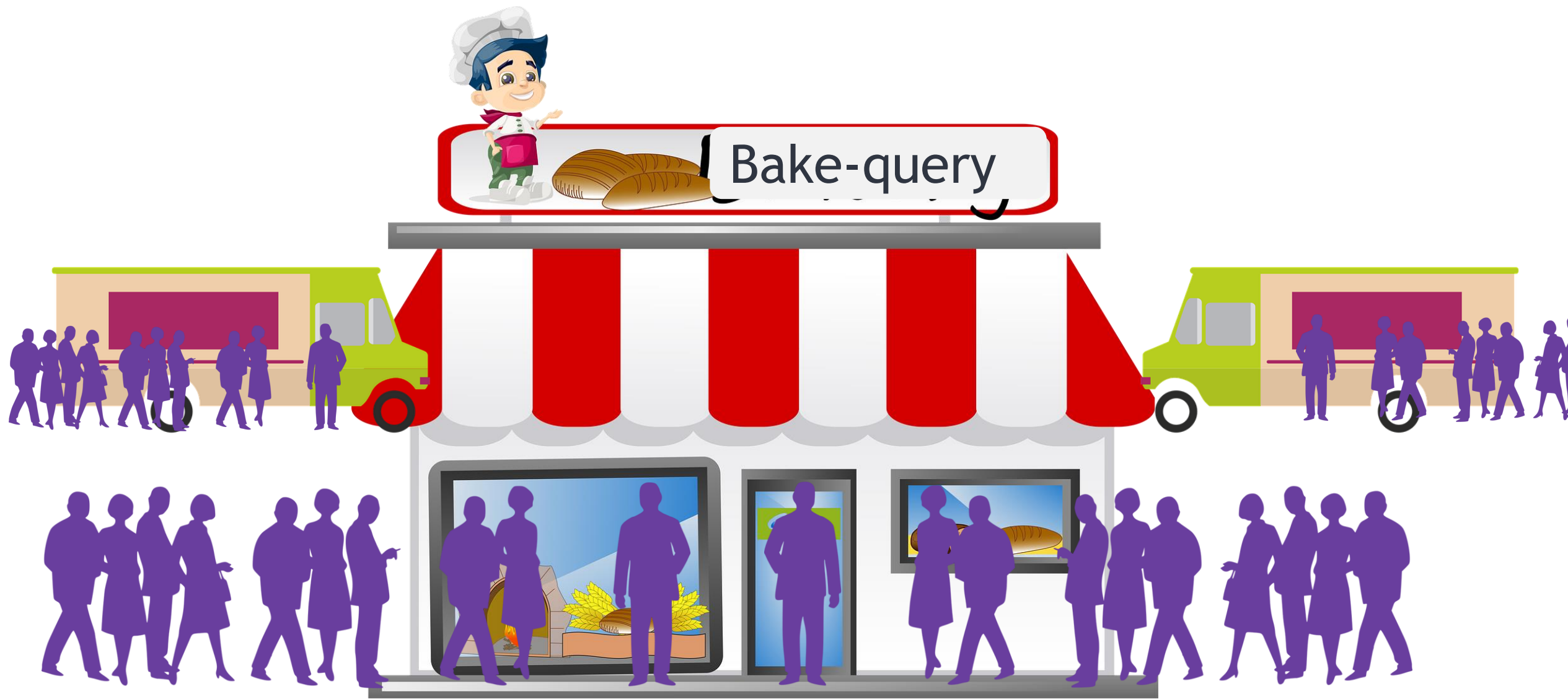
Available		Selected
----- Select One or More -----		----- Select One or More -----
%All		
%DB_%DEFAULT		
%DB_ENSLIB		
%DB_IRISAUDIT		
%DB_IRISLIB		
%DB_IRISLOCALDATA		
%DB_IRISSYS		
%DB_IRISTEMP		
%DB_USER		
%Developer		
%EnsRole_Administrator		
%EnsRole_AlertAdministrator		
%EnsRole_AlertOperator		
%EnsRole_Developer		

Assign

Assign with Grant Option

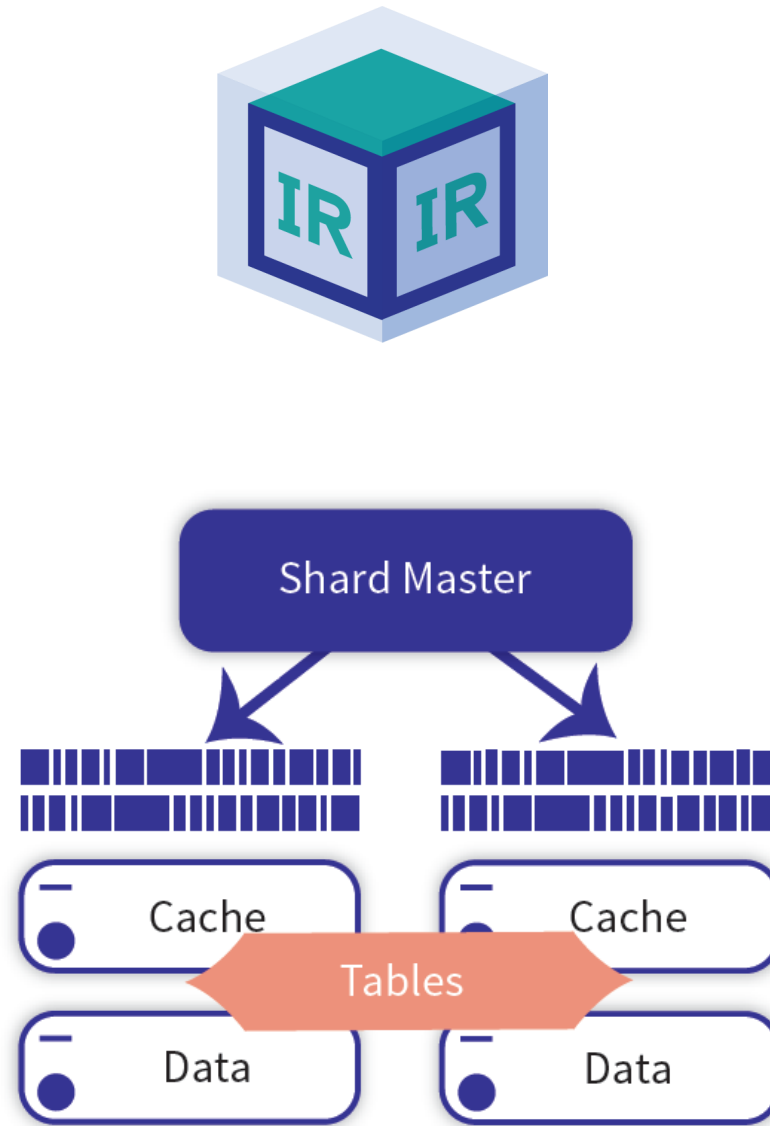
Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.



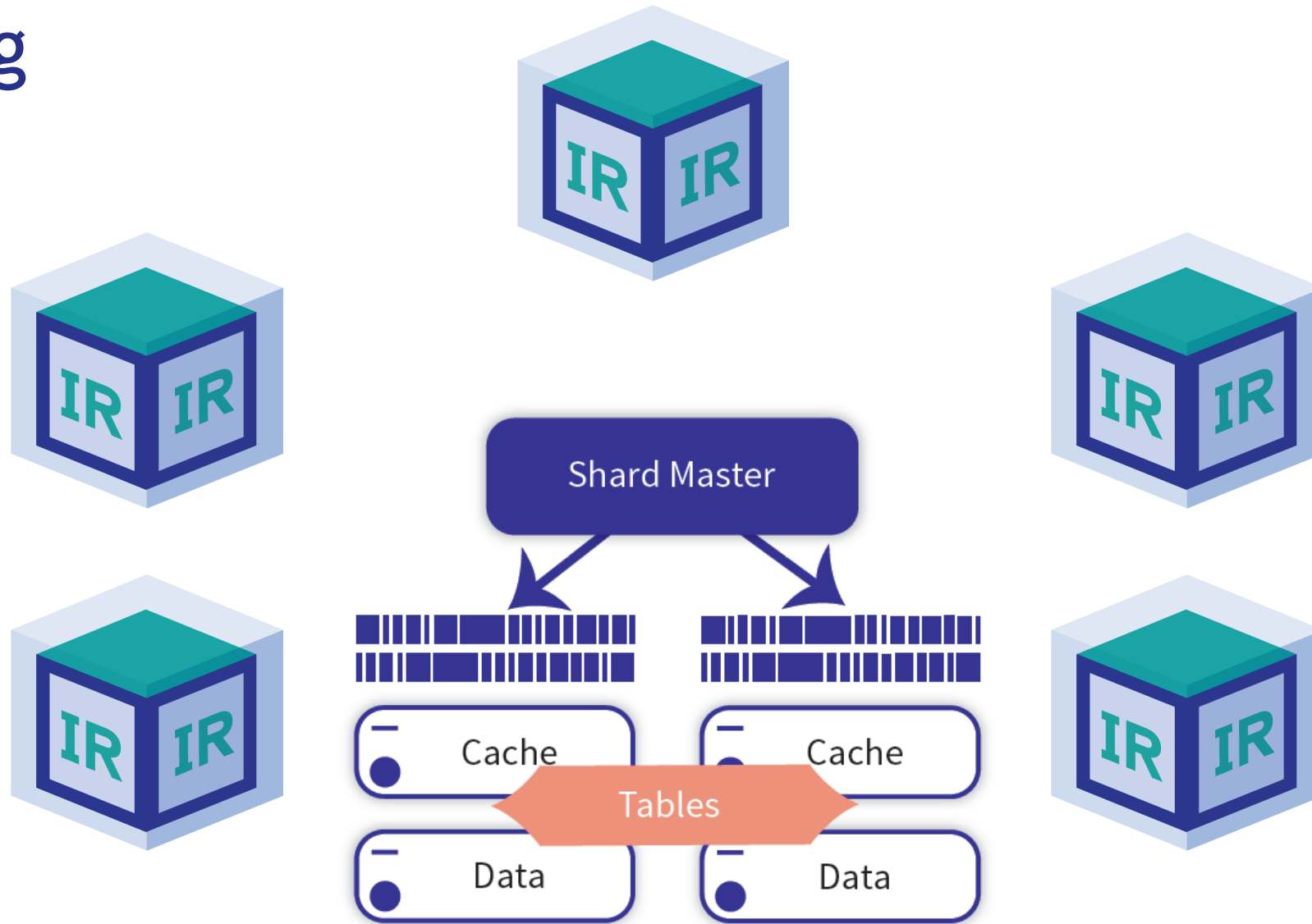




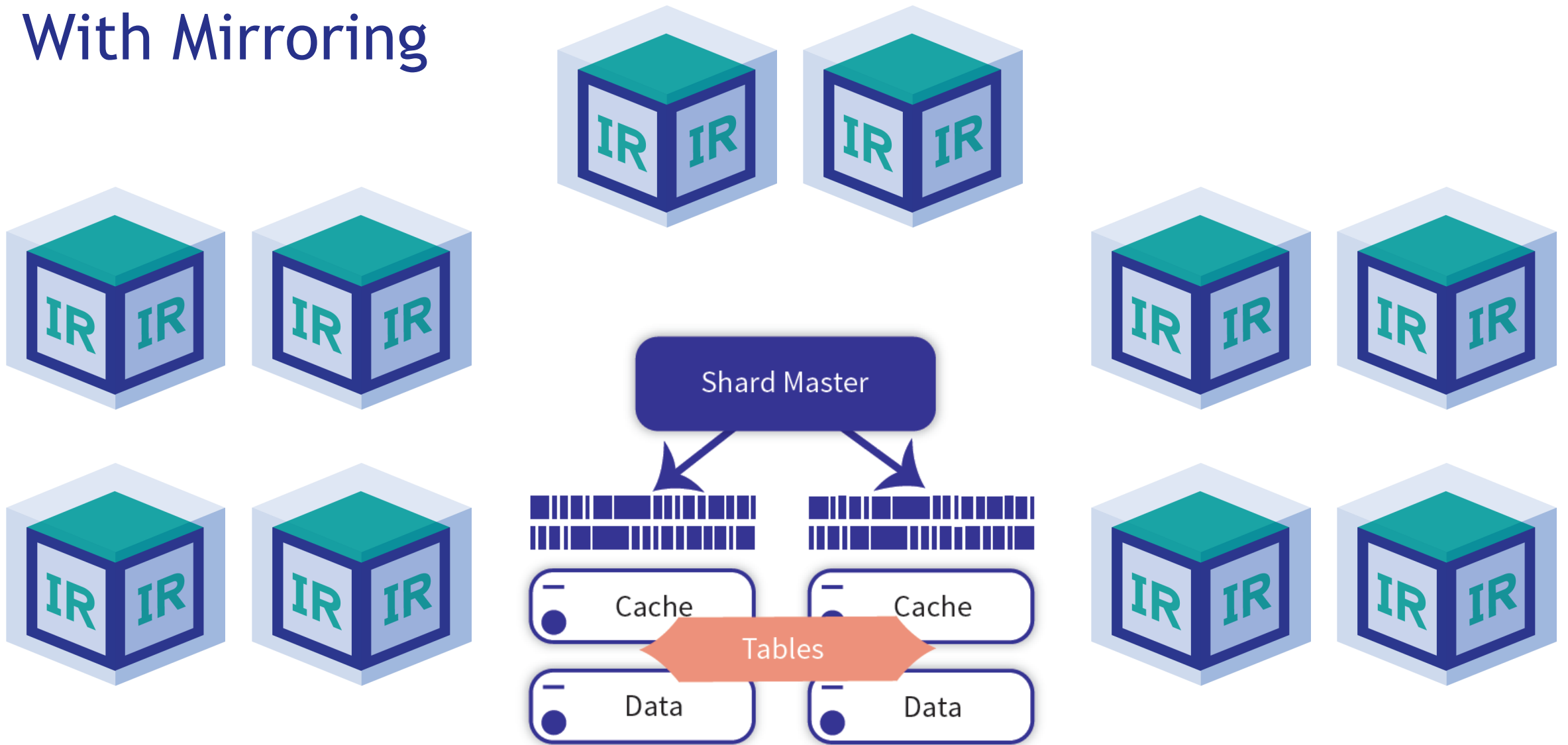
Sharding



Sharding



With Mirroring



Name New User
Required.

Full Name

Comment

Password ☐ Enter new password ☒ Leave as is

Change password on next login ☐

Password never expires ☐

User enabled ☒

Account Never Expires ☐

Account expiration Date (yyyy-mm-dd)

Startup Namespace

Startup Tag^Routine

Email Address

Mobile Phone Service Provider [Create a new provider](#)

Mobile Phone Number

Two-factor Authentication

User New User is assigned to the following roles:

Role Name	Grant Option
None.	

Assign the user to additional roles by selecting one or more available roles and pressing [Assign].

Available		Selected
----- Select One or More -----		----- Select One or More -----
%All		
%DB_%DEFAULT		
%DB_ENSLIB		
%DB_IRISAUDIT		
%DB_IRISLIB		
%DB_IRISLOCALDATA		
%DB_IRISSYS		
%DB_IRISTEMP		
%DB_USER		
%Developer		
%EnsRole_Administrator		
%EnsRole_AlertAdministrator		
%EnsRole_AlertOperator		
%EnsRole_Developer		

Assign

Assign with Grant Option

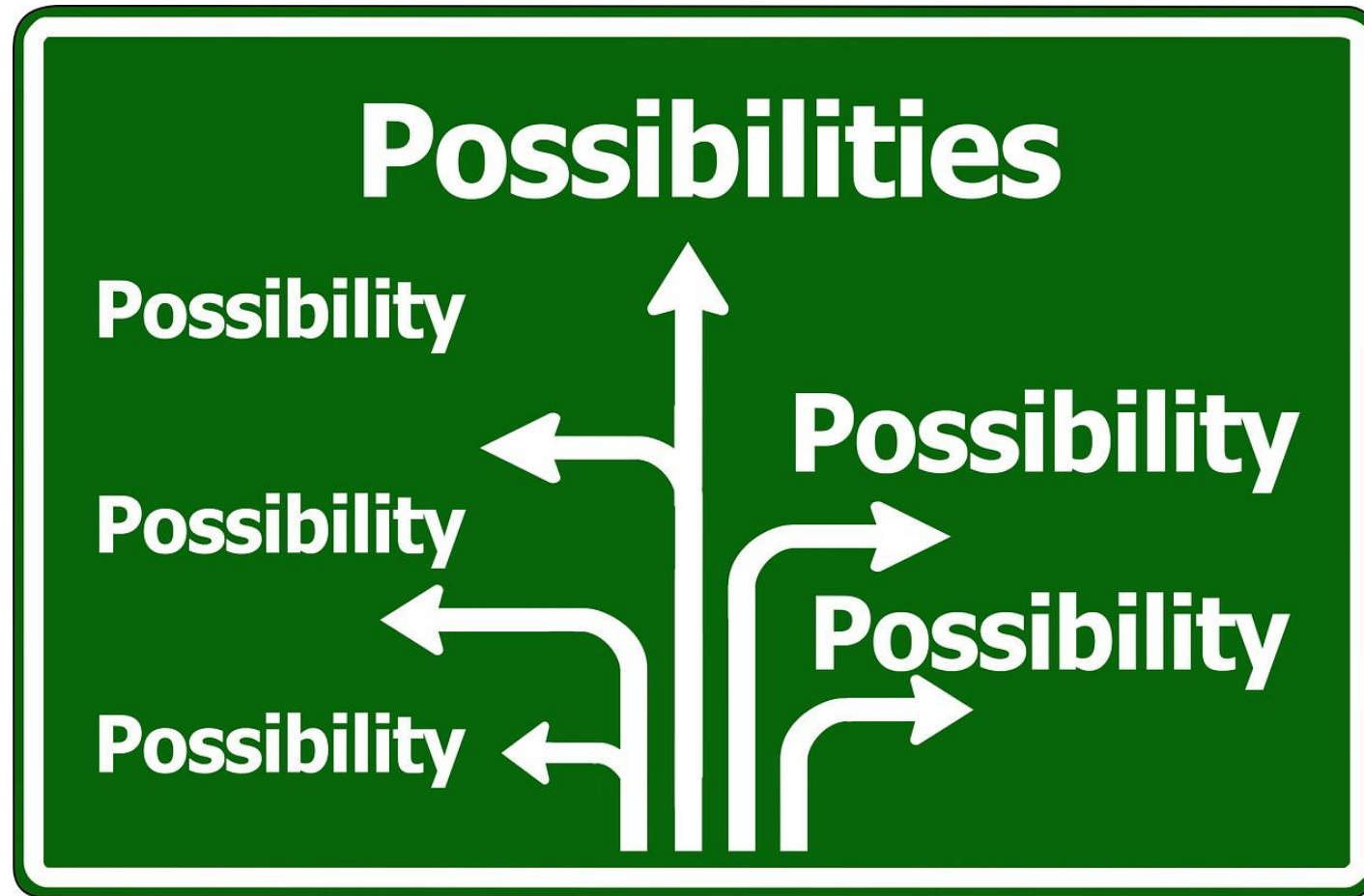
Hold the [Shift] or [Ctrl] key while clicking to select multiple roles.







There is a better way



Keep track of roles almost automatically



Different permissions based on groups



Centralized location all parties can draw roles out of



LDAP



Quick Overview of LDAP and LDAP Configs

LDAP

Lightweight Directory Access Protocol



x500 standard

ISODE Consortium
July 1993

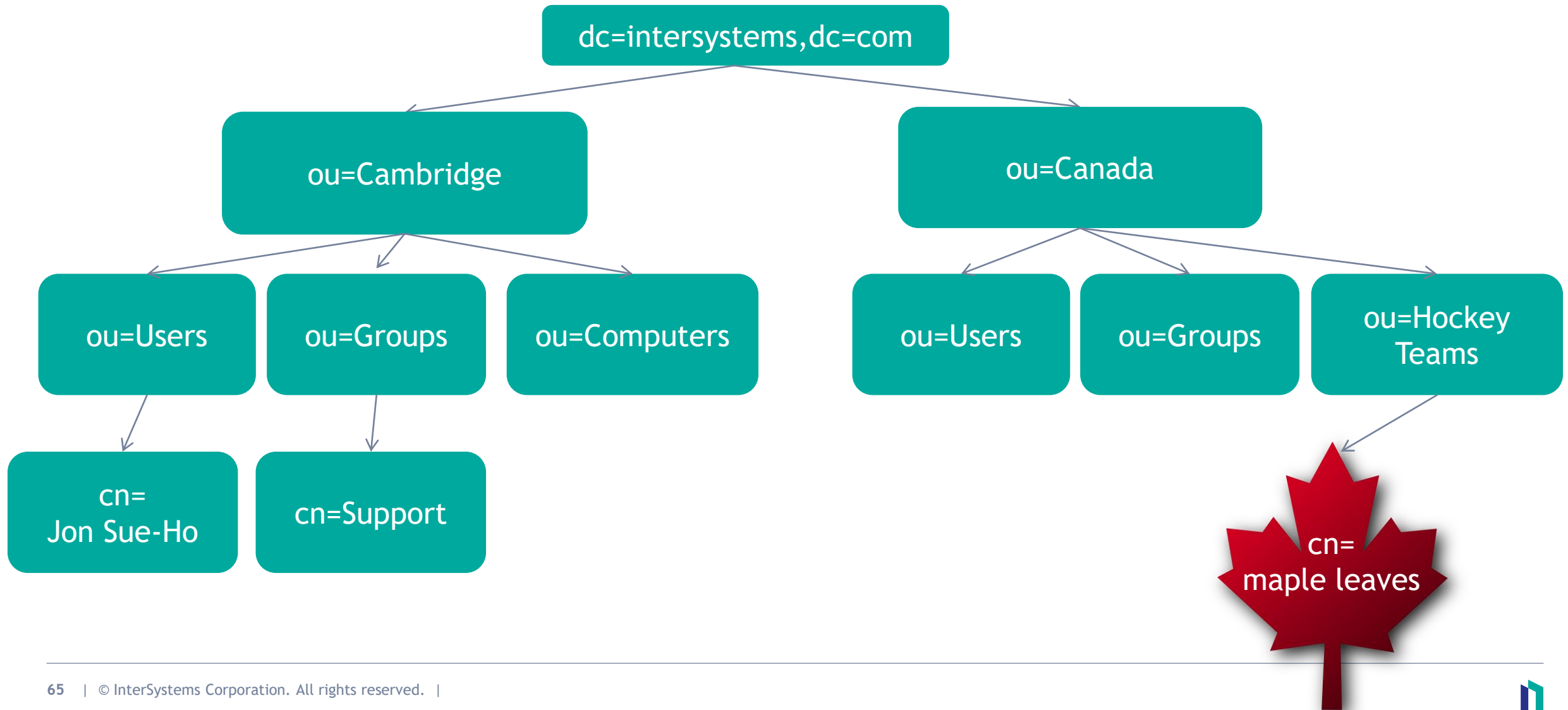
X.500 Lightweight Directory Access Protocol

Status of this Memo

This RFC specifies an IAB standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "IAB Official Protocol Standards" for the standardization state and status of this protocol. Distribution of this memo is unlimited.



Hierarchical Tree Structure



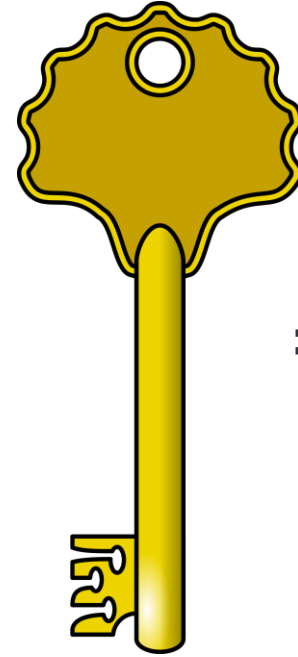
Attributes - Key Value Pairs

Examples

SSN = 987-65-4321

email = jonsueho@bake-query.com

Employee Title = Support Advisor



= Some Value

Groups

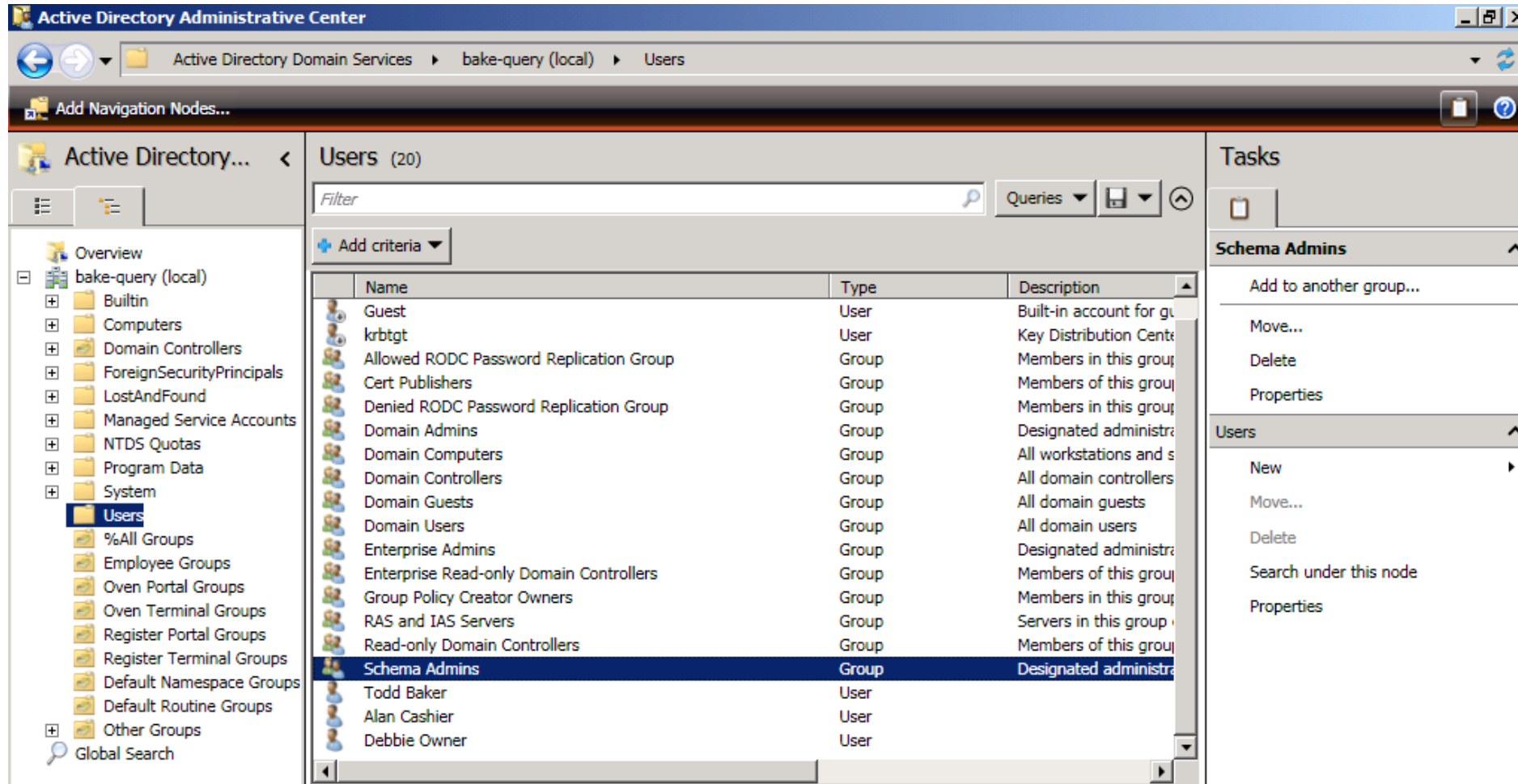
LDAP objects to which users can belong

A group's "member" attribute shows which users belong to the group

A user's "memberOf" attribute shows which groups that user belongs to



It looks like this



Or sometimes like this

Softerra LDAP Administrator 2017

dc=baldingwaiters,dc=com > ou=people > cn=MikeWaiter

File Edit View Favorites Server Entry Schema Reports Tools Window Help

Scope Pane

- Softerra LDAP Administrator
 - Local Servers
 - dc=baldingwaiters,dc=com
 - ou=people
 - cn=doug dougman
 - cn=Steve Steveman
 - cn=Test Testman
 - cn=gloriagloriaman
 - cn=MikeWaiter**
 - ou=groups
 - cn=intersystems-Group-SALESAPP-Role-%All
 - cn=TestGroup
 - cn=GroupABC
 - cn=intersystems-Group-AppServe-Role-%All
 - ou=more

Name	Value	Type
objectClass	top	OID
objectClass	person	OID
sn	mikewaiter	Directory String
cn	MikeWaiter	Directory String
memberOf	cn=intersystems-Group-AppServe-Role-%All,ou=groups,dc=baldingwaiters,dc=com	DN
userPassword	{sha}jChozBgWv9LRwlymduH+QnuLDIw=	Octet String



InterSystems LDAP Configurations - The Past

Edit Security LDAP Options:

Allow LDAP authentication	☒
LDAP server is a Windows Active Directory server	☒
LDAP domain name	bake-query
LDAP host names	bake-query.com
LDAP username to use for searches	administrator
LDAP username password	☐ Enter new password ☐ Clear password ☒ Leave as is
LDAP Base DN to use for searches	DC=bake-query,DC=com
LDAP Unique search attribute	sAMAccountName
Use TLS/SSL encryption for LDAP sessions	☒
Use LDAP Groups for Roles/Routine/Namespace	☒
Search nested Groups for Roles/Routine/Namespace	☒
User attribute to retrieve comment attribute	description
User attribute to retrieve full name from	displayName
User attribute to retrieve default namespace	intersystems-Namespace
User attribute to retrieve default routine	intersystems-Routine
User attribute to retrieve roles	intersystems-Roles
LDAP attributes to retrieve for each user	



Attributes or Groups?

Use LDAP Groups for Roles/Routine/Namespace ☒



Using Attributes

Values of attributes chosen in the config and set on the LDAP server determine roles, namespace, and routine when logging into an instance

User attribute to retrieve default namespace	intersystems-Namespace
User attribute to retrieve default routine	intersystems-Routine
User attribute to retrieve roles	intersystems-Roles



“Patty Cake” User

Attributes:

Name = Patty Cake

SomeAttributeforNamespace = Oven

SomeOtherAttributeforRoles = %Developer,OvenPortalUser

YetAnotherAttributeforRoutine = DinnerRoll



Using Groups

Names of groups in the LDAP server determine user attributes within the instance:

intersystems-Role-%Developer

intersystems-Role-OvenTerminalUser

intersystems-Namespace-Oven

intersystems-Routine-DinnerRoll



Use LDAP Groups for Roles/Routine/Namespace



Search nested Groups for Roles/Routine/Namespace



“Todd Baker” User

Member of the following Groups on the LDAP Server:

intersystems-Role-%Developer

intersystems-Role-OvenTerminalUser

intersystems-Namespace-Oven

intersystems-Routine-DinnerRoll



“intersystems-Role-OvenTerminalUser” Group

Users who are members:

Todd Baker

Patty Cake

Sweeney Todd



User has same roles on all instances!

You could keep them out using “Role required to connect to this system” set in “System-wide Security Parameters”, but that’s an “all or nothing” scenario

You couldn’t set different roles for the same user on different instances (or groups of instances!)

Closest work around is defining the role differently or not defining it at all

Role required to connect to this system	Permission_from_JonSue-Ho
--	---------------------------



InterSystems LDAP Configurations - The Future!

Login Domain Name **bake-query.com**

Description

Kerberos configuration ☒

LDAP configuration ☒

LDAP Enabled ☒

LDAP server is a Windows Active Directory server ☒

LDAP host names
Required.

LDAP username to use for searches
Required.

LDAP username password ☐ Enter new password ☐ Clear password ☒ Leave as is

LDAP Base DN to use for searches
Required.

LDAP Unique search attribute
Required.

Use TLS/SSL encryption for LDAP sessions ☒

Allow ISC_LDAP_CONFIGURATION environment variable ☐

Use LDAP Groups for Roles/Routine/Namespace ☒

Search nested Groups for Roles/Routine/Namespace ☒

Allow Universal group Authorization ☐

Authorization Group ID

Authorization Instance ID

User attribute to retrieve default namespace

User attribute to retrieve default routine

User attribute to retrieve roles

User attribute to retrieve comment attribute



Authorization Group and Instance IDs + Multiple Domains

Cool New Stuff!

InterSystems IRIS Data Platform 2018.2 (and some future release of Caché/Ensemble)

Group IDs and Instance IDs (different roles on different instances!)

Multiple Domains



Authorization Group and Instance IDs

Authorization Group ID Domestic

Authorization Instance ID Computer_Main



Authorization Group ID

Authorization Group ID lets you specify roles for all instances that use that ID in their configuration.

intersystems-Group-Domestic-Role-%Developer
intersystems-Group-Domestic-Role-OvenTerminalUser
intersystems-Group-Domestic-Namespace-Oven
intersystems-Group-Domestic-Routine-DinnerRoll



Authorization Group ID Domestic

Authorization Instance ID Computer_Main



Authorization Group ID

Use cases for Authorization Group ID:

Reporting systems in one group, Production systems in another

ECP app servers in one group, ECP data servers in another

Members of the same mirror all in one group

Shard master and shard servers all in one group

Authorization Group ID

Domestic

Authorization Instance ID

Computer_Main



Authorization Instance ID

Authorization instance ID lets you specify roles for that specific instance.

Default Value: MachineName_InstanceName

intersystems-Instance-Computer_Main-Role-%Developer
intersystems-Instance-Computer_Main-Role-OvenTerminalUser
intersystems-Instance-Computer_Main-Namespace-Oven
intersystems-Instance-Computer_Main-Routine-DinnerRoll



Authorization Group ID Domestic

Authorization Instance ID Computer_Main



Universal Group Authorization

Allow the “old rules” for this instance with no Group or Instance ID specified, eg:
intersystems-Role-%Developer

Allow Universal group Authorization

☐

Multiple Domains

Before you just got one LDAP Configuration

Now you can make as many as you want!

Create New LDAP/Kerberos configuration

Test LDAP Authentication

The following user LDAP/Kerberos configurations are currently available:

Filter:		Page size:	0	Max rows:	1000	Results: 4	Page:	<	<<	1	>>	>	of 1
	Login Domain Name		LDAP Enabled		Description								
»	bake-query.com		Yes				Delete						
	baldingwaiters.com		Yes				Delete						
	iscinternal.com		No				Delete						
	windyhairconsultants.com		Yes				Delete						



Demo!

Example!



Instances (scaled down)

BakeryMain

BakeryFrance

BakeryJapan

BakeryApp1

BakeryApp2



Users of Interest (sorted by domain)

Bake-query:

Debbie Owner

Todd Baker

Alan Cashier

Balding Waiters:

Mike Waiter

Windy Hair Consultants:

Marsha Consultant



Roles of Interest (already configured on each instance)

OvenPortalUser

OvenTerminalUser

RegisterPortalUser

RegisterTerminalUser

%All



Different Roles for Different Users on Different Instances

Employee / Instance	BakeryMain	BakeryFrance	BakeryJapan	BakeryApp1	BakeryApp2
Bakers	OvenPortalUser, OvenTerminalUser	OvenTerminalUser	OvenTerminalUser	None	None
Cashiers	RegisterPortalUser, RegisterTerminalUser	RegisterTerminalUser	RegisterTerminalUser	None	None
Owners	%All	%All	%All	%All	%All
Waiters	None	None	None	%All	%All
Consultants	%All	None	None	None	None



Authorization Group and Authorization Instance IDs

	BakeryMain	BakeryFrance	BakeryJapan	BakeryApp1	BakeryApp
Group ID	Domestic	International	International	AppServe	AppServe
Instance ID	Computer_Main	Ordinat_France	Konpyutaa_Main		



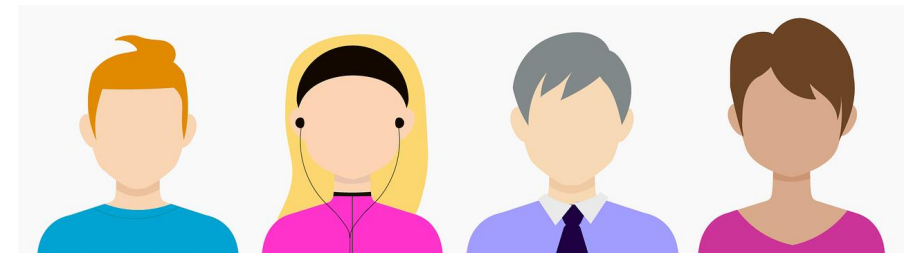
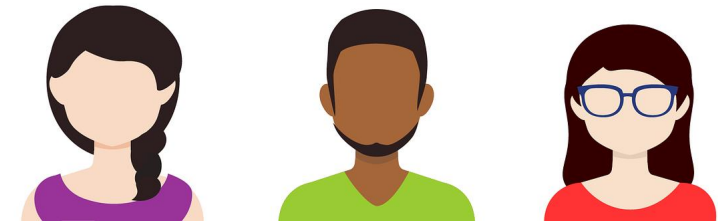
Demo!









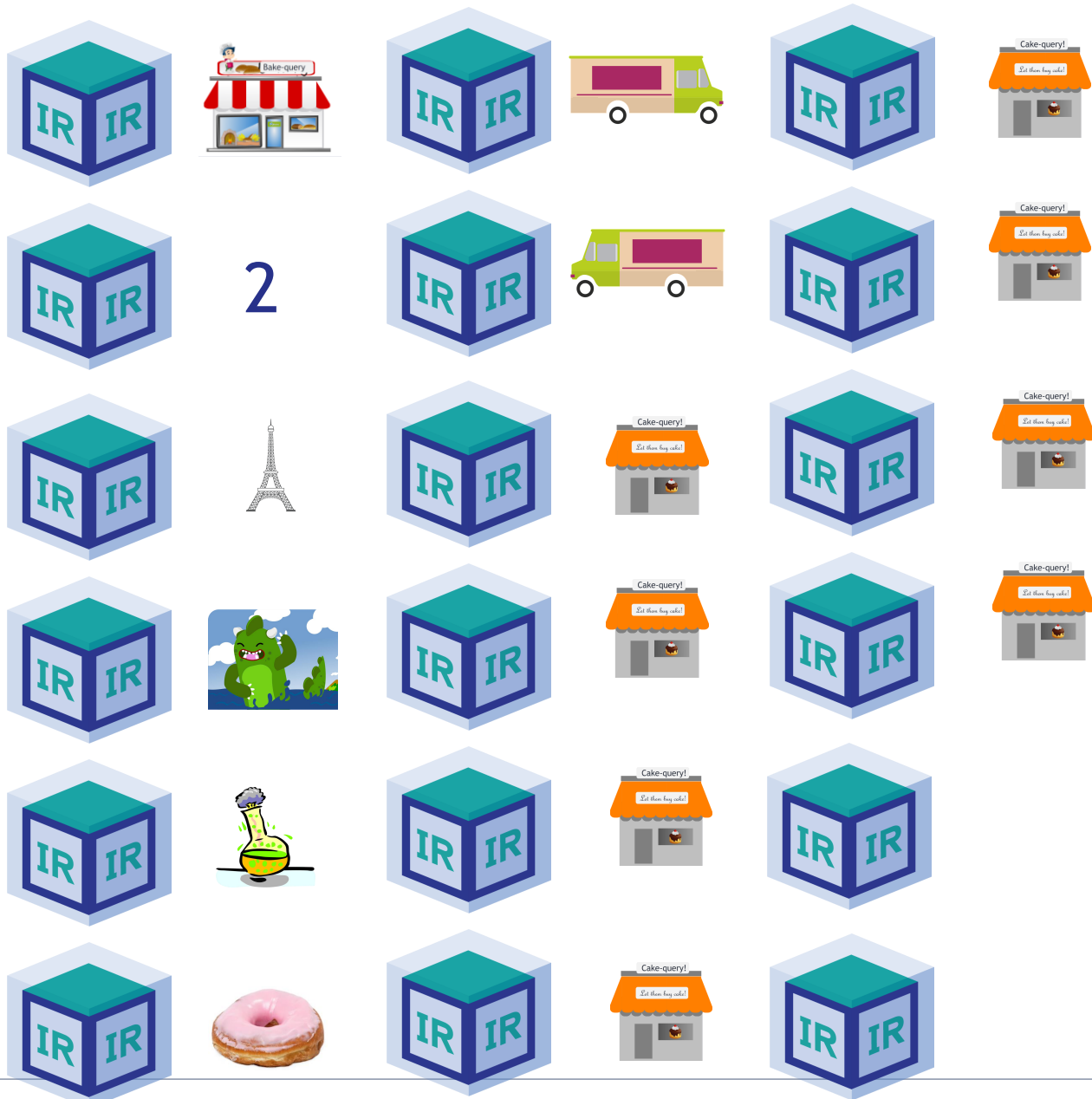


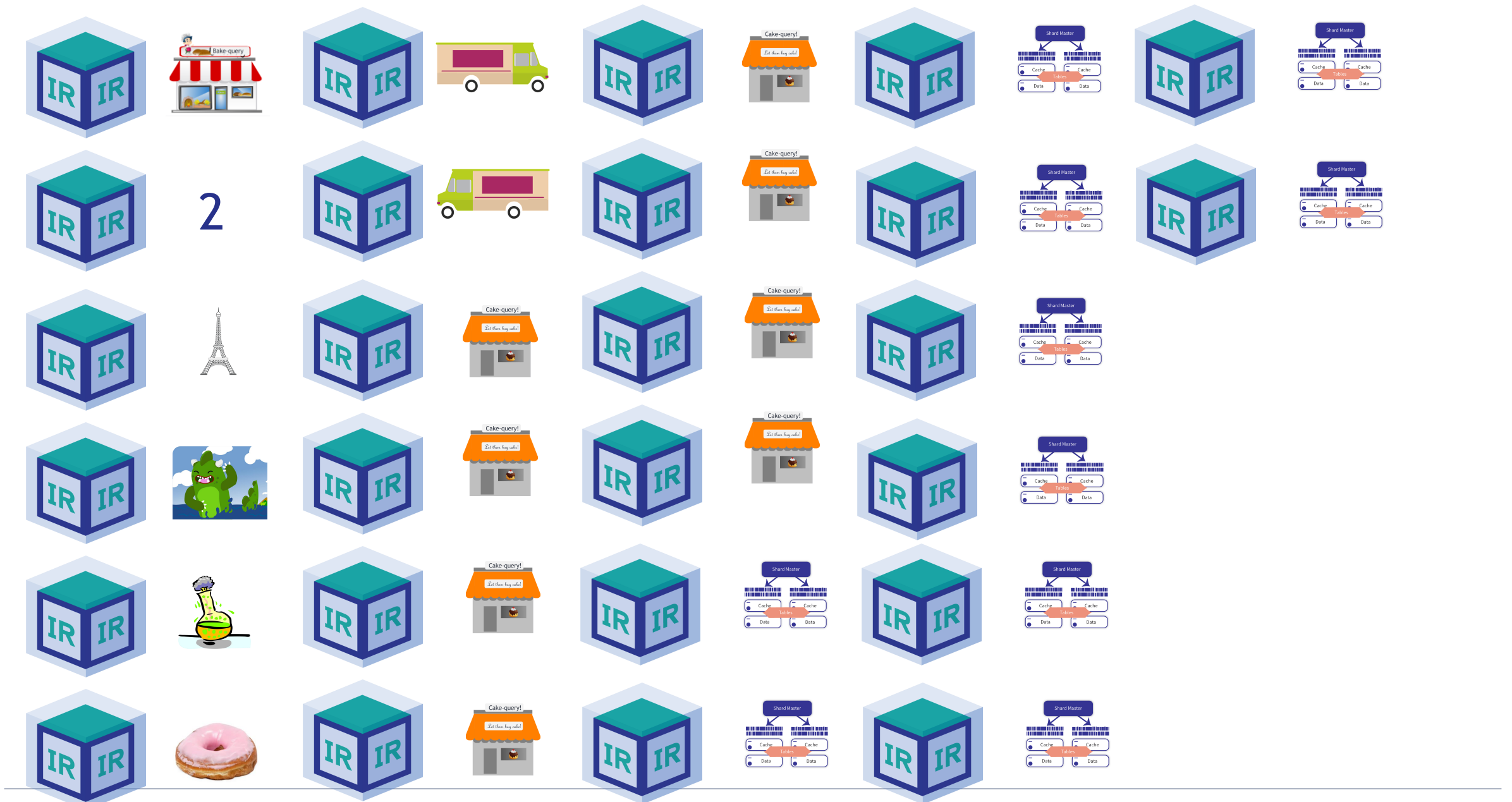


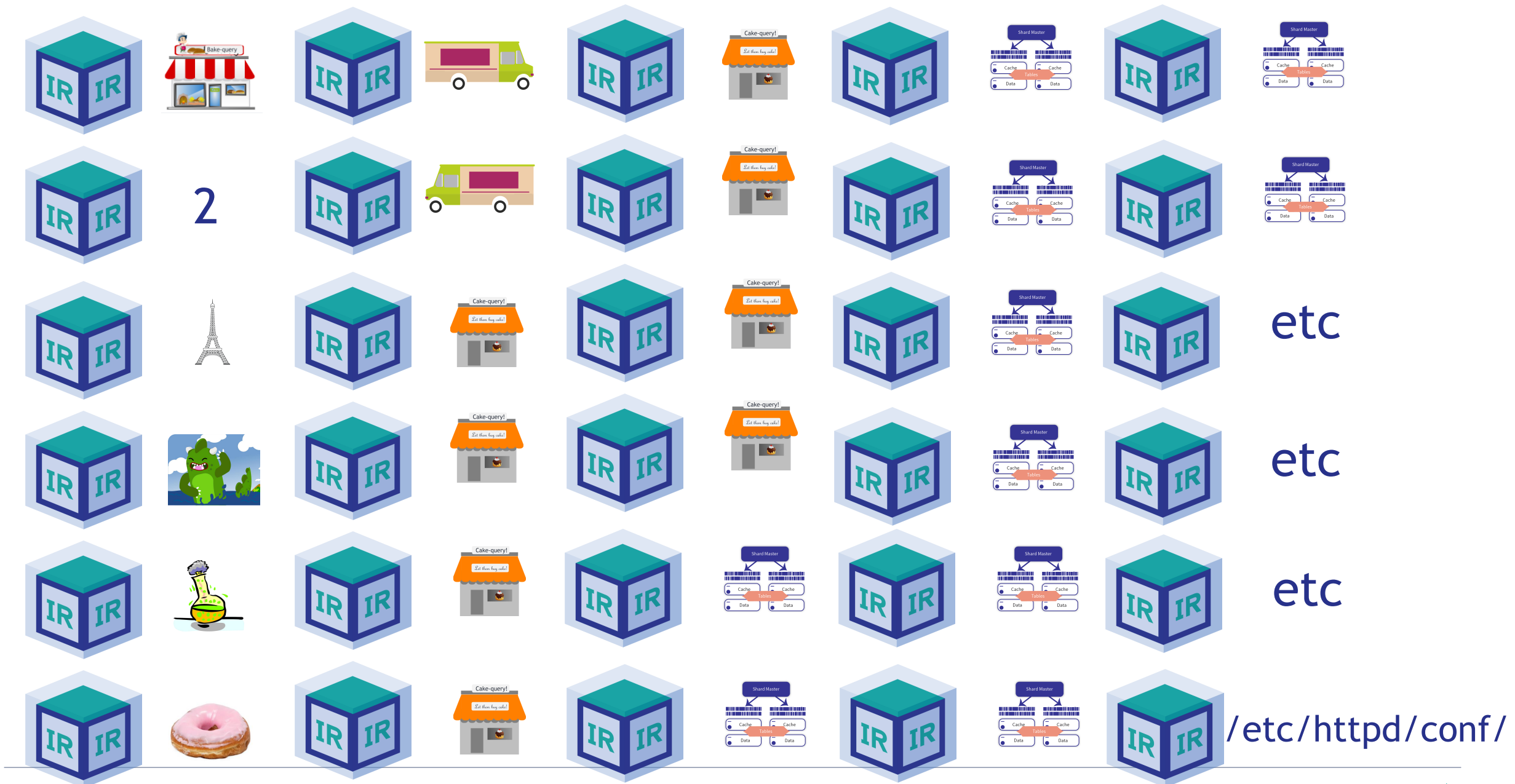


2

















Learn More!

First Look: LDAP and InterSystems Products

https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=AFL_ldap

Security Administration Guide: Using LDAP

https://docs.intersystems.com/irislatest/csp/docbook/DocBook.UI.Page.cls?KEY=GCAS_LDAP

https://docs.intersystems.com/latest/csp/docbook/DocBook.UI.Page.cls?KEY=GCAS_LDAP

Active Directory Integration with LDAP (custom LDAP routines via delegated authentication)

<https://learning.intersystems.com/course/view.php?id=931>

LDAP | InterSystems Developer Community

<https://community.intersystems.com/tags/ldap>





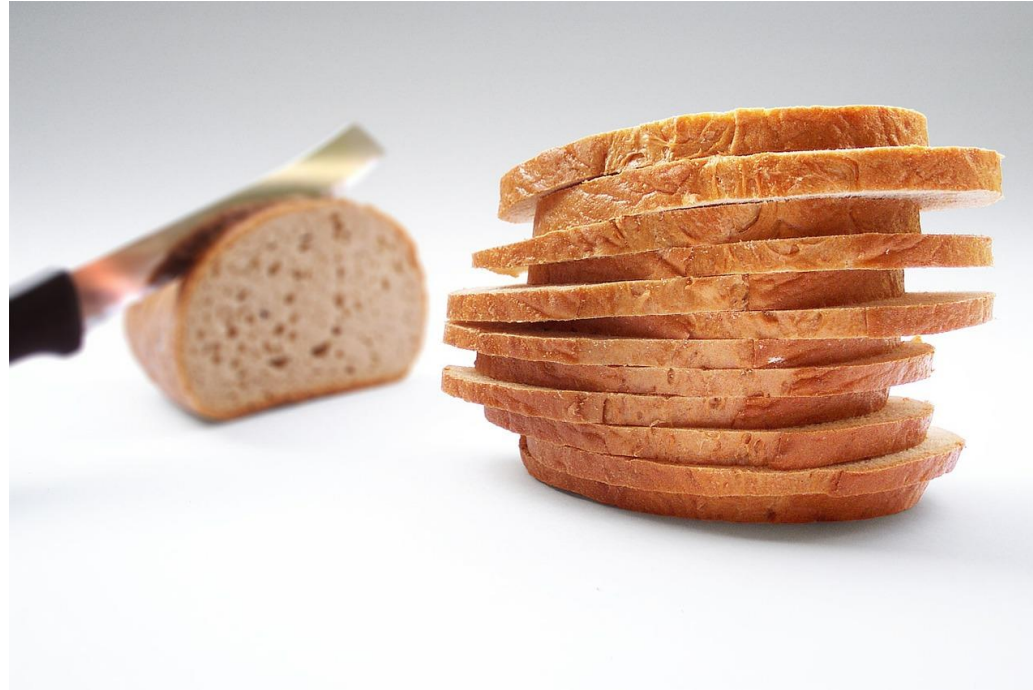












Questions



bake-query.com

cake-query.com

baldingwaiters.com

windyhairconsultants.com

