Starburst
ANALYTICS ANYWHERE

Starburst Global Security

Access All of your Data - Anywhere...

- The Good: Presto allows your users to access your data from virtually any source
- The Bad: Controlling data access
- The Solution: Implement Starburst Global Security

Starburst
ENTERPRISE PRESTO

Agenda

1. Global Security Introduction
2. System Level Security in Starburst Presto
3. Policy Creation and Application
4. Access Policies
5. Row-Level & Masking
6. Secure Zones
7. LDAP UserSync
8. Example Company

Starburst Global Security Introduction

Starburst

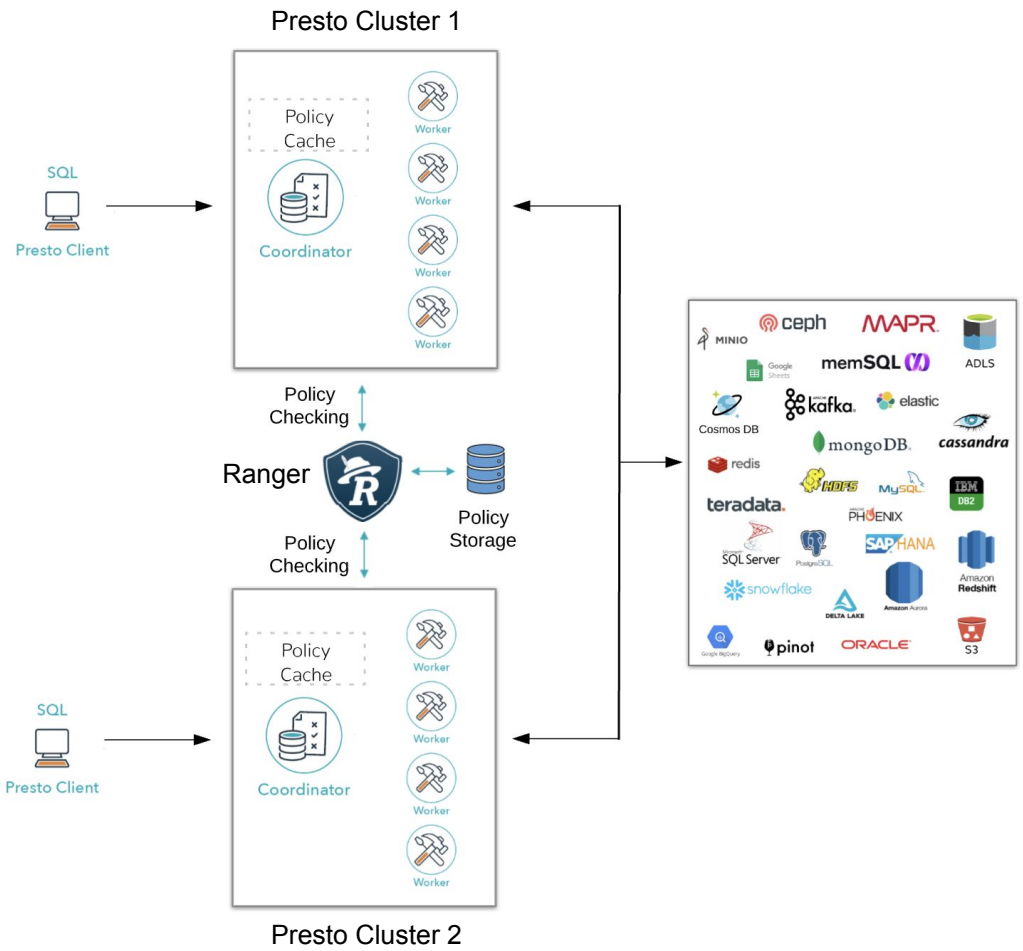
Global Security in Starburst Presto

- Flexible fine-grained access control policies across all connectors
- Column masking for any connectors
- Row-level filtering covering all connectors
- User/Group LDAP/AD synchronization
- Security Zones allow policy delegation to users and groups

Starburst

Global Security Architecture

- One or more Starburst Presto clusters "point" to a Ranger instance
- For each query issued against the Presto cluster, Ranger is queried to match against existing policies
- Based on a decision tree of policies, policies are applied to the query
- Policies can be cached in Presto to improve query performance



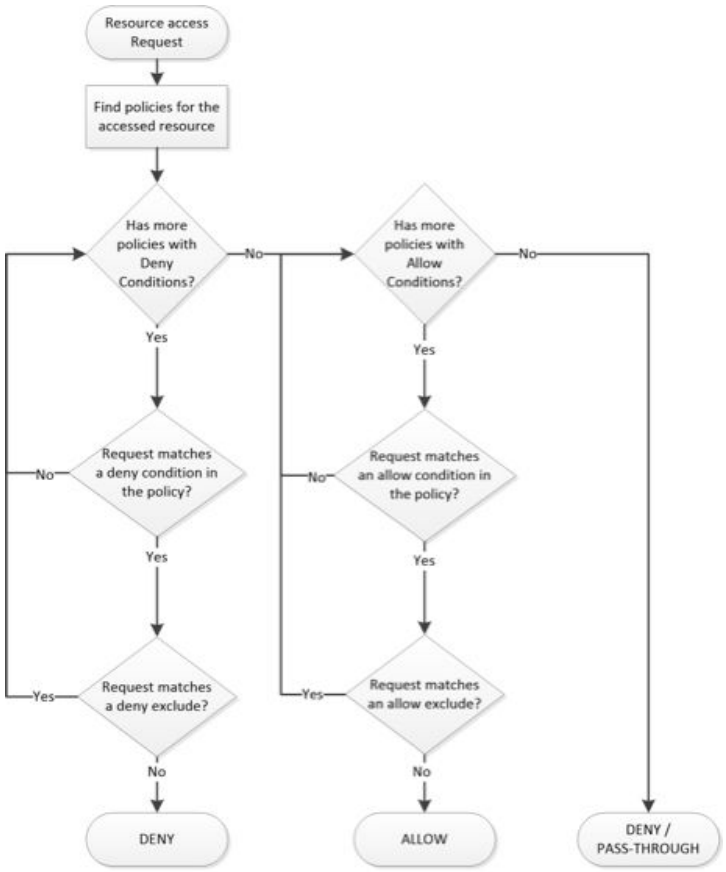
Starburst

System Level Security in Starburst Presto

Starburst

Policy Evaluation Flow

- Once a query is issued to Presto, the decision tree on the right is followed within Ranger
- All Deny policies are matched and enforced first
- After all deny policies have been met, allow policies are evaluated.



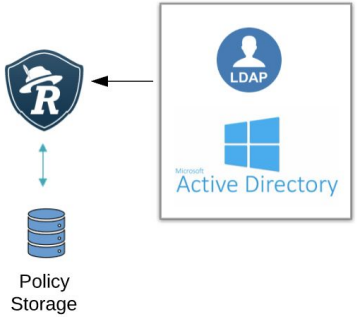
Apache Ranger Policy Evaluation Flow

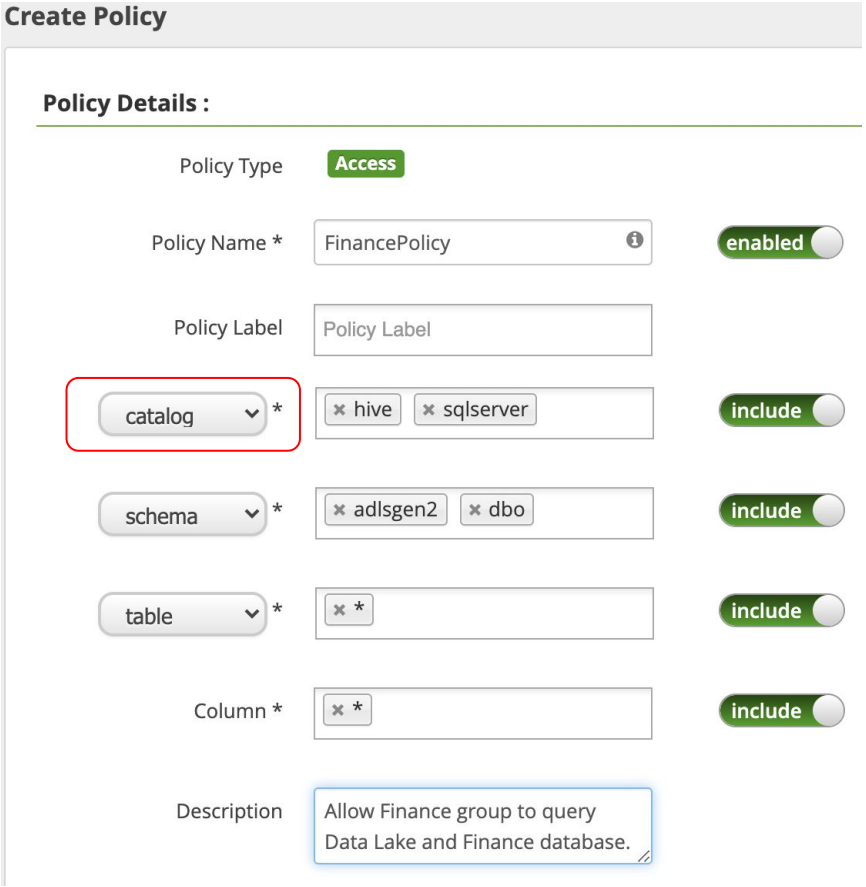
Starburst

System Level Security in Starburst Presto

- Policies applied on all connectors
- Object types are: Catalog, procedures, session properties and query
- Ability to add a validity period to each policy
- User/Group UserSync from LDAP or Active Directory

LDAP/AD User/Group Synchronization

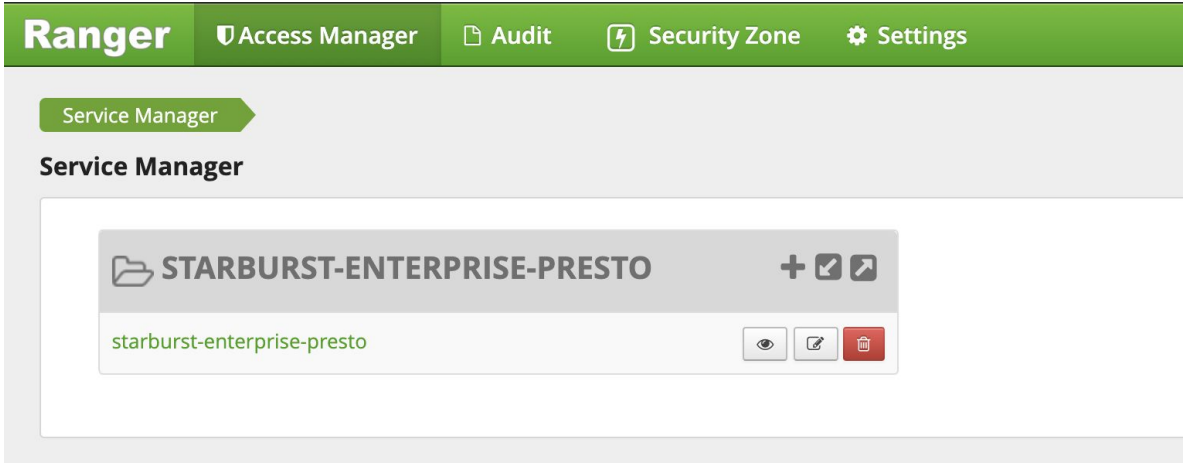




Starburst

Ranger Interface Overview

1. Access Manager -
   a. Resource Based Policies - Create policies for access to catalogs, schemas, procedures, session parameters, tables, column, masking and row-level filtering
   b. Tag Based Policies - Ability to create policies based on Tags
   c. Reports - Search and report on policies
2. Audit - Combined with an independent Solr or HDFS storage will log all access events
3. Security Zone - Delegate catalog policy control to certain groups/users
4. Settings - User and group management



Starburst

Policy Creation and Application

Policy Creation

Three different types of policies

1. Access Control
2. Column Masking
3. Row Level Filtering

Access Control	Column Masking	Row Level Filtering
1. Control access to catalogs, schemas, tables, procedures, query and session properties. 2. All objects are “deny all” at first installation. Must add policies to allow access. 3. Flexible “deny” then “allow” or “allow” then “deny all others”	1. Columns from any table from any connector can be masked 2. Only one column can be masked per policy 3. Masking types: mask, partial mask, nullify and hash	1. Applied at any connector row, based on condition 2. Conditions are set at the user and group levels 3. Filtering is done using a “where clause” Example: nation <> 9

Starburst

Policy Creation - Access Policies

Policy Details :

Policy Type: Access

Policy ID: 8

Policy Name *: MarketingPolicyCatalogs

Policy Label: Policy Label

catalog *: sqlserver, mysql, snowflake, deltalake, hive

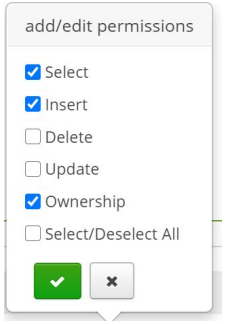
schema *: *

table *: *

Column *: *

Description: This policy will be the main policy to allow access to the

- Multiple entries or wildcards can be used for each section
- Different permission levels can be set
- Deny policies get evaluated first



Example: Marketing doesn't have access to the postgresql catalog, because it has not been explicitly granted

```
presto> select * from
postgresql.public.customer limit 5;
Query 20200729_191304_00249_8tbeg failed:
Access Denied: Cannot access catalog
```

Allow Conditions :

Select Role	Select Group	Select User	Permissions
Select Roles	Marketing	Select Users	Select, Insert, Ownership

Starburst

Policy Creation - Column Masking

Policy Details :

Policy Type	Masking
Policy ID	16
Policy Name *	MarketingInterns
Policy Label	Policy Label
Catalog *	× hive
Schema *	× adlsgen2
Table *	× customer
Column *	× name
Description	Mask customer name for Marketing Interns

- Currently supported masking types are Mask, Partial mask, Hash and Nullify
- Only one policy can be attached to a column at a time
- Can be applied to users and/or groups

Select Masking Option

- (●) Mask
- ( ) Partial mask: show last 4
- ( ) Partial mask: show first 4
- ( ) Hash
- ( ) Nullify

Example

```
presto> select custkey,name from hive.adlsgen2.customer
limit 2;
 custkey |        name
---------+--------------------
   75001 | xxxxxxxxxxxxxxxxxx
   75002 | xxxxxxxxxxxxxxxxxx
```

Select Group	Select User	Access Types	Select Masking Option
× Marketing-Interns	Select Users	Select	Mask

Starburst

Policy Creation - Row Level Filtering

Policy Details :

Policy Type	Row Level Filter
Policy ID	10
Policy Name *	RowFilterMarketing
Policy Label	Policy Label
Catalog *	× hive
Schema *	× adlsgen2
Table *	× nation
Description	Filter out NationKey = 24 for Marketing group.

- Each row-filter policy can only refer to one column
- Filter similar to where clause in a sql statement
- Can be applied at the user or group level

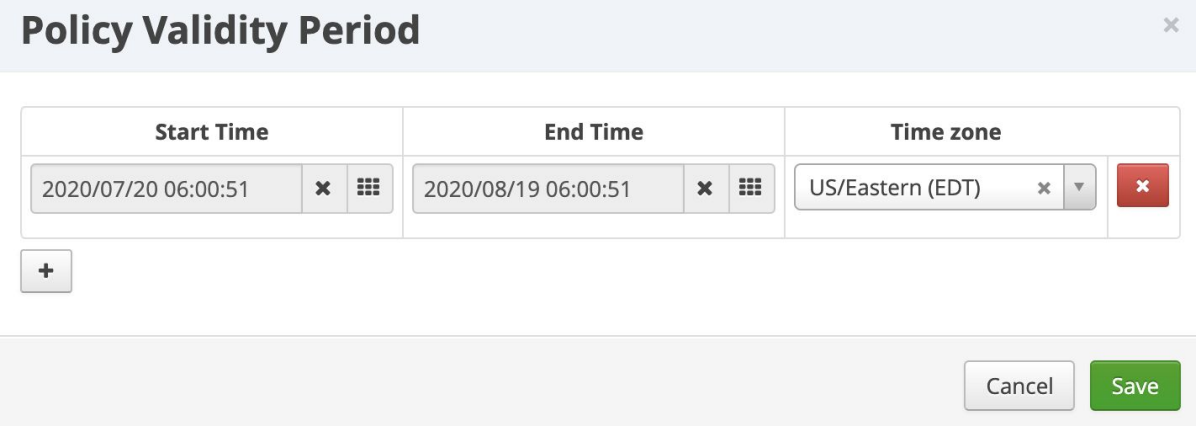
Row Filter Conditions :

Select Role	Select Group	Select User	Access Types	Row Level Filter
Select Roles	× Marketing	Select Users	Select	nationkey=24

Starburst

Policy Creation - Policy Validity Period

- Provides a date/time-based period to enforce policies
- Available on access, masking and row-level filtering policies



Starburst

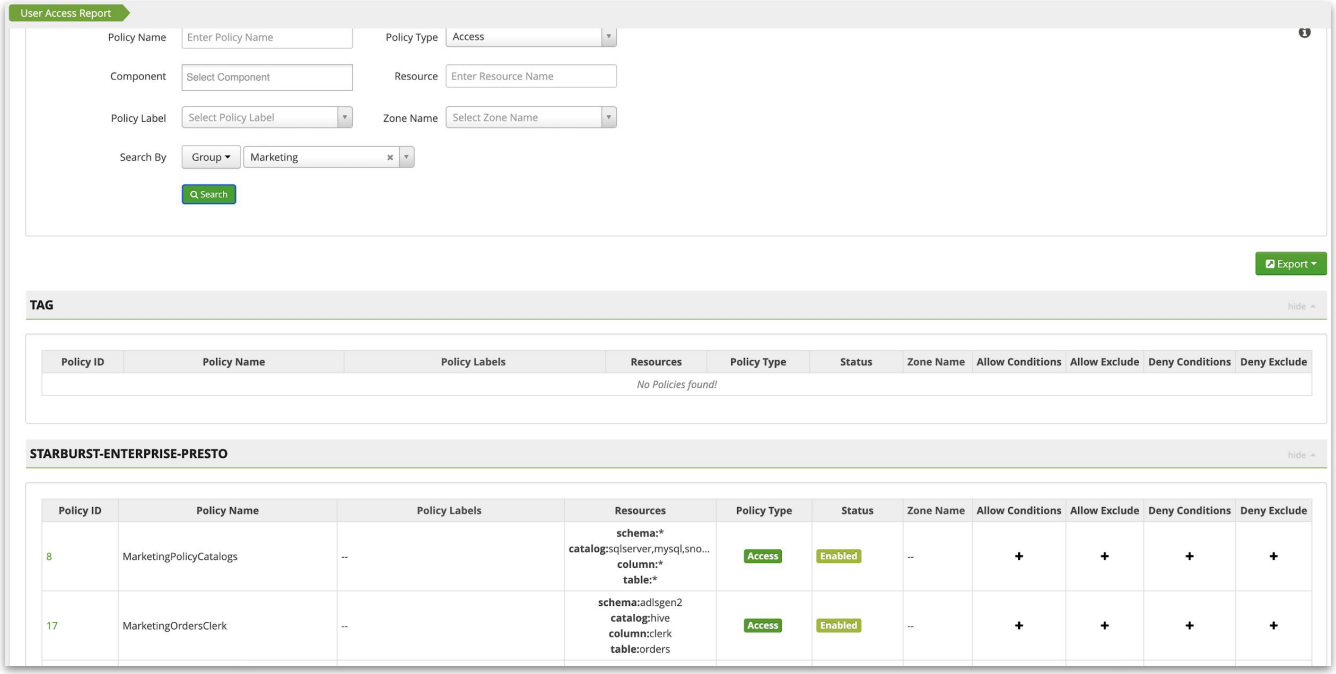
Reports

Reports

You can use the Reports page to help manage policies more efficiently as the number of policies increases

- Search policies by a variety of fields including groups or users
- Export results to Excel, csv or json
- Expand on different conditions:

Allow Conditions	Allow Exclude	Deny Conditions	Deny Exclude
+	+	+	+



Allow Conditions	Groups	Users	Accesses
	Marketing	--	select insert ownership

Starburst

Security Zones

Security Zones

Security Zones allow the creation and administration of policies to groups and/or users.

MarketingResources

This zone will delegate the Marketing group to manage policies on the SQL Server Marketing database

Zone Administration

Admin Users	--
Admin Usergroups	Marketing
Auditor Users	admin
Auditor Usergroups	--

Zone Tag Services

No tag based services are associated with this zone

Services

Service Name	Service Type	Resource
starburst-enterprise-presto	STARBURST-ENTERPRISE-PRESTO	**catalog :** sqlserver

- Multiple users/groups can be added to a zone
- Filter similar to where clause in a sql statement
- Can be applied at the user or group level

Starburst

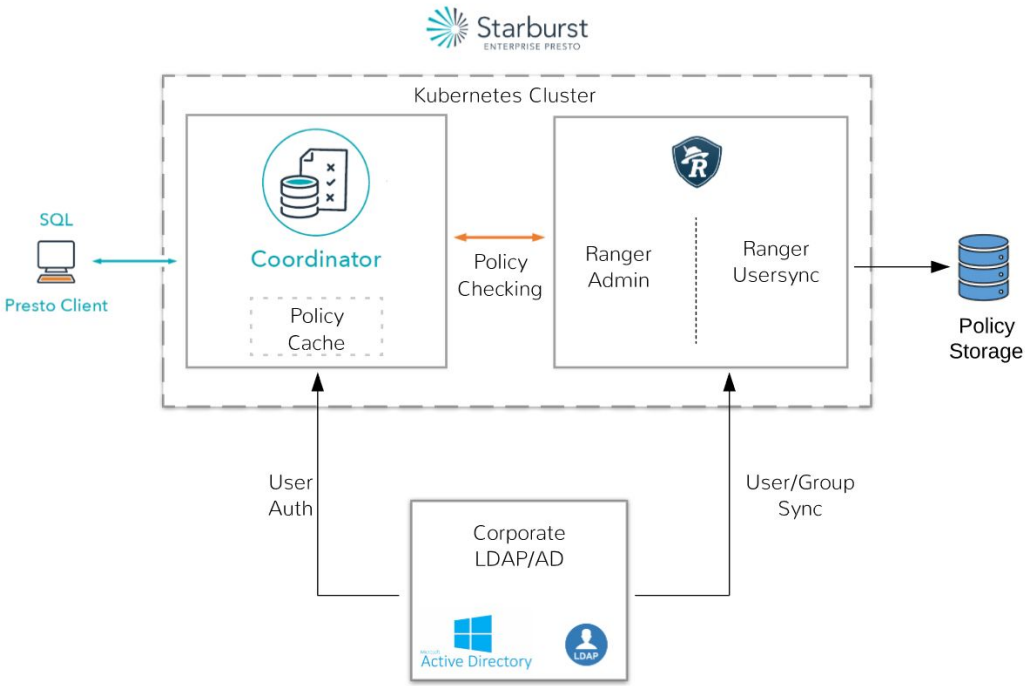
LDAP Usersync

Starburst

LDAP/Active Directory Usersync

Ranger users and groups can be synchronized with a corporate LDAP or Active Directory (AD) system to reduce administration time in Ranger

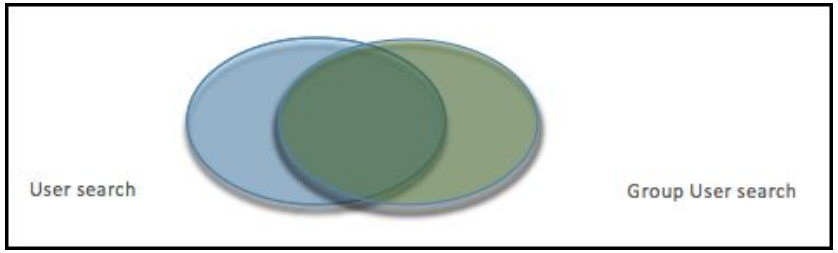
- Users that are authenticated using Presto are also applied within Ranger
- Usersync runs as a container within Starburst Presto k8s service
- Users/Groups are synchronized every hour



LDAP/Active Directory Usersync - Syncing Tips

Synchronizing LDAP/AD objects can be a challenge. Determine what sets of users and groups they belong to before getting started.

- ldapsearch is a handy tool to query LDAP/AD
- Usersync runs as its own container in k8s
- Logs can be found by viewing the container logs for ranger-usersync



Common Usersync Variables: (bind user/p required)
RANGER__SYNC_LDAP_URL: ldaps://xxxx:636
RANGER__SYNC_LDAP_BIND_DN:
RANGER__SYNC_LDAP_BIND_PASSWORD:
RANGER__SYNC_LDAP_SEARCH_BASE:
RANGER__SYNC_LDAP_USER_SEARCH_BASE:
RANGER__SYNC_GROUP_SEARCH_ENABLED:
RANGER__SYNC_GROUP_USER_MAP_SYNC_ENABLED:
RANGER__SYNC_LDAP_USER_NAME_ATTRIBUTE:

Starburst Ranger Usersync Documentation:

https://docs.starburstdata.com/latest/kubernetes/ranger.html#ldap-user-synchronization

Starburst

Example Company

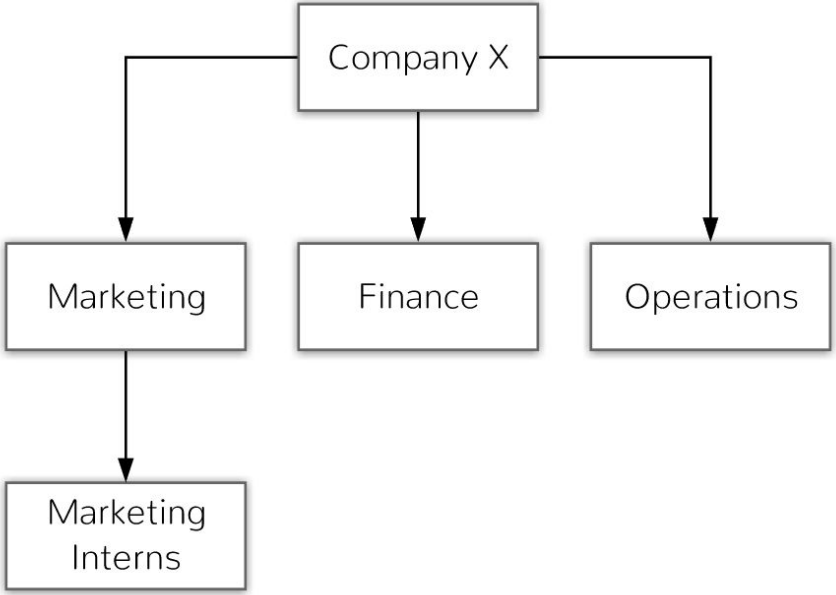
Example Company

Company Name: Example Corp

Departments: Marketing, Finance & Operations

Sub Departments: Marketing Interns

Users:
ted-marketing
vishal-operations
nancy-finance
kevin-marketing-intern



Data Sources

ADLS - Corporate Data Lake

SQL Server - Marketing Database

PostgreSQL - POS System Database

Starburst

Permissions Overview

Marketing

ADLS
Data Lake

Read only
Write to Sandbox

Full Access

Finance

ADLS
Data Lake

Read only
Write to Sandbox

Full Access

Full Access

Operations

ADLS
Data Lake

Read only
Write to Sandbox

Full Access

Starburst

Policy Layout

Group	Data Source	Policy Name	Description
Marketing	SQL Server	Marketing-MarketingDB	Full Access to SQL Server Marketing database
All	Data Lake	All-DataLake	Read-only access to the Data Lake for each department
Marketing	Data Lake	Marketing-Sandbox	Full access to the Marketing Sandbox - Read-only for interns
Finance	All sources	Finance-All	Read-only access to all sources
Finance	Data Lake	Finance-Sandbox	Full access to the Finance Sandbox
Operations	POS	Operations-POS	Full Access to POS PostgreSQL database
Operations	Data Lake	Operations-Sandbox	Full access to the Operations Sandbox
Marketing	Data Lake	MarketingInterns-CustMask	Mask customer name for Marketing Interns
Public	Data Lake	NationRowFilter	Restrict NationKey = 19 from anyone

Marketing Database - Full Access

Policy Name * Marketing-MarketingDB

Policy Label Policy Label

catalog * × marketing

schema * × *

table * × *

Column * × *

Description Full Access to SQL Server Marketing database

Select Group	Select User	Permissions
× Marketing	Select Users	Select Insert Delete Update Ownership

Starburst

Data Lake - Read Only Access

Policy Name * All-DataLake

Policy Label Policy Label

catalog * × hive

schema * × adlsgen2

table * × *

Column * × *

Description Read only access to the Data Lake

- Demo-Finance
  - hive
    - adlsgen2
    - financesb
  - marketing
  - pos
  - system
- Demo-Marketing
  - hive
    - adlsgen2
    - marketingsb
  - marketing
  - system
- Demo-Operations
  - hive
    - adlsgen2
    - operationssb
  - pos
  - system

Select Group	Select User	Permissions
× Marketing × Operations × Finance	Select Users	Select

Starburst

Marketing Sandbox

Policy Type: Access

Policy ID: 10

Policy Name *: Marketing-Sandbox

Policy Label: Policy Label

catalog *: × hive

schema *: × marketingsb

table *: × *

Column *: × *

Description: Full access to the Marketing Sandbox but deny other groups.

Allow full access to only the Marketing group and read-only for interns

Select Group	Select User	Permissions
× Marketing	Select Users	Select Insert Delete Update Ownership
× Marketing-Interns	Select Users	Select

Deny other groups access to the sandbox

Deny All Other Accesses : True

- hive
  - adlsgen2
  - marketingsb
- marketing
- system

Starburst

Masking Customer Name for Marketing Interns

Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups
MarketingInterns-CustMask	--	Enabled	Enabled	--	Marketing-Interns

Operations sees customer name

```
select * from hive.adlsgen2.customer limit 10;
```

ult

ct * from hive.adlsgen2.customer limit 1 | Enter a SQL expression to filter results (use Ctrl+

123 custkey	ABC name	ABC address
75,001	Customer#0000750(	iQyegZCktrxX8jMFs9ip
75,002	Customer#0000750(	TRzWtXys54mXmbNLlZQ4UR,5VkzA4Ycjsx
75,003	Customer#0000750(	OVaJQHekQKFzsjqYpkLD
75,004	Customer#0000750(	DM8SVyMtxAqxUhSFtMoYXSwAPRi,rCxLHaC
75,005	Customer#0000750(	UFagliT4yLXrlK4,KpBFwt7Pa5egjXuWw8 P6u
75,006	Customer#0000750(	TCS8unq57G
75,007	Customer#0000750(	iPQBVCkNZIwA,g3VUeFzV
75,008	Customer#0000750(	imzHhGJHRabMisy43J4P,RAo3K
75,009	Customer#0000750(	bWv8PnIGSz
75,010	Customer#00007501	VYzjCpkja24Kbnvv0Oa1,b2pVU1pd45AYCoZK

Marketing interns do not

```
select * from hive.adlsgen2.customer limit 10;
```

lt

ct * from hive.adlsgen2.customer limit 1 | Enter a SQL expression to filter results (use Ctrl-

123 custkey	ABC name	ABC address
75,001	xxxxxxxxxxxxxxxxxx	iQyegZCktrxX8jMFs9ip
75,008	xxxxxxxxxxxxxxxxxx	imzHhGJHRabMisy43J4P,RAo3K
75,009	xxxxxxxxxxxxxxxxxx	bWv8PnIGSz
75,010	xxxxxxxxxxxxxxxxxx	VYzjCpkja24Kbnvv0Oa1,b2pVU1pd45AYCoZK
75,002	xxxxxxxxxxxxxxxxxx	TRzWtXys54mXmbNLlZQ4UR,5VkzA4Ycjsx
75,003	xxxxxxxxxxxxxxxxxx	OVaJQHekQKFzsjqYpkLD
75,004	xxxxxxxxxxxxxxxxxx	DM8SVyMtxAqxUhSFtMoYXSwAPRi,rCxLHaC
75,005	xxxxxxxxxxxxxxxxxx	UFagliT4yLXrlK4,KpBFwt7Pa5egjXuWw8 P6u
75,006	xxxxxxxxxxxxxxxxxx	TCS8unq57G
75,007	xxxxxxxxxxxxxxxxxx	iPQBVCkNZIwA,g3VUeFzV

Starburst

Row Filter Example

Policy Name * NationRowFilter18

Policy Label Policy Label

Catalog * × hive

Schema * × adlsgen2

Table * × nation

Description Filter out nationkey = 18

Filter out nationkey = 18
to all users/groups

```
select * from hive.adlsgen2.nation
```

ct * from hive.adlsgen2.nation order by Enter

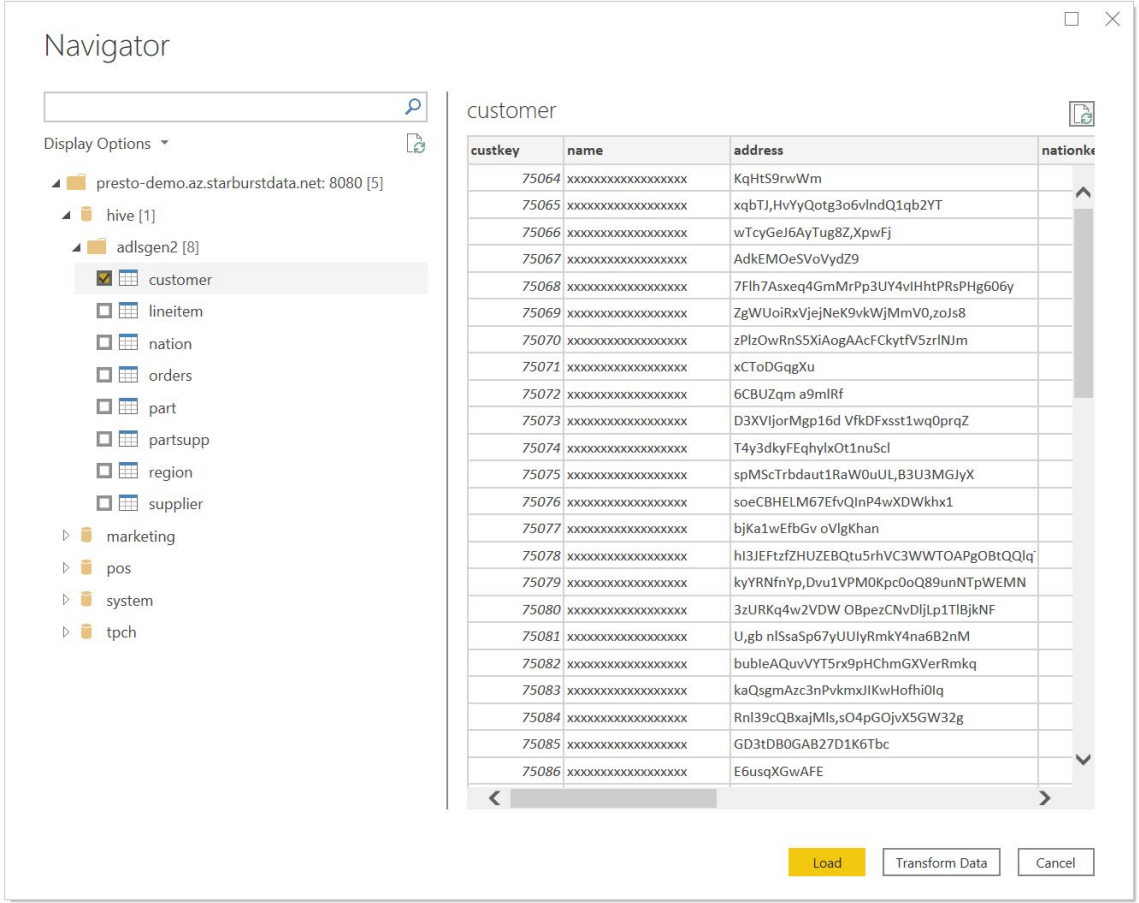
123 nationkey	ABC name	123 reg
0	ALGERIA	
1	ARGENTINA	
2	BRAZIL	
3	CANADA	
4	EGYPT	
5	ETHIOPIA	
6	FRANCE	
7	GERMANY	
8	INDIA	
9	INDONESIA	
10	IRAN	
11	IRAQ	
12	JAPAN	
13	JORDAN	
14	KENYA	
15	MOROCCO	
16	MOZAMBIQUE	
17	PERU	
19	ROMANIA	

Select Group	Select User	Access Types	Row Level Filter
× public	Select Users	Select	nationkey<>18

Starburst

Policies are applied to all SQL clients

This example shows Power BI and masking policy for the customer name



Starburst

Global Security in Starburst Presto

- Flexible fine-grained access control policies across all connectors
- Column masking for any connectors
- Row-level filtering covering all connectors
- User/Group LDAP/AD synchronization
- Security Zones allow policy delegation to users and groups

Starburst

Thank You

www.starburstdata.com