
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

ANT321

What's new in AWS Lake Formation

Mert Hocanin (he/him)

Principal Big Data Architect
AWS Lake Formation
AWS

Purvaja Narayanaswamy (she/her)

Software Development Manager
AWS Lake Formation
AWS

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

Quick overview of AWS Lake Formation

New integrations with Lake Formation

New features of Lake Formation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Quick overview of AWS Lake Formation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Lake Formation

Build, manage, secure, and
share data in data lakes in days



Build data lakes with
database-like features quickly



Simplify security management
and governance at scale



Provide self-service access to data

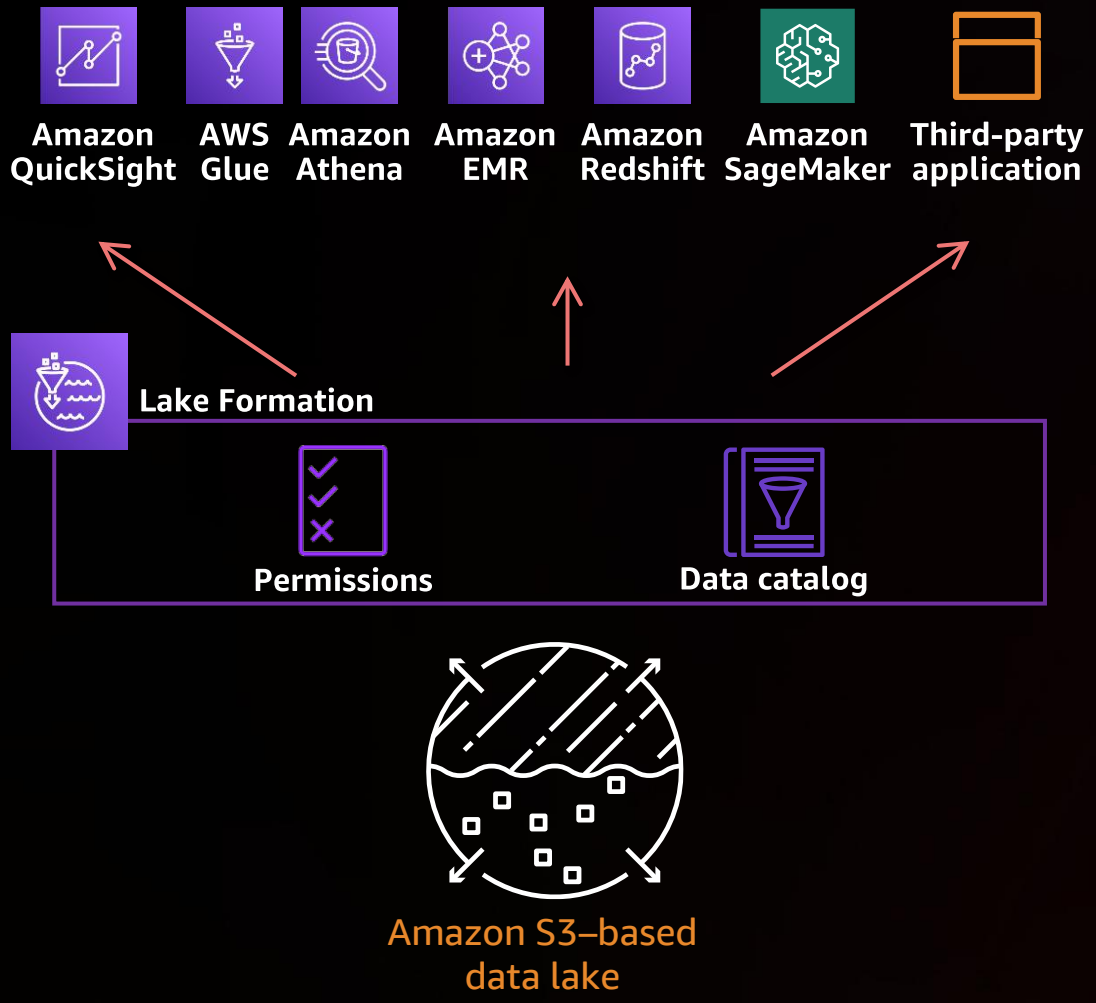


Enable data accessibility across
your organization

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

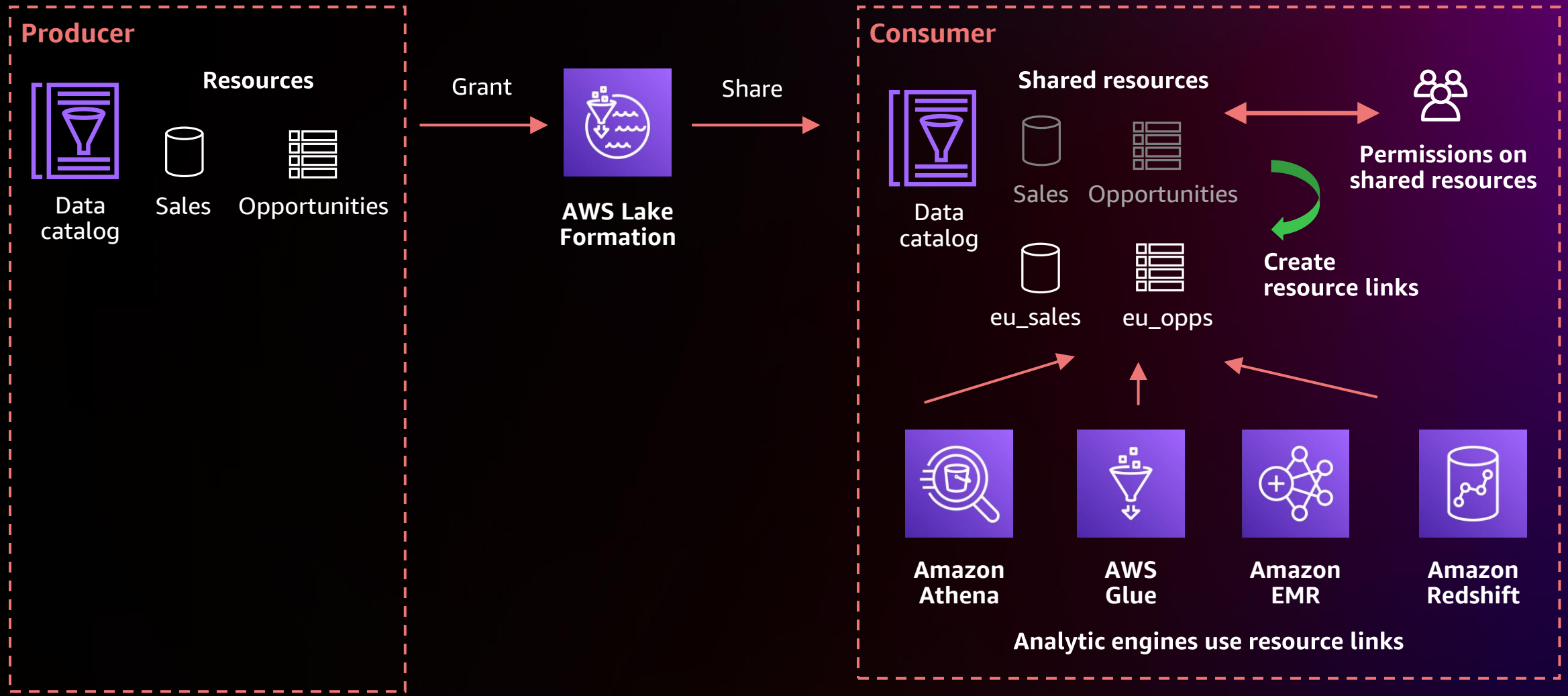
Lake Formation secures your data lake



- DB-style fine-grained permissions on resources
- Scale permissions management using Lake Formation tag-based access control (LF-TBAC)
- Unified Amazon S3 permissions
- Integrated with services and tools
- Easy to audit permissions and access

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lake Formation facilitates cross-account sharing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New integrations with Lake Formation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon Lake Formation integrations



Amazon EMR

- SAML enabled Amazon EMR clusters
- Runtime Roles (New!)



Amazon Redshift

- External tables through Amazon Redshift Spectrum
- Data shares* (New!)
- Federated IAM identities (New!)



AWS Glue

- Glues dynamic frames



Amazon QuickSight

- QuickSight authors



AWS Data Exchange

- Publishing and subscribing with Lake Formation* (New!)



Amazon Athena

- SQL queries



Third-party vendors

- Ahana (New!)
- Starburst (New!)
- Dremio* (New!)

* Currently in Preview

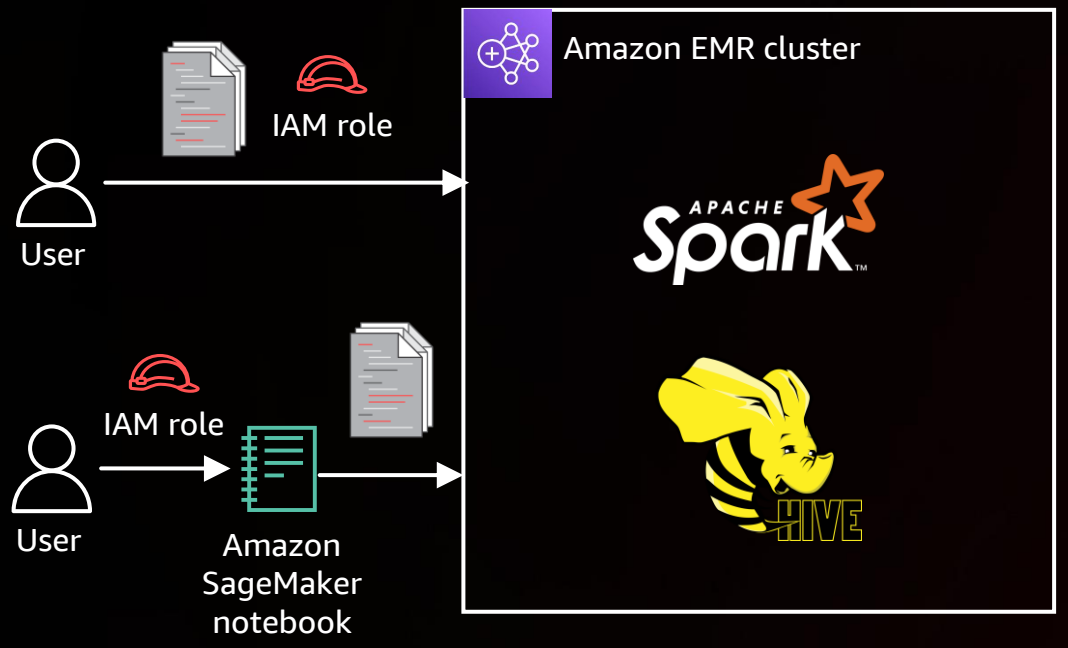
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW!

Expanded support for Lake Formation permissions – Amazon EMR Runtime Roles

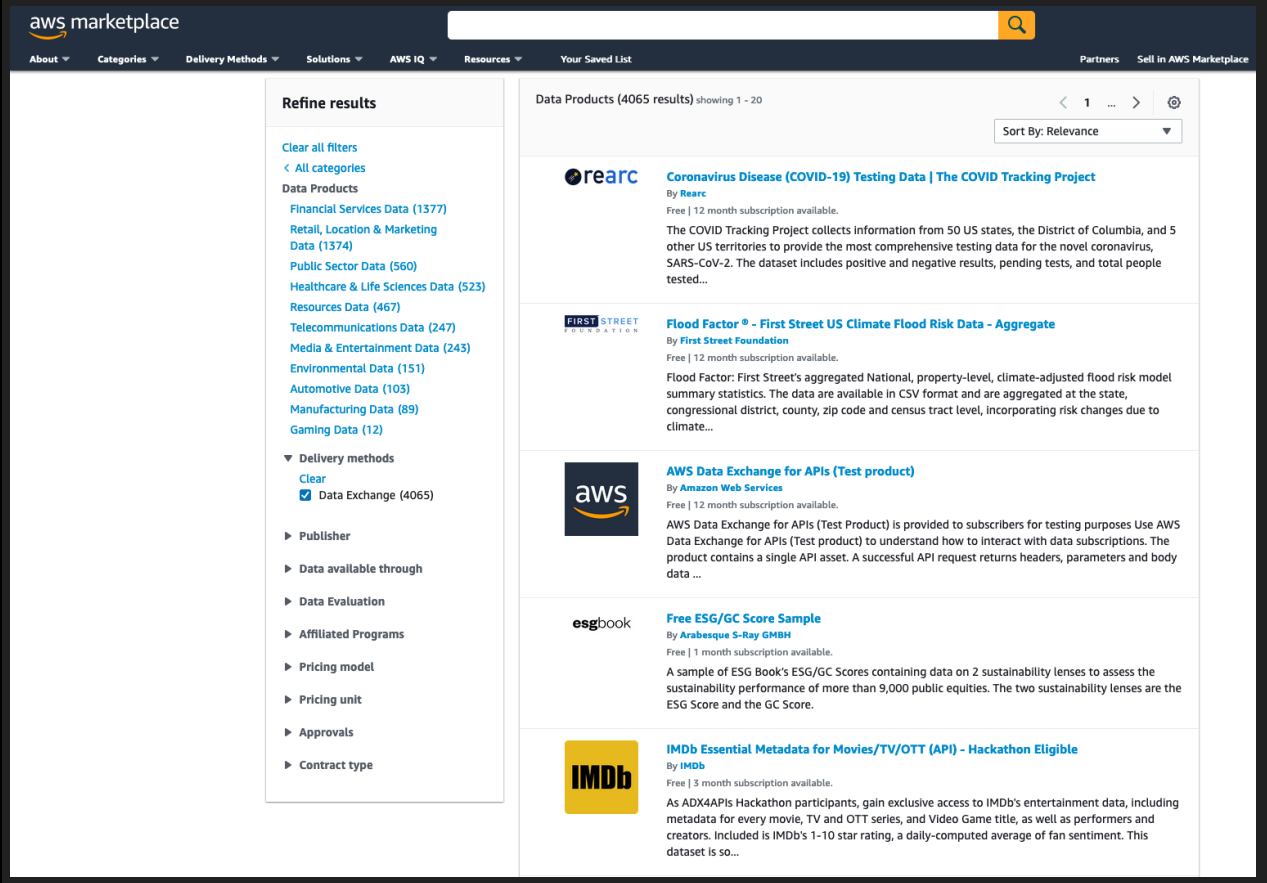
Amazon EMR Runtime Roles



- Jobs submitted using a Runtime Role enabled cluster will use Lake Formation for enforcement
- Jobs can be submitted through Amazon EMR steps, Amazon SageMaker notebooks, or directly to the cluster using JDBC for Hive or Livy for Spark

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

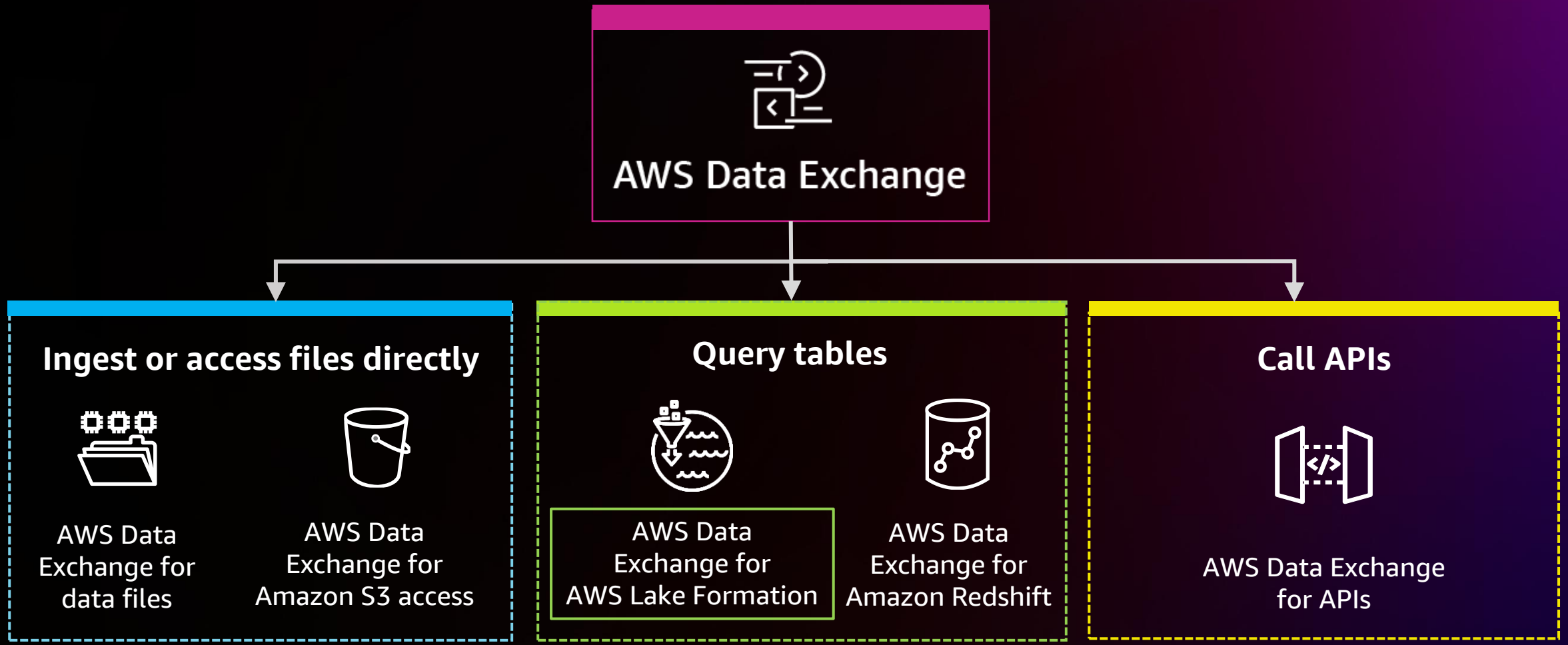
AWS Data Exchange enables customers to easily find, subscribe to, and use third-party data in the cloud



- 300+ data providers and 3,500+ data products
- Over 1,500 free public data products to easily evaluate the data you need
- Support for private products and private data trials
- Data delivery using files, tables, and APIs

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

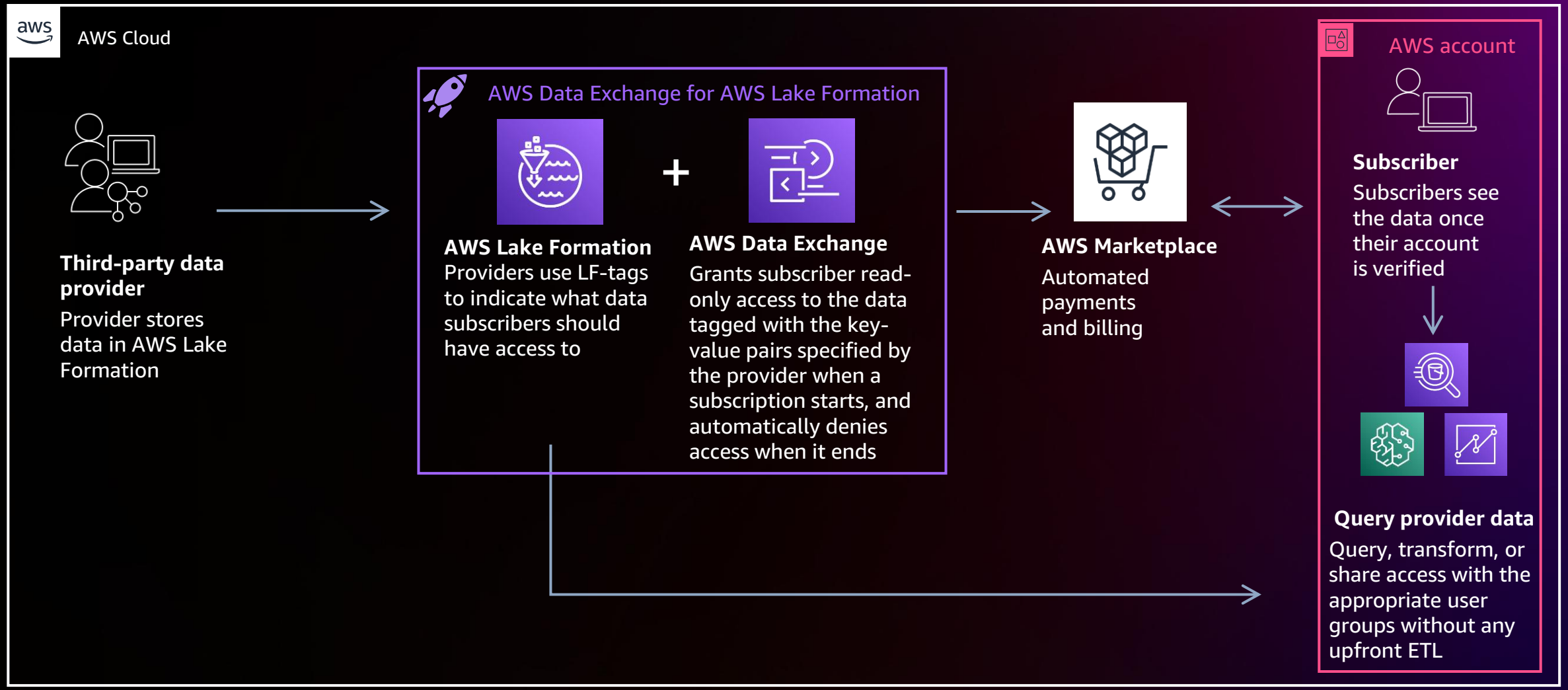
AWS Data Exchange – Third-party data using files, tables, or APIs, all in one service



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW!

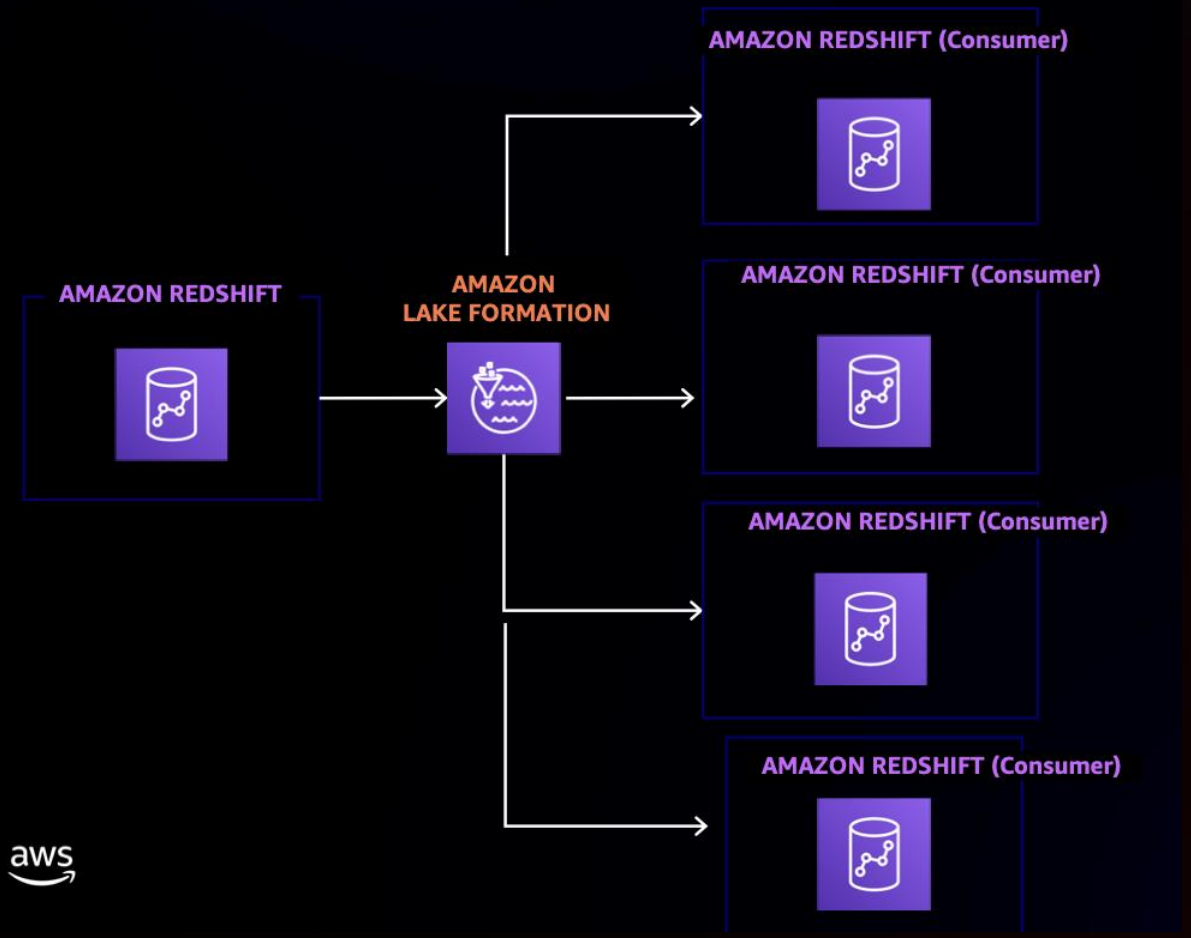
AWS Data Exchange for AWS Lake Formation (Preview)



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW!

Centrally manage access to your Amazon Redshift data shares within AWS Lake Formation



Centrally manage granular access to data across all-consuming data services within your organization

Improve security and governance with row-level and column-level granular permissioning on the data share

No more manual scripting or complex querying in individual data shares to understand your users access to data

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lake Formation and Amazon Redshift Spectrum integration using IAM user identity

OLD MODE

- Required customers to manage Amazon Redshift cluster-attached IAM-roles and users needed to assume the cluster role
- Challenges around the number of roles that can be tied to a cluster

NEW MODE

- Federated identity support to manage Amazon Redshift Spectrum tables
- No need to manage cluster-attached IAM roles for Redshift Spectrum
- Redshift Spectrum can directly pass IAM user FAS credentials to AWS Lake Formation for fine-grained access controls
- Support available in JDBC client

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Lake Formation Partners







* Integration is currently in Private Preview

This is not a complete list. To view all AWS Partners for this category, visit AWS Partner Solutions Finder. This list of partners is current as of October 19, 2022.

aws

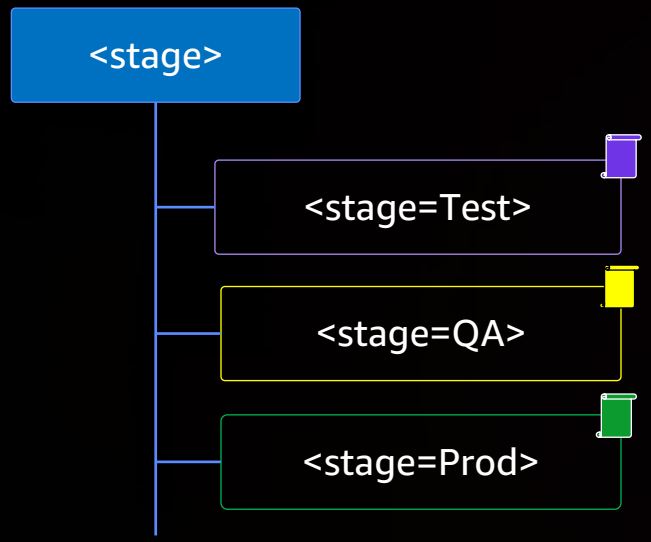
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

New features of AWS Lake Formation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

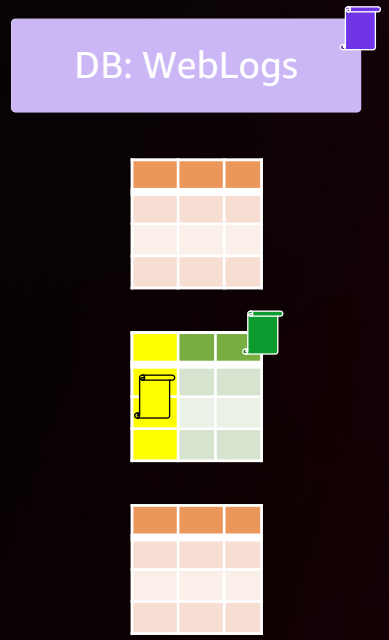
Lake Formation tag-based access control: Recap

Define LF-tags



Specify who can assign LF-tags and values

Assign LF-Tags to resources



Tag databases, tables, and columns

LF-tags are hierarchical and may be overridden

Create policies on LF-tags



IAM user/role



AD users and groups (SAML assertion)

Scale by applying permission on LF-tags

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Lake Formation tag-based access control: Cross Account Access

OLD MODE

- Cross-account access to AWS Glue Data Catalog resources requires manual additions to the resource policy
- Policy size limits as number of recipient account increases
- Limitation around sharing to accounts within ORG and ORG units
- Recipient account lacks notion of invitation to accept/deny cross account tag-based resource share

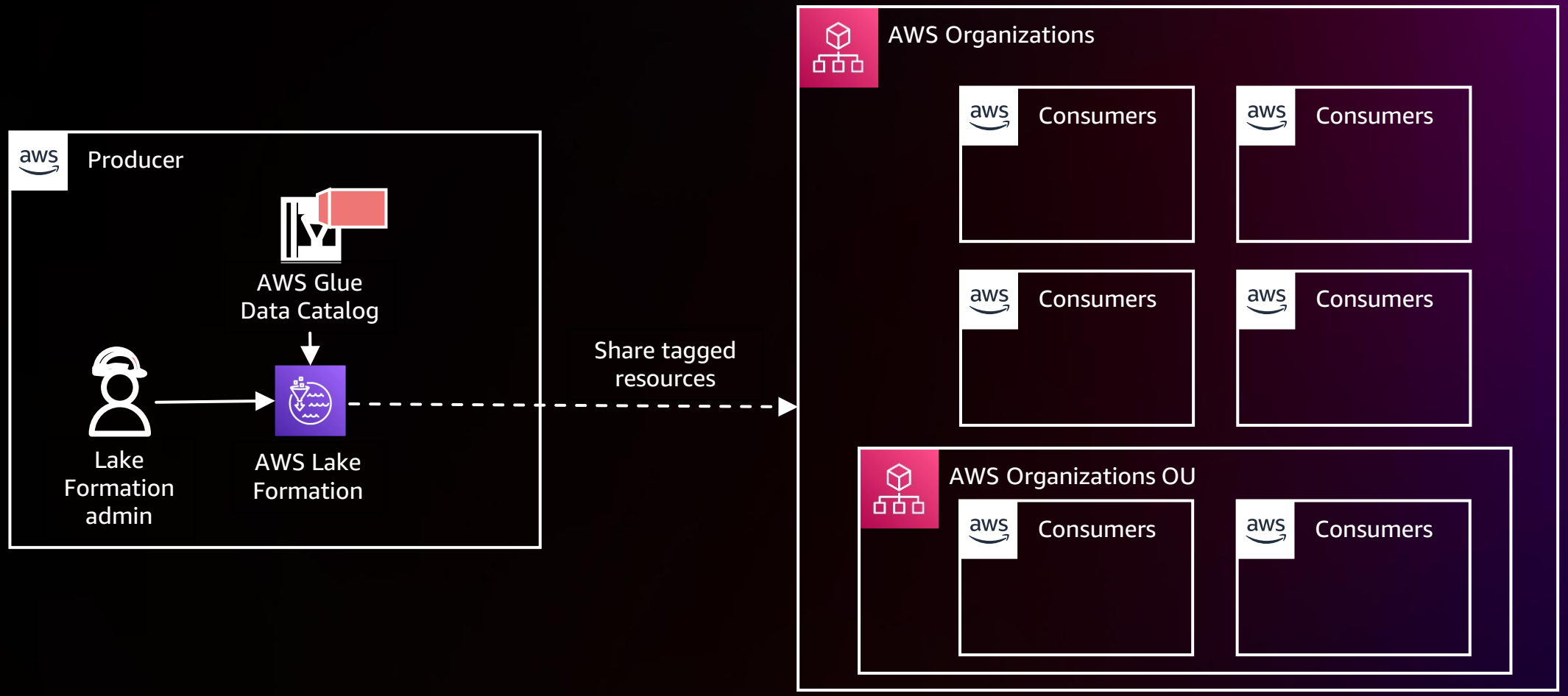
```
{
  "Effect": "Allow",
  "Action": [
    "glue:*"
  ],
  "Principal": {
    "AWS": [
      "<recipient-account-id>"
    ]
  },
  "Resource": [
    "arn:aws:glue:<region>:<account-id>:table/*",
    "arn:aws:glue:<region>:<account-id>:database/*",
    "arn:aws:glue:<region>:<account-id>:catalog"
  ],
  "Condition": {
    "Bool": {
      "glue:EvaluatedByLakeFormationTags": true
    }
  }
}
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

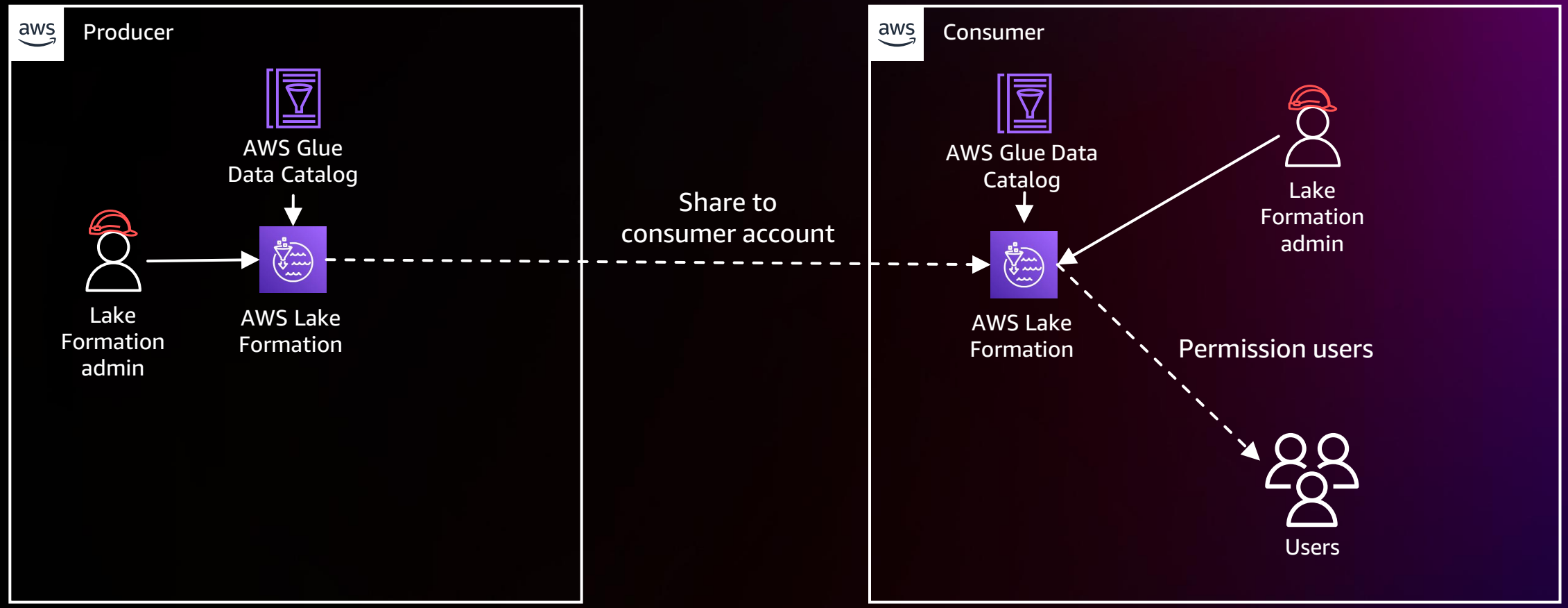
NEW!

LF-tagging now supports AWS Resource Access Manager (AWS RAM) for cross-account sharing



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

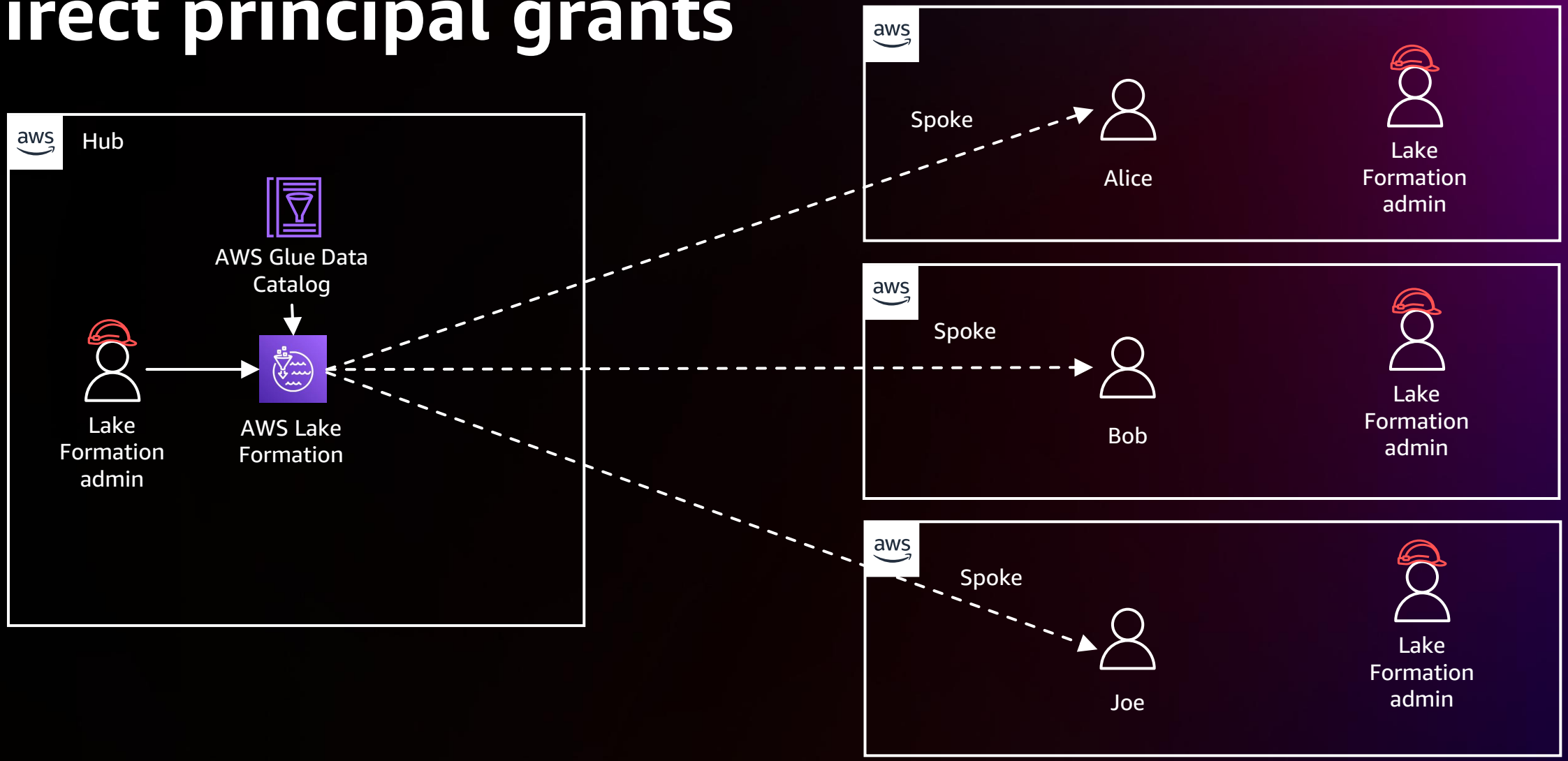
Cross-account sharing and delegation



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

NEW!

Centralize permissions with cross-account direct principal grants



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Q&A

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Mert Hocanin
hocanint@amazon.com

Purvaja Narayanaswamy
npurvaja@amazon.com



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.