



16 Sep, 2025

A Practical Introduction to Data Access Management

- Varun Sharma, Solution Architect, IPS
- Deep Mani, Principal Advisory Consultant, IPS

Where data & AI come to **LIFE**

Housekeeping Tips



- Today's Webinar is scheduled for **1 hour**
- The session will include a webcast and then your questions will be answered live at the end of the presentation
- All dial-in participants will be muted to enable the speakers to present without interruption
- Questions can be submitted to "All Panelists" via the **Q&A option** and we will respond at the end of the presentation
- The webinar is **being recorded** and will be available on our [Success Portal](#) - where you can download the **slide deck** for the presentation. The link to the recording will be emailed as well.
- Please take time to complete the **post-webinar survey** and provide your feedback and suggestions for upcoming topics.

Feature Rich Success Portal



Bootstrap trial and
POC Customers



Enriched Customer
Onboarding
experience



Product Learning
Paths and Weekly
Expert Sessions



Informatica
Concierge



Tailored training and
content
recommendations

More Information



Success Portal

<https://success.informatica.com>



Communities & Support

<https://network.informatica.com>



Documentation

<https://docs.informatica.com>



University

<https://www.informatica.com/in/services-and-training/informatica-university.html>

Safe Harbor

The information being provided today is for informational purposes only. The development, release, and timing of any Informatica product or functionality described today remain at the sole discretion of Informatica and should not be relied upon in making a purchasing decision.

Statements made today are based on currently available information, which is subject to change. Such statements should not be relied upon as a representation, warranty or commitment to deliver specific products or functionality in the future.

Agenda

1 Introduction – CDAM

2 Design Patterns – Policy Enforcement

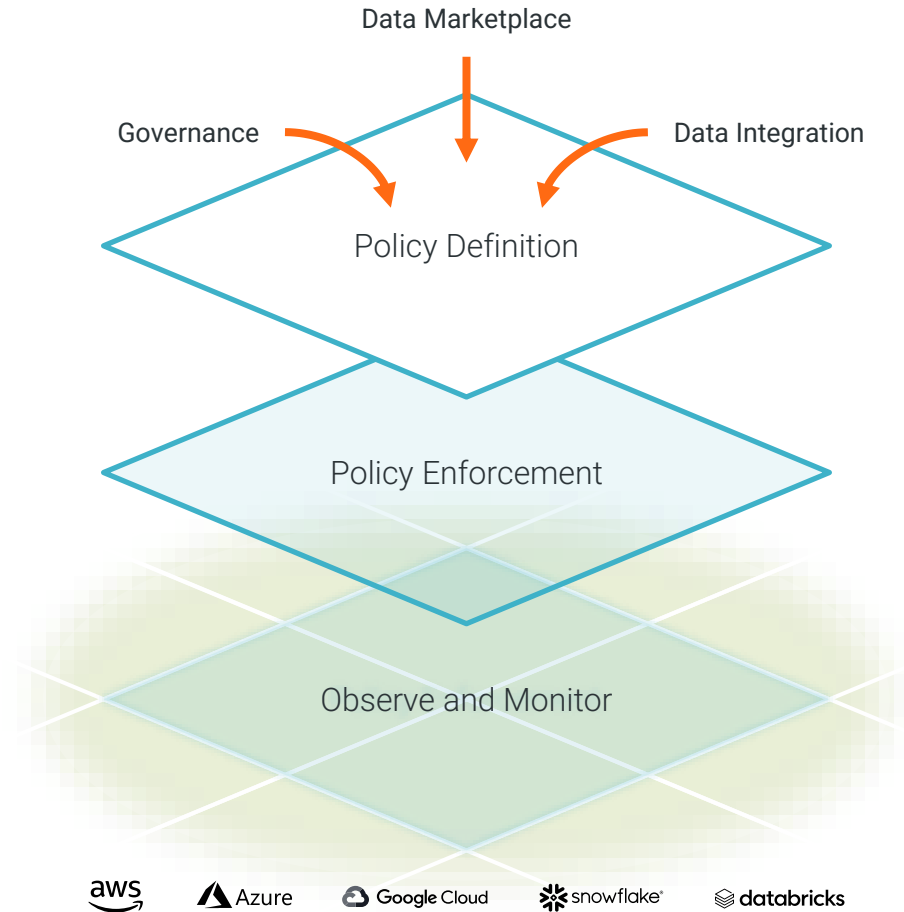
3 Sizing

4 Change Management/User experience

Informatica's Data Access Management

Ensure the right people have access to the right data at the right time

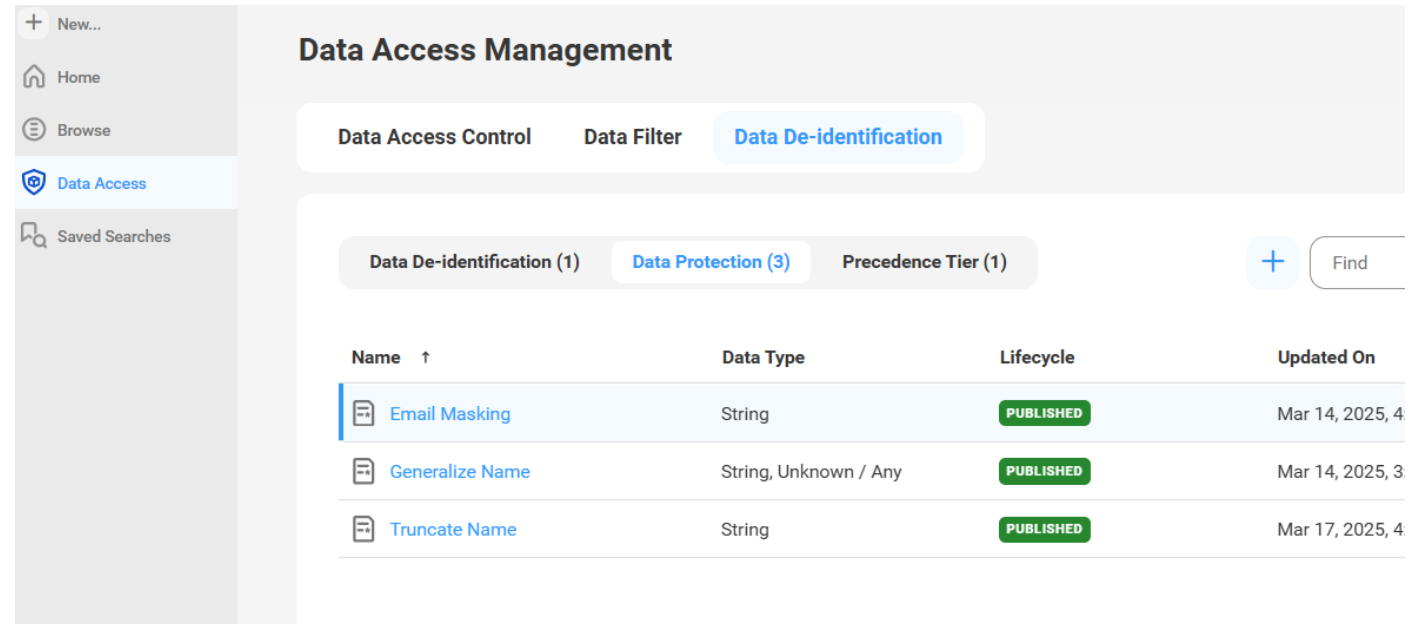
- Metadata-driven policies, universal enforcement
- Leverage discovery and classification
- Defined in one place, enforced everywhere
- Re-usable, scalable, logical policies
- Broad range of policy enforcement points
- Streamline access requests
- Observe, monitor, and audit data access






Defined in one place, enforce everywhere

Data Access Management is accessible via Data Governance and Catalog interface. Use Data Access Management page to develop policies that can be applied within Data Operation through Data Integration or self-service access through Data Marketplace.

- Intuitive, no-code policy authoring to align data access management with approved business use
- A comprehensive range of controls to minimize risk and preserve utility
- Use conditional logic to compose rules mapping data classifications and contextual attributes to controls



The screenshot displays the 'Data Access Management' interface. On the left is a navigation sidebar with options: '+ New...', 'Home', 'Browse', 'Data Access' (highlighted), and 'Saved Searches'. The main content area is titled 'Data Access Management' and features three tabs: 'Data Access Control', 'Data Filter', and 'Data De-identification' (selected). Below the tabs, there are three sub-tabs: 'Data De-identification (1)', 'Data Protection (3)', and 'Precedence Tier (1)'. A '+ Find' button is located to the right of these sub-tabs. The main area contains a table with the following data:

Name ↑	Data Type	Lifecycle	Updated On
 Email Masking	String	PUBLISHED	Mar 14, 2025, 4
 Generalize Name	String, Unknown / Any	PUBLISHED	Mar 14, 2025, 3
 Truncate Name	String	PUBLISHED	Mar 17, 2025, 4

Re-usable, Scalable, Logical Policies

There are following types of policies to protect data and control access to your data:

- Data access control policies - grant groups of users read, write, or delete access to tables or views
- Data filter policies - restrict or limit which records Data Access Management delivers to users
- Data de-identification policies – de-identify sensitive data while retaining data utility

The image displays two screenshots of the Data Access Management interface. The left screenshot shows the 'Data Filter' tab selected, displaying a table with one policy: 'Country Filter'. The right screenshot shows the 'Data De-identification' tab selected, displaying a table with one policy: 'PII Masking'.

Data Access Management - Data Filter

Name ↑	Lifecycle	Status
Country Filter	PUBLISHED	ENABLED

Data Access Management - Data De-identification

Name ↑	Precedence Tier	Lifecycle
PII Masking	PII Tier	PUBLISHED

Data Filter - Conditions & Rules

The **condition** defines when the policy will be triggered, while the **rule** specifies the actions that will be executed as part of policy.

Country Filter
DATA FILTER

Overview **Conditions** Rules Relationships Stakehol

Conditional Trigger

Activate this Data Filter **WHEN** the following attributes are present. Remove all conditional tri

Activate If

Or

User Group is any of Data Consumers

Rules (1)

Country Filter

Conditions

Or

Usage Context is any of Analytics

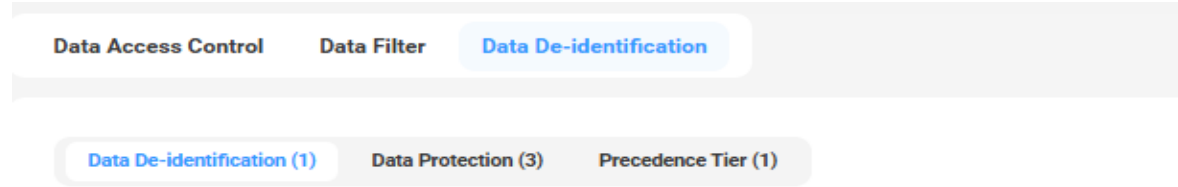
Filter

Or

Class Country ISO Code String is not any of NZ AU

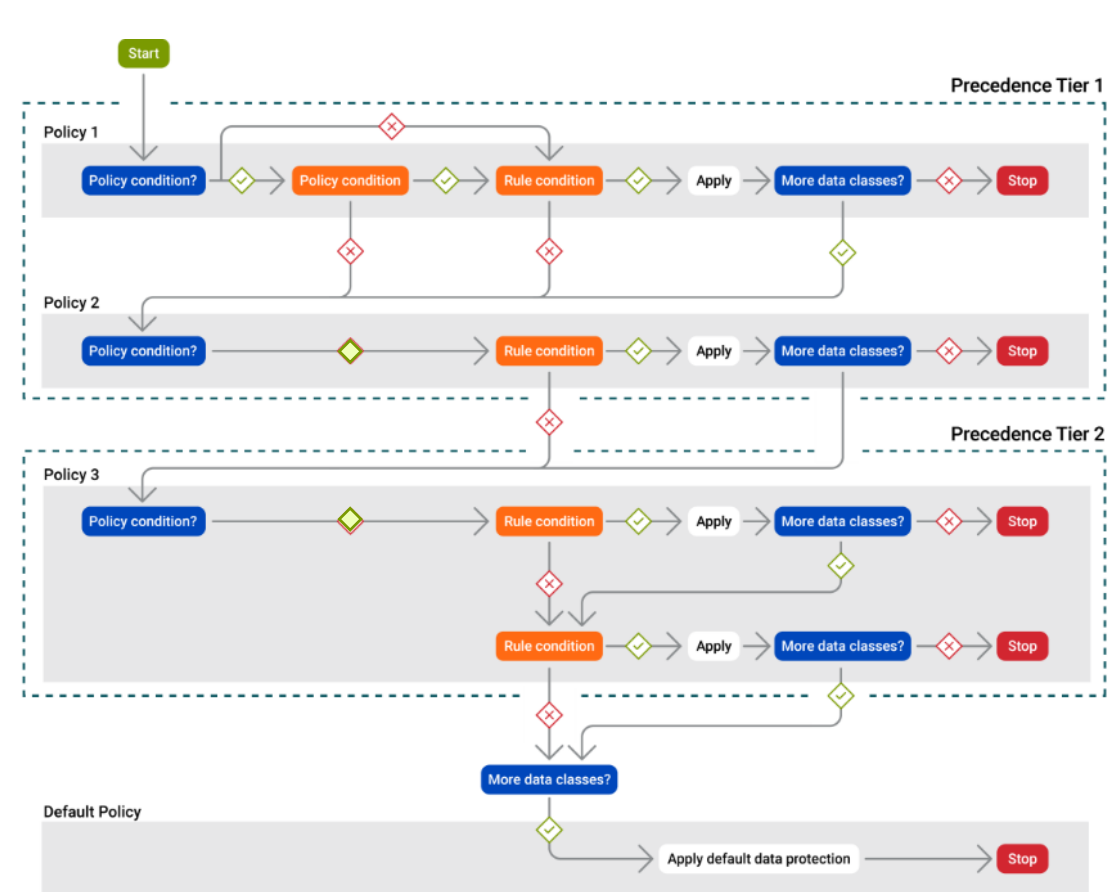
Then Deny Access to Records

Data De-identification



Precedence tiers

- The priority and sequence of evaluating data de-identification policies and applying data protections.
- Data Access Management processes based on rank from lowest integer to highest.
- Within each precedence tier, Data Access Management processes data de-identification policies from top to bottom.






Data De-identification

Transform data to de-identify sensitive data using a range of data protection technique.

Data Protection technique includes:

- **Tokenize** to maintain the original format and replace input with randomly generated equivalents
- **Generalize** to convert input to a common year or month
- **Truncate** to keep only minimal contents visible
- **Constant value** to mask string value with piece of text
- **Hashing** to replaced input value to hashed value
- **Substitute value** to replaces input values with readable substitutes

Name ↑	Data Type	Lifecycle
 Email Masking	String	PUBLISHED
 Generalize Name	String, Unknown / Any	PUBLISHED
 Truncate Name	String	PUBLISHED

Email Masking

DATA PROTECTION

Overview **Techniques** Stakeholders

Techniques (1)

String

Technique Type:
Tokenize

Regular Expression:
[a-z]{1,10}\@[a-z]{5}\.com

Consistency Behavior:
Randomly Tokenize

Data De-identification

The image displays the Informatica PII Masking configuration interface. The main header is "PII Masking" with the subtitle "DATA DE-IDENTIFICATION". Below the header is a navigation menu with tabs for "Overview", "Conditions", "Rules", "Relationships", "Stakeholders", and "Tickets".

The "Conditions" tab is selected, showing a "Conditional Trigger" section with the instruction: "Activate this Data De-identification WHEN the following attributes are present. Remove all conditional triggers to allow".

Under "Activate If", there is a rule configuration box containing an "Or" connector and a condition: "User Group is any of Data Consumers".

The "Rules" tab is also selected, showing a "Rules (1)" section with a "Name Masking" rule. This rule is configured with the following conditions and actions:

- Conditions:** An "Or" connector followed by "Data Entity Classification is any of PII".
- Field Level De-identification:** A "Then" connector followed by two actions:
 - "Class First Name protect with Generalize Name"
 - "Class Email protect with Email Masking"

CDAM Policy Enforcement

3 ways to achieve this



Integration into CDI.

This is your data copying mechanism. Data is read from source, policy applied, de-identified copy is written to target.



Dynamic de-identification (the proxy).

The underlying data is never changed. The proxy is a middleware layer between the data consumer (in DBeaver, e.g.) and the database. The data consumer connects to the proxy and issues queries. The proxy sends these queries to the underlying database, gets the result set, applies the policy to the result set, and sends the de-identified result set to the data consumer.



Pushdown, a.k.a. Native Access Controls.

For now, this is at an object-level only (tables/views). You create a Data Access Control policy that dictates a group has read, write, or delete permissions on some set of technical assets (tables/views). CDAM converts this to GRANT statements on the native platform, calls the native platform, and issues the appropriate GRANT statements. Effectively we sync the access controls in our policy with the access control mechanism of the native platform. We support Databricks and Snowflake.

Design Patterns- CDI CDAM

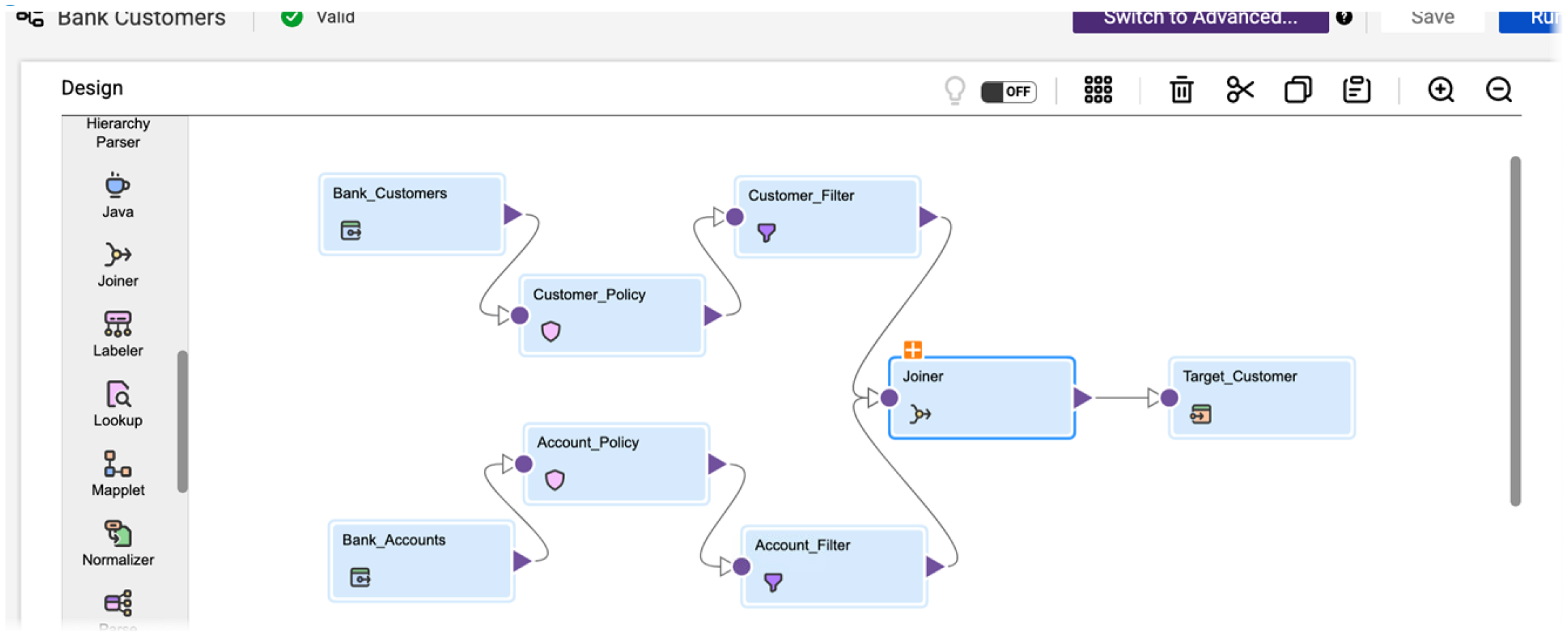
Multiple tables in source – Option 1

The screenshot displays the Informatica Designer interface. The top section, titled "Design", shows a workflow diagram with three components: "Source", "AccessPolicy", and "Target", connected by arrows. The "Source" component is selected, and its properties panel is open below. The "Properties" panel has tabs for "Properties", "Preview", and "Source". The "Source" tab is active, showing the "Details" section. The "Connection:" field is highlighted with an orange box and labeled "Connection Name". The "Source Type:" dropdown is set to "Query". The "Query:" field contains a SQL query, with the word "TABLE" highlighted in an orange box. The query is as follows:

```
SELECT DISTINCT CPA.*
FROM PRISM_BACKUP_CLIENT_POLICY
WHERE PRISM_BACKUP_CLIENT_POLICY.CPA,
PRISM_BACKUP_CLIENT_POLICY.CPA,
PRISM_BACKUP_CLIENT_POLICY.CPA,
```

Design Patterns- CDI CDAM

Multiple tables in source –Option 2



Design Patterns- CDI CDAM

Multiple tables in source –Option 3

Create views

Create views in applications for multiple tables

- Use views in the catalog and CDAM steps

Design Patterns- CDI CDAM

Pro's/Con's

Considerations	Option1(SQ)	Option2(JOIN)	Option3(VIEWS)
Cost	Less than option 2	IPU can be more compared to option 1 and option 3	Less than option 2
Changes in Application/DB	SQL required for ETL	No changes joins are done at ETL	More Change Management on Application side

Design Patterns- CDI CDAM

Parameters : Use of reference id in Access Policy transformations

• Sample Configuration in the CDI > Mapping :

1 Definition 2 Input Parameters

✓ The template and parameters are valid.

Other Parameter Details

ConsumerParam:*

DataAssetParam:*

DemoParam:*

Run Preview for Mapping_Employee_CDM

1 Definition 2 Input Parameters

Failed to create the following transformation: 'AccessPolicy' (500 Internal Server Error: '{"message": "com.informatica.ccgf.utility.sal.rest.ApiException: /cdmp-marketplace/api/v1/cdam/manifest :: Bad Request", "stackTrace": null}')

Other Parameter Details

Param:*

Validate

For the parameters to be used in the Access Policy Transformation , we need to make use of the Asset ID of the Usage Context / Consumer / Data Asset .

Design Patterns- CDI CDAM

Avoid Schema Mismatch

In CDI , when using snowflake as Source in 'Access Policy Transformation', all column values are redacted to NULL. The session logs indicate an error:

```
TRANSF_1_1_1> AccessPolicy_0 [2025-06-12 04:24:19.420] [ERROR] Result failed. Reason: Mismatch between input record schema and the Privitar Platform schema. Privitar schema has 6 field(s) with names: [ADDRESSID, CITY, PARTYID, STATE, STREET, ZIPCODE] while the input record has 8 field(s) with names: [ADDRESSID, CITY, COUNTRY, EMAILID, PARTYID, STATE, STREET, ZIPCODE]
```

Sizing

- Asset Volume & Concurrency: More data assets and simultaneous tasks demand greater processing capacity (CPU, memory, Secure Agents).
- Data Characteristics: Large, high-velocity data volumes increase resource consumption.
- Policy Complexity: Metadata-driven policies can simplify management, but complex policies (row, column, cell-level controls) demand more processing.
- Native Platform Leverage: Utilizing "policy pushdown" to native controls in platforms like Snowflake or Databricks can reduce Secure Agent workload.

CDAM-Marketplace Design Pattern

Navigation menu:

- Browse
- Search
- Compare
- My Data
- My Orders
- Tasks
- History
- Setup

Current user: KL_DC_STUDE... ACC-27

Delivery

TARGET	● CDAM
DESCRIPTION	test CDAM
TYPE	Manual
MANAGED ACCESS ⓘ	Enabled
FORMAT	JDBC
METHOD	URL
SYSTEM	CDAM
LOCATION ⓘ	jdbc:informatica:data-access://hostname@informatica.com:51320?request.access=bdde39c1-13d3-11f0-a4fe-67e36493f41a

Right sidebar:

- CDAM
- CERTIFIED USE
- ORDER
- 2 Apps
- USAGE CONTENT
- BUSINESS JUSTIFICATION
- APPROVAL

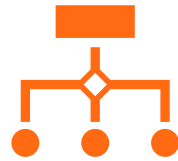
CDAM-Change Management

Workflow- User Experience



Controlled and Secure Policy Editing:

Users don't edit live data access policies directly. Instead, they propose changes in a safe, version-controlled "draft" mode. This prevents accidental or unauthorized modifications to who can access sensitive data.



Automated Approval Workflows:

Once a change is proposed, the system automatically routes it to the correct stakeholders (like Data Owners or a governance board) for review. This eliminates manual emails and ensures a formal, consistent approval process is always followed.



Clear, Transparent Review:

Approvers are shown a simple side-by-side comparison highlighting exactly what has changed (e.g., a masking rule being removed). This allows for quick, informed decisions without having to decipher complex technical settings.



Automated Enforcement and Auditing:

After final approval, the new policy is automatically deployed and enforced on the underlying data platform (like Snowflake or Databricks) with no manual steps required. The entire lifecycle—from request to enforcement—is logged in a complete audit trail for compliance.

Summary

- Permissions: https://knowledge.informatica.com/s/article/000242364?language=en_US
- CDAM: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/The_Data_Access_Management_page.html
- Data filter: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Data_filter_policy_behavior.html
- Data De-identification: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Creating_data_de-identification_rules.html
- Data Protection: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Data_protections.html
- Precedence tiers: https://onlinehelp.informatica.com/IICS/prod/DGC/en/index.htm#page/ae-data-accessmanagement/Precedence_tiers.html



Thank You

Where data & AI come to **LIFE**

