**Scenario 1: Snowflake Credentials Only (No Direct AWS Access)**

**Goal:** FIS provides Worldpay with full Snowflake access while managing all AWS infrastructure. Worldpay has no access to the FIS AWS environment.

**Setup:**

* **FIS (AWS Account):**
  + FIS has its own AWS account where it deploys and manages the Snowflake instance for Worldpay.
  + FIS manages all related AWS resources (EC2, S3, VPC, etc.).

**Snowflake Deployment:**

* FIS deploys Snowflake within its AWS account.

**Snowflake User Management (No AWS AD):**

* **Onboarding New Users:**
  + FIS creates new Snowflake user accounts manually for each Worldpay user or configures SCIM with their IDP. FIS also assigns the necessary roles and privileges within Snowflake.
  + FIS provides Worldpay users with their Snowflake connection details, username, and password.

**Worldpay Access:**

* Worldpay users connect directly to the Snowflake instance using their FIS-provided credentials.

**Responsibilities:**

* **FIS (AWS):**
  + AWS infrastructure management for Worldpay's Snowflake deployment.
  + Snowflake virtual warehouse scaling, monitoring, and storage management.
* **Worldpay:**
  + Data loading, transformation, and analysis within Snowflake.
  + Internal Snowflake user management and access controls for their team.

**AD Group Integration at AWS:**

* None: Worldpay has no direct access to FIS AWS environment, so no AD integration at FIS AWS side is required for this scenario.

**Pros:**

* Security: Worldpay has no access to FIS's AWS infrastructure, greatly reducing risk.
* Simplicity: Worldpay focuses solely on using Snowflake.
* Clear Responsibility: Clear delineation of responsibilities between FIS and Worldpay.

**Cons:**

* Limited Flexibility: Worldpay must rely on FIS for all infrastructure-related changes.
* Requires Strong Internal Controls: FIS needs robust monitoring of both its AWS and Snowflake resources.

**Scenario 2: Limited AWS Management Access (with Restrictions)**

**Goal:** FIS grants Worldpay's Snowflake team limited, restricted AWS management access via AD groups, allowing them to perform specific infrastructure-related tasks.

**Setup:**

* **FIS (AWS Account):**
  + FIS maintains its AWS account and the core AWS infrastructure for the Snowflake deployment.
* **IAM Role for Worldpay (with AD Integration):**
  + FIS creates a dedicated IAM role for Worldpay's Snowflake team.
  + FIS configures an IAM Identity Provider to trust Worldpay's AD domain (or potentially a shared domain, depending on the setup).
  + The IAM role's trust policy allows users from specific Worldpay AD groups to assume the role.
  + The IAM role is assigned a strict IAM policy based on resource tags or names, allowing only specific actions.

**Snowflake Deployment:**

* FIS deploys Snowflake. They can delegate management of Snowflake internal users to Worldpay or control them internally based on the agreement.

**Worldpay Access:**

* Worldpay users from the defined AD groups assume the FIS-provided IAM role using their Worldpay AD credentials for access to the AWS environment.
* Worldpay users access Snowflake using their Snowflake user credentials.

**Responsibilities:**

* **FIS (AWS):**
  + AWS account management, core infrastructure setup, management of the IAM Identity Provider and the restricted IAM role.
  + Security policies for AWS resources.
* **Worldpay (Snowflake Team):**
  + Snowflake deployment and management within FIS environment (scaling, storage etc.).
  + Limited AWS management tasks as permitted by the restricted IAM role.
  + Managing snowflake users if delegated.

**AD Group Integration at AWS:**

* Yes: The IAM role's trust policy explicitly references the Worldpay AD IdP and the required AD group. Only members of the specified AD groups can assume the IAM role.

**Snowflake User Onboarding:**

* Snowflake User Management (with or without SCIM): FIS may provide full administrative access within Snowflake for Worldpay or manage their Snowflake users themselves. If Worldpay manages their snowflake user, they will have complete control over this using the ACCOUNTADMIN role or SCIM.

**Pros:**

* Controlled access: AD groups used to control which Worldpay users can assume the IAM role.
* Increased Flexibility: Worldpay's Snowflake team can perform some AWS infrastructure tasks.

**Cons:**

* Significant Complexity: Requires intricate setup and management of IAM, IdP, and IAM policies.
* Increased Risk: A misconfigured role or policy could lead to security problems.
* Requires Continuous Monitoring: Both FIS and Worldpay must monitor their respective activities.

**Scenario 3: Limited AWS Read-Only Access (for Auditing/Visibility)**

**Goal:** FIS grants Worldpay read-only access to monitor their Snowflake infrastructure using their AD groups.

**Setup:**

* **FIS (AWS Account):**
  + FIS manages the AWS account and all infrastructure components.
* **IAM Role for Worldpay (with AD Integration):**
  + FIS creates an IAM role that allows read-only access to AWS resources relevant to Snowflake.
  + FIS configures an IAM Identity Provider to integrate with Worldpay's AD.
  + The IAM role's trust policy is defined to allow users from specific Worldpay AD groups to assume this role.
  + The IAM policy assigned to the IAM role provides read-only permissions (e.g., ec2:Describe\*, s3:Get\*, cloudwatch:Get\*, logs:Get\*, logs:Describe\*).

**Snowflake Deployment:**

* FIS deploys Snowflake.
* They can delegate management of Snowflake internal users to Worldpay or control them internally based on the agreement.

**Worldpay Access:**

* Worldpay users from the designated AD groups access AWS with their AD credentials to assume the IAM role for the required read-only access.
* Worldpay users access Snowflake using their Snowflake user credentials.

**Responsibilities:**

* **FIS (AWS):**
  + AWS account management, configuration of the IAM Identity Provider, and the IAM role management.
  + Snowflake deployment and management if needed.
* **Worldpay:**
  + Monitoring AWS infrastructure.
  + Managing Snowflake access and data operations.

**AD Group Integration at AWS:**

* Yes: The IAM role's trust policy is tied to specific Worldpay AD groups.

**Snowflake User Onboarding:**

* Snowflake User Management (with or without SCIM): FIS may provide full administrative access within Snowflake for Worldpay or manage their Snowflake users themselves. If Worldpay manages their snowflake user, they will have complete control over this using the ACCOUNTADMIN role or SCIM.

**Pros:**

* Visibility: Worldpay can monitor the AWS infrastructure supporting their Snowflake deployment.
* Controlled access: Read-only access based on AD groups.
* Reduced risk: Cannot make modifications to AWS resources.

**Cons:**

* More complexity with IAM and IdP setup.
* Requires careful management of read-only access policies.

**Comparison Table:**

| **Feature** | **Scenario 1: Snowflake Credentials Only** | **Scenario 2: Limited AWS Management Access** | **Scenario 3: Limited AWS Read-Only Access** |
| --- | --- | --- | --- |
| AWS Access Level (Worldpay) | None | Limited Management Access with restrictions | Read-Only |
| AWS Resource Management | FIS (Fully Managed) | FIS (Mostly Managed, Worldpay has restricted access) | FIS (Fully Managed, Worldpay can monitor) |
| AWS AD Integration | No (no AWS access) | Yes (IAM role linked to Worldpay's AD groups) | Yes (IAM role linked to Worldpay's AD groups) |
| Complexity (FIS) | Low | High | Medium |
| Security Risk | Lowest (Worldpay has no AWS access) | Higher (Potential for misuse by misconfigured policy) | Low (Read-only access only) |
| Flexibility (Worldpay) | Low (reliant on FIS for all AWS actions) | Medium (Can perform some AWS tasks based on the role) | Medium (visibility only) |
| Responsibility (FIS) | Full control of all AWS & Snowflake resources | AWS management, security policy management, and restricted IAM role management | AWS management, and IAM role for readonly access management |
| Responsibility (Worldpay) | Manages Snowflake user access and all operations within Snowflake | Snowflake deployment, and management and limited AWS tasks | Snowflake data operations and monitoring the underlying infrastructure |
| Snowflake User Management | Manual or SCIM controlled by FIS, or if delegated, controlled by Worldpay | Manual or SCIM controlled by FIS, or if delegated, controlled by Worldpay. | Manual or SCIM controlled by FIS, or if delegated, controlled by Worldpay. |
| AWS Auth for Worldpay | Not needed. | Worldpay's AD via IAM role AssumeRole | Worldpay's AD via IAM role AssumeRole |