# **Administrator Best Practices and Tips for Futureproofing your Databricks Account:**

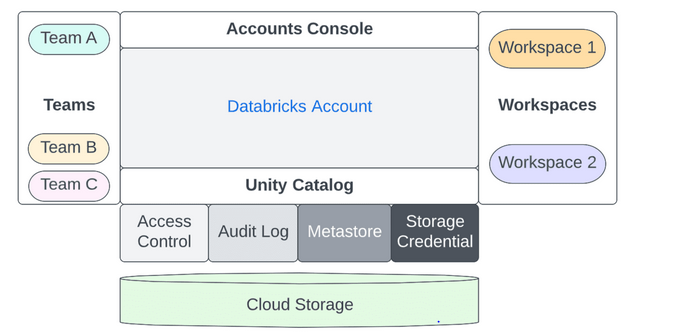
**Administrative considerations of managing a workspace, such as how to**:

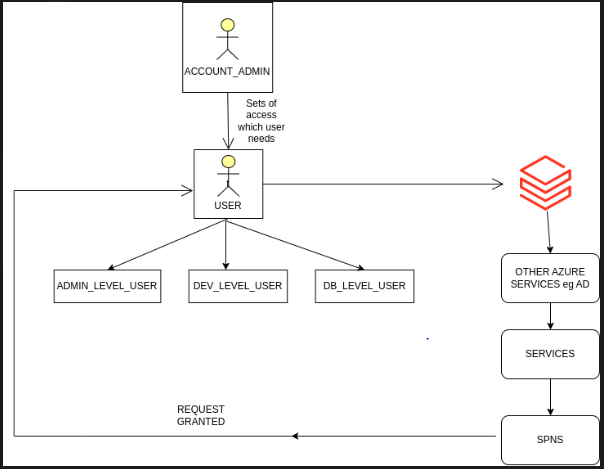
* Set up policies and guardrails to future-proof onboarding of new users and use cases
* Govern usage of resources
* Ensure permissible data access
* Optimize compute usage to make the most of your investment

To state this in a different way, we can break down the primary responsibilities of an

**Account Administrator and workspace admin** as the following**:**

**Account admin role:**

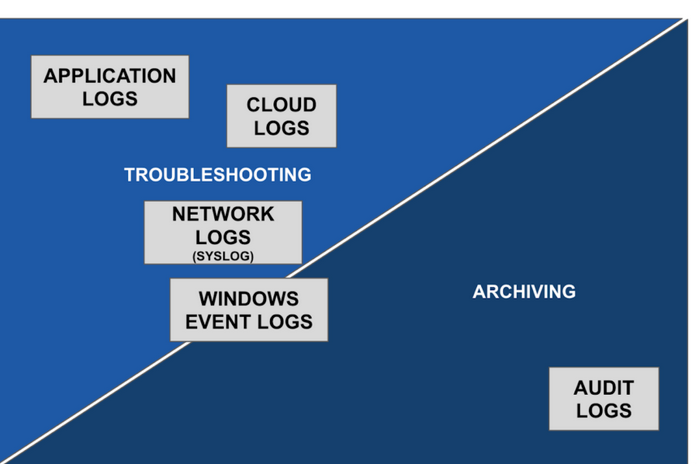


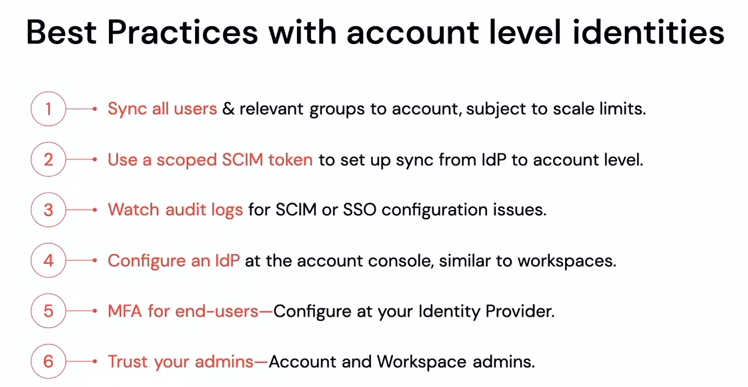
* **Identity Management**: Provisioning principals and SSO for workspace access via identity federation.
*   
  **Example**:   
  Integrating Azure Active Directory with Workspace's allows users to log in once and access various resources seamlessly.  
    
  Do’s:  
  **Do Use Federated Identity Management**:
  + Leverage federated identity solutions to allow users to authenticate across multiple systems and applications without needing separate credentials.

**Do Plan for User Lifecycle Management**:

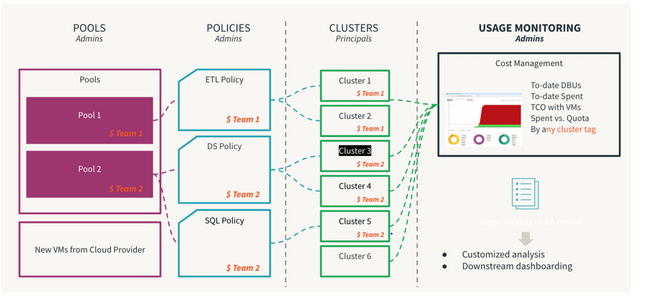
* + Establish processes for onboarding, offboarding, and role changes to ensure that access rights are appropriately managed throughout the user lifecycle.

1. **Don't Allow Unmonitored Access**:
   1. Avoid granting access to systems without monitoring. Implement logging and monitoring to track user activity and detect anomalies.

* **Audit Logging**: Implementing audit logs for activity tracking.  
  
* **Usage Monitoring**: Tracking account-level usage and billing metrics.  
  Example: Based on the capacity planned, how the scaling is done to observe cost metrics. Either from tableau or azure billing.  
  **Example**: Quarterly cost estimate monitoring can be efficient
* **Workspace Organization**: Creating and structuring workspaces as needed.  
  **Example**:Managing Workspaces of different environments such as dev, Prod, NPE.
* **Workspace Management**: Overseeing storage, credentials, and network settings.  
  **Example**:  
  Workspace admin should proactively check with solution architect on capacity planning, security principles and remote network planning for the traffic of workspace.
* **Workload Automation**: Automating development workloads with Infrastructure as Code (IaaC).  
  Example : Azure devops, terraform
* **Feature Control**: Enabling/disabling account-level features like serverless workloads.  
  **Example**:  
  For monthly patching of update and yearly upgrade planning across infrastructure. SIQ approval should be from Account admin and solution Architect.



**Workspace admin role:**



* **Role Assignment**: Assigning user/admin roles to principals at the workspace level.  
  Example:  
    
  Users: User identities recognized by Databricks and represented by email addresses.

Service principals: Identities for use with jobs, automated tools, and systems such as scripts, apps, and CI/CD platforms.  
  
**Example**:  
Users roles should be updated, as further modifications can be made in the workspace, table, clusters etc. To avoid multiple follow-ups with the previous users if the tables or cluster are created under a particular user.  
As we might get the issue while moving managed table to external table.

* **Entitlement Management**: Setting appropriate access control lists (ACLs) for principals.
* **SSO Configuration**: Optionally enabling Single Sign-On at the workspace level.
* **Cluster Policies**: Defining policies to manage computer resources and orchestration (jobs/pipelines/workflows).
* **Feature Control**: Turning features on/off at the workspace level.
* **Security Controls**: Implementing data protection measures, including restricting DBFS and preventing data downloads.
* **Access Control**: Enabling access control for workspace objects, clusters, jobs, and tables.
* **Log Delivery**: Setting up storage for cluster logs through cluster policies.  
  **Example**: Plan the storage of log age cycle to avoid space issues.

## Recommendations and best practices

Best practices:

* Clearly define roles for Account and Workspace admins ensure appropriate workflow management across all workspaces.
* Centralized principal management via Account Level Identities simplifies administration, with SSO, SCIM, and Audit Logs recommended at the account level.
* Cluster Policies offer self-service guardrails, with account admins providing default policies and workspace admins adding specific controls.
* Account admins can monitor workload consumption across all workspaces through the accounts console.
* Use Delta Live Tables for new pipelines and Unity Catalog for user management and data access control.

Ref: <https://www.databricks.com/blog/2022/08/26/databricks-workspace-administration-best-practices-for-account-workspace-and-metastore-admins.html>