|  |  |
| --- | --- |
| **What are the core components of SailPoint IGA?**  **Business** **need** - Access Certification,Access Request , Automated Provisioning , Password Management , Policy Management,  **Business model** - Policy Model, Role Model , Workflow Engine , Identity Warehouse, Reporting , Risk Model ,  **Business data** - Users • Applications • Data ,  **Integration Framework** = Connectors APIs Plugins  **Business applications** - Cloud apps, On-prem apps, 3rd party Integrations  **Compliance Manager** - On-boarding app -Automate access certifications, policy management, and audit reporting to streamline compliance processes and improve the effectiveness of identity governance  **Lifecycle Manager** - Lifecycle Manager helps your organization manage changes to access through user-friendly self-service requests and lifecycle events for fast, automated delivery of access to users.  **Lifecycle Manager** – Provisioning related activitiesAccess requests, creation of identities, creation of an entitlement, managing passwords  **Artificial Intelligence and Machine Learning** - Apply advanced governance capabilities, using the power of SailPoint Predictive Identity to discover suspicious or anomalous access, maintain continuous compliance and enjoy greater productivity across the entire organization.  **Privileged Account Management Module** -IdentityIQ Privileged Account Management module provides a standardized approach for extending critical identity governance processes and controls to highly privileged accounts, enabling IdentityIQ to be used as a central platform to govern standard and privileged accounts.  **Connectors and Integration Modules** -SailPoint's extensive connector library and advanced integrations let organizations connect and govern access to all types of digital identities across evolving on-premises, hybrid, and cloud environments.  **Cloud Access Management** -Discover and protect access across all your cloud platforms and resources. SailPoint Cloud Access Management allows you to get complete visibility and control across your cloud infrastructure and workloads, detect potential anomalies, and better enforce access policies across all users  **Password Manager** -IdentityIQ Password Manager delivers a simple-to-use solution for managing user passwords across cloud and on-premises applications policies from any desktop browser or mobile device.  **Access Risk Management** -Access Risk Management automates real-time access risk analysis, simplifies GRC processes, and even identifies a potential user's risks before access is granted.  **What is the difference between trusted and target application?**  **Trusted application** – Application from which data is imported to SailPoint. It can be authoritative or non-authoritative.Trusted application is any repository for employee information for your enterprise that represents the primary and most trusted information about identities, such as a human resources application.  **Target Application** – Application to which data is provisioned from SailPoint.  Target applications enable Data Management to be used as a primary gateway to integrate data between different source systems and target applications.  IdentityIQ with our library of connectors and advanced integrations to intelligently govern access to all your essential business applications.  **SailPoint installation steps**  1.unzip the version file and copy the identityIQ.war file and its patch ( jar ) file .  2. goto tomcat and and paste the identityIQ folder.  3. deploy the war file.  4. add extended identity attribute ( in real time you can skip this step ).  5. generate schema.  6. create database.  7. initialize default sailpoint/system object.  8. deploy the patch file  9. upgrade the database  10. apply the patch  11. add the log path  12. start the tomcat server  13. configure email logs  **Authoritative application onboarding steps.**  1.Create an application  2. run aggregation task - data will be pull  3.configure identity mapping  4.configur manager correlation  5.run refresh identity cube task ( Data would be updated on identity cube )  **Defining Non-Authoritative Applications**  **Define application**  • Select connector type  • Define account schema- Used to represent individual accounts  • Define group schemas (if needed) - Used to represent individual group rights  • Specify account correlation  • Define rules (if needed)  1. Connector Rules - Support Data Transformation operations • Connector Rules vary based on the connector type  2. Application Rules - Act on accounts/account groups (Resource Objects) • Available for all connector types  • Define aggregation task and schedule  **How to add a custom attribute and to source mapping for the same**  **add a custom attribute steps :-**  1.Click New Attribute or click an existing attribute to display the Edit Extended Attribute page.  2.Enter or change the attribute name and an intuitive display name.  3.Select the attribute type from the drop-down list, String, Integer, Boolean, Date, Rule, or Identity.  4.add more information for the extended attribute, as needed.  \*Enter a description of the additional attribute.  \*Select a category for the attribute.  \*Activate the Searchable option to enable this attribute for searching throughout the product.  \*Activate the Editable option to enable this attribute for editing from other pages within the product.  \*Mark the attribute as required. For string type attributes only.  \*Enter allowed values for the attribute. For string type attributes only.  \*Specify a default value.  5. Click Save to save your changes and return to the Edit Role Configuration page.  **Source Mapping Steps:-**  1.Go to Admin > Connections > Sources and select the source you want to update.  2.In the Accounts tab, select Create Account from the left panel.  3. select one of the following mapping types, and map the related attributes accordingly:Identity Attribute,Generator ,Static ,Disable  4.Select Save when you've finished mapping the source attributes.  **Explain High-level steps involved in trusted application on-boarding?**  1) Create an application  2) Run aggregation task - data will be pulled - only one activity is to pull data from source to SailPoint  3) Configure identity mapping  4) Configure manager correlation  5) Run refresh task  **What is use of SailPoint IGA product for organizations?**  It automates and streamlines identity processes and decisions such as access certification, lifecycle management, analytics, access modelling and role insights. As 84% of organizations have experiences a data breach, it is essential for an enterprise – no matter how large or small – to protect their business.  **What is the significance of:**  a. **detect deleted accounts**:- Compare current aggregated accounts with the accounts previously aggregated and report any deleted accounts.  b. **promote managed attributes** :- A managed attribute is the value of an account attribute that has been promoted to a first-class object in the IdentityIQ database so the system can track other data related to these attributes, such as a description or an owner.  c. **enable delta aggregation** :- Enable the connector to aggregate only those accounts that have changed since the last aggregation. This requires support by the connector.  d. **only create links if they can be correlated with existing identity** :- Check to updated existing identities, but not to create new identities if a match is not found  **How do we populate identity attributes and Manager date in SailPoint IIQ?**  **Identity attribute -** Log into SailPoint Identity IQ as an admin  Click on System Setup > Identity Mappings  Click New Identity Attribute  Enter the attribute name and display name for the Attribute  **Manager data** – Manager correlation rule builds and maintain the manager hierarchy  **What if we have multiple unique attributes in the source data how do you analyze data and which rule would you use?**  If it is a non-authoritative source, then we can see which unique attribute of identity is matching from 2 given unique attributes and the same we will be using for correlation.  If the above questions is referring to: Using two/multiple attributes how can we define unique attribute then for that we have build a custom correlation rule.  **What are the different type of properties available with respect to attribute in Sailpoint?**  There are 3 types of properties available with respect to attribute in SailPoint.:  1.**Managed**: If we set this property for the group attribute then respective group added under entitlement tab in Identity cube.  2.**Entitlement**: If we set this property for the group attribute then respective group added in entitlement catalog.  3.**Multivalued**: This is for setting multiple values for given attribute  **Application Accounts, Entitlements, Roles**  **an account** refers to a user's account on a supported source.  **Business Roles** identify affiliations or job functions by which users can be grouped. Roles are a form of digital identity, associated with permissions related to specific applications, defining what the member of the Role can or cannot do with their access.  **Entitlements** represent individual system. These application specific permissions are referred to as Entitlements, which provide a specific set of privileges, within a specific application.  Entitlements = low level of access  **What is the sequence of rule execution in SailPoint while application on-boarding?**  1.**Pre-Iterate Rule** - PreIterate rule runs once prior to aggregation  2**.BuildMap Rule** -Runs for every line in the file • Converts incoming data into map  3.**Managed Entitlement Customization Rule** - Set fields such as owner, requestable, or descriptions on ManagedAttributes (entitlements, groups)  4.**Customization rule** - Modify/normalize incoming account data prior to saving to an Identity  5.**Correlation rule** - Build and maintain account correlations  6.**Manager correlation rule** - Build and maintain manager hierarchy  7.**Creation rule** - Perform customizations at cube creation time Example: Set default IdentityIQ password  8.**PostIterate Rule** - PostIterate rule runs once after aggregation  **BeanShell** rule for data transformation  **Application Rules** –  Act on accounts/account groups (Resource Objects) • Available for all connector types  • **Correlation** **Rule** (when matching isn’t enough) - Build and maintain account correlations  • **Customization** **Rule** - Modify/normalize incoming account data prior to saving to an Identity  • **Managed Entitlement Customization Rule** - Set fields such as owner, requestable, or descriptions on ManagedAttributes (entitlements, groups)  • **Merged Map** **Rule** - If default merge capabilities aren’t enough, a rule here can control merging  • **Primarily used with Authoritative Applications**  **Manager Correlation Rule** - Build and maintain manager hierarchy  **Creation Rule** - Perform customizations at cube creation time Example: Set default IdentityIQ password  **Connector Rules** - Support Data Transformation operations • Connector Rules vary based on the connector type  **Aggregation & Correlation (**Non-authoritative application)   1. Non-authoritative application contains accounts 2. Application/Connector defines what to read, how to connect 3. Aggregation task runs 4. Connector reads accounts, tries to correlate to existing Identity Cubes 5. Positive Correlation – add account to existing cube 6. Unsuccessful Correlation – add account to new cube (mark as un-correlated)   **Identity Cube Creation Process**   1. Authoritative resource contains accounts 2. Application/Connector defines schema and how to connect to resource 3. Aggregation task runs 4. Connector reads accounts 5. IdentityIQ creates authoritative cubes 6. Identity Mappings define the creation of Identity Attributes | **What does “Identity Cube” represent in SailPoint application?**  All of the information associated with an identity, including all of their accounts on all sources, all attributes and entitlements of those accounts, as well as Identity Now attributes and entitlements such as the lifecycle state  **Identity Cube**  Term to refer to each unique identity stored in IdentityIQ repository. IdentityIQ repository means identity warehouse. its a representation of an individual employee in an organization and entire information .  Identity Cube contains a lot of details of perticular employee Examples: • Identity Attributes• Application Accounts• Entitlements/Roles• History • Risk Score• Policy Violations• User Rights (Capabilities/Scoping)  all are stored in object so that’s why its told as Identity Cube.  **QuickLinks**:-  QuickLinks are tasked-based links to frequently-used areas of IdentityIQ. An administrator can customize these links. Quick links are a collection of links to frequently used application pages, which allow users to complete common actions  **What is difference between identity attribute and application attributes?**  **identity attribute :-** Identity Attributes are used to describe Identity Cubes and by proxy describe the real-world user.  **application attributes :-** Use the Edit Application Configuration page to define extended application attributes not provided by the application connectors during aggregation.  **How does SailPoint IIQ know if it is trusted source during integration of any application?**  During aggregation application should be marked as authoritative application (checkbox should be checked). Then IIQ knows that it’s a trusted source.  **What is correlation and how many types we can define correlation?**  Correlation is the process IdentityNow uses to match and assign source accounts to identities  Account Correlation :- determine how application accounts are assigned to identities within IdentityIQ, using account and identity information  Manager Correlation :- configure how managers should be matched to identities.  **Define Group and Workgroup? How do you create Group and Workgroup**  **Group** - Groups are sets of Identities created based on the value of a single identity attribute.  Groups are created on the Group Configuration window (menu option Setup > Groups) by clicking Create New Group on the Groups tab.  **Workgroup** - is a Set of identities treated as a single IdentityIQ identity. Workgroups are used for Sharing of IdentityIQ responsibilities.  Workgroups are created on the Setup > Groups > Workgroups tab by clicking Create Workgroup.  IDM:- Identity governance management  **Provisioning/De-Provisioning**  User Provisioning (Account Provisioning) can be triggered by events like hiring, promotions, and transfers. Deprovisioning, on the other hand, refers to the process of disabling or removing a user's access to a system or application.  Deprovisioning is the act of removing user access to applications, systems, and data within a network. It's the diametric opposite of provisioning, which grants, deploys, and activates services for users in a system.  **What is Identity & Access Management?**  Identity and access management (IAM) ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs.  **Identity Warehouse**  In the SailPoint user dashboard, Identity Warehouse is a typical Warehouse where all identities are maintained  **Identity Refresh**  Refresh identity tasks scan all identities to ensure that all identity information is up-to-date and accurate  **Refresh task** :- to reflect the changes of identity cube data in sailpoint we run a refresh task. Update identity attributes from the application account attributes, and through calculations  **Use of refresh** :- to check policy violations, for risk scoring , to trigger life cycle events ( ex. Joiner , movers events) , to get notifications .  **Aggregation task** :- is used it to pull the data from the source application into sailpoint. Read data from applications to account attributes  **Aggregation**  Reconciliation is a term used in Identity Management for recognizing changes to Identity attributes and their subsequent synchronization with other user stores or an Identity Manager.  In SailPoint IIQ Identity Management system reconciliation is referred as Aggregation.  **Reconciliation**:- Reconciliation is a term used in Identity Management for recognizing changes to Identity attributes and their subsequent synchronization with other user stores or an Identity Manager.  **What is the significance of identity and display attributes in Account schema?**  Schemas define the data to be read from the resource  **Account schema** :-Identifies the attribute that holds user groupsIdentity attribute is used to pick up unique identities from application which will get unique identities.  **Accounts Schema** :- is represents a target resource account and define what data to read.  **Display attribute** is used as object name as it appears throughout the IIQ.  **Schemas**  • Definition of what data to read from the application and how to interpret that data  • **Schema types**  1.**Account (required)** • Represents individual accounts on a target resource (Active Directory or SAP Accounts, for example)  2.**Group (optional)** - Represent native account groups from target resource(LDAP Groups or Active Directory Groups, )  **Planning**  **Accounts Represent** user identities who may sign into that system Attributes Additional information associated with account  **Entitlements Specify** what actions a user is authorized to perform in a given application (i.e. access payroll)  **Account Groups** Specify set of security rights/permissions (i.e. Administrator) Membership in group provides user with group’s access rights  **What is a Workflow?**  A workflow is a set of steps that are completed every time a specific event occurs.  **Workflows are also used for**  • Role Creation • Identity Update • Identity Refresh • Identity Correlation • Entitlement Creation/Update • Sunrise/Sunset Role Assignment • Sunrise/Sunset Role Activation • Policy Violations  **What can Workflows do?**  • Check for Policy Violations • Gather information from users • Get Approvals/Generate Workitems • Send Emails • Audit • Adjust Provisioning Plan • Call Subprocesses (child workflows) • Run other Workflows • Really anything you can code in Java/BeanShell  **Workflows Types of Steps**  • Placeholders  • Used for visual cues and flow (Start/Stop)  • Code Steps  • Script or Rule – BeanShell code  • Call – call into compiled Java code  • Interaction Step  • Approval (Interaction)  • WorkItem created and provides a Form or Renderer  • SubProcess  • Execute a subprocess within the current flow  • Additional Options (implemented in XML)  • Wait (causes specific step to pause)  • Catches=Complete (guarantees step will run after workflow ends for whatever reason)  **Step Action: Script**  Step action is a BeanShell script of any complexity.  **Step Action: Call**  • Step action is to call a method in the StandardWorkflowHandler  • Method “audit” is called with arguments  **Step Action: Subprocess**  • Calls another workflow  • Defines parameter passing behavior to map subprocess variable using Return tags  **Step Action: Approval**  • Approvals are special kind of step that interacts with users  • Approval steps cannot have call or script actions or call subprocesses  • Approval objects may be nested  **Transitions**  • Define which step to pass control to  • Are valuated when the step action or approval completes  • Can be multi-valued  1. Evaluation is in the order specified in the transition  2. Transfer control to first transition that evaluates to true or which has no condition  **Pre-Conditions**  • A conditional statement executed prior to running a step  • Used to determine if the step should be executed  **How do you define account schema and group schema when the data is on 2 different CSV files?**  **For Account Schema –**  Add File path and Apply Filtering and Merging details in Settings Section.  Add Schema where Object Type will be Account.  Add Identity Attribute, Display attribute.  Add Type, Description and Properties for all attributes.  Put group attribute type as “group”. This will establish relation between account and group schema. Mark this attribute as Entitlement & Multi-Value.  **For Group Schema –**  In Configurations -> Settings, click on add object type = group  Add File path and Apply Filtering and Merging details in Settings Section.  Same Attribute which is added as type “group” in Account Schema should be added Identity attribute in Group Scheme.  No need to mark same attribute as Entitlement and Multi-Valued. As we have already defined that in Account Schema. Mark other attributes if required.  **Information on the cube is**  • Discovered - vie an aggregation • Requested - requested by user • Assigned - by normally whenever new person joined an organization • Calculated  **Any real time use case that you can think of which can be fulfilled using SailPoint IGA Product?**  onboarding of employees to the new org.  **Identity Mappings** used to add new Identity Attributes Example: Cost Center, Employment Status, Job Title • Identity Mappings define source for Identity Attributes  **Capabilities** :- Define what additional rights a user has within IdentityIQ . Control which menu options are available  **Scoping** :- The act of subdividing data into logical groups and granting access based on those subdivisions •.Scopes control the objects a user can see and act upon.  **Define Merging with real time scenario using below CSV?**  **Merging** is a process in which data from delimited file is transformed. In this process we will combine multiple cells having different values for single identity.  In above scenario given in CSV file, we can observe that there are multiple columns which are not unique. Such columns are  app2\_privileged, app2\_service, app2\_inactive, groupmbr  Multiple rows are present for same identity but with different values for these 4 columns.  As we can see column - app2\_privileged, app2\_service, app2\_inactive has Boolean values. That means it will have only single value either True or False. After uploading file it should read latest values for those fields. This will be handled at the time of populating data, latest/last record of that identity will be fetched.  After populating data only one column needs to be merged, which is “groupmbr”. Hence will implement this using default Merging option available in Configurations section. We will specify index column and column to be merged in Merging section.  **What is JML process?**  Joiners, movers, and leavers is a key HR process in most organizations. It's the HR process of handling employees from the perspective of joining the organization, moving departments/areas, and leaving the organization, essentially the lifecycle of an employee  **What are Lifecycle Events?**  • Activities that happen in the normal course of a person’s employment  • Joining the company (joiners)  • Changing departments/managers (movers)  • Leaving the company (leavers)  **Lifecycle Events can be created based on:**  • Attribute Change  • Manager Change  • Create  • Native Change  • Rule (Rule type = IdentityTrigger)  **Lifecycle Event: Native Change Detection**  • Definition: detect account changes that occur natively on an application  **Provided workflows**  • Manager approval for all native changes  • Email manager for all native changes  **Attribute synchronization**  • Automatically synchronizes changes to identity attributes with downstream systems |