CloudBees CI (Jenkins) Onboarding into SIAM  
  
Overview  
  
This document outlines the steps to onboard CloudBees CI (Jenkins) into the SIAM (Service Integration and Access Management) system. It ensures that users and roles in CloudBees CI are properly mapped to SIAM-managed roles and that necessary permissions are granted for each role.  
  
CloudBees CI (Jenkins) uses a system of roles and groups to manage access to different resources. The following roles and groups are available across different controllers in CloudBees CI.  
  
  
---  
  
CloudBees CI Roles  
  
DevOps Internal Controller:  
  
1. System Administrator: Full access to manage all configurations, users, and system settings.  
  
2. Administrator: Administrator access to manage CloudBees CI configurations and users, but with limited system control.  
  
3. DevOps Run: Access to manage and run builds, deployments, and releases.  
  
4. DevOps Build: Access to create, manage, and execute builds and related processes.  
  
Other Controllers (e.g., CloudBees CD):  
  
1. Administrator: Full administrative control, including user management and system configurations.  
  
2. ReadOnly: Limited access with read-only permissions to view configurations, jobs, and builds without making changes.  
  
These roles must be mapped to SIAM roles for ensuring proper access control and compliance.  
  
  
---  
  
SIAM Integration Process  
  
1. Creating SIAM Roles for CloudBees CI  
  
Before associating users to roles, the following roles must be created in the SIAM system for each CloudBees CI controller:  
  
CloudBees CI System Administrator: Mapped to the System Administrator role in the DevOps internal controller.  
  
CloudBees CI Administrator: Mapped to the Administrator role in the DevOps internal controller or other controllers.  
  
CloudBees CI DevOps Run: Mapped to the DevOps Run role.  
  
CloudBees CI DevOps Build: Mapped to the DevOps Build role.  
  
CloudBees CI ReadOnly: Mapped to the ReadOnly role in other controllers.  
  
Note: Each role in SIAM should be assigned with appropriate permissions according to the responsibilities of the CloudBees CI role.  
  
  
---  
  
2. User Creation Process in CloudBees CI  
  
CloudBees CI users can be created manually or through LDAP integration. SIAM should ensure that every user who requires access to CloudBees CI creates a Request Item (RITM) for role approval.  
  
API to Create a User in CloudBees CI  
  
To create a user in CloudBees CI:  
  
Endpoint:  
  
POST /createItem?name=USERNAME  
  
Example:  
  
curl -X POST "https://cloudbees-ci-url/createItem?name=newusername" -u "admin:password" -d '<user><fullName>New User</fullName><email>newuser@example.com</email></user>'  
  
User Management in SIAM  
  
In SIAM, when a user requests access to CloudBees CI, the request will be tied to a specific role:  
  
System Administrator: SIAM role for users requiring full access to manage CloudBees CI configurations and settings.  
  
Administrator: SIAM role for users who need to manage pipelines and configuration settings, but not full administrative tasks.  
  
DevOps Run: SIAM role for users responsible for running builds and deployments.  
  
DevOps Build: SIAM role for users who manage and execute builds.  
  
ReadOnly: SIAM role for users with limited access (view-only) to CloudBees CI.  
  
  
---  
  
3. Mapping Users to Roles in CloudBees CI  
  
CloudBees CI uses roles to manage access. These roles need to be mapped to SIAM roles. The Role-based Authorization Strategy Plugin in CloudBees CI can be used to assign users to specific roles.  
  
API to Fetch All Roles in CloudBees CI  
  
To fetch all roles in CloudBees CI:  
  
Endpoint:  
  
GET /role-strategy/roles/api/json  
  
Example cURL Command:  
  
curl -X GET "https://cloudbees-ci-url/role-strategy/roles/api/json" -u "admin:password"  
  
API to Add Users to Roles  
  
To assign users to a particular role:  
  
Endpoint:  
  
POST /role-strategy/roles/ROLE\_NAME/grantUser  
  
Example cURL Command:  
  
curl -X POST "https://cloudbees-ci-url/role-strategy/roles/ROLE\_NAME/grantUser" -u "admin:password" -d 'userName=USERNAME'  
  
This API adds the user (USERNAME) to the specified role (ROLE\_NAME).  
  
  
---  
  
4. Fetching Groups and Users in CloudBees CI  
  
To onboard CloudBees CI users into SIAM, it's necessary to fetch the groups and their associated users.  
  
API to Fetch All Groups in CloudBees CI  
  
To fetch all groups:  
  
Endpoint:  
  
GET /group/api/json  
  
Example cURL Command:  
  
curl -X GET "https://cloudbees-ci-url/group/api/json" -u "admin:password"  
  
This API will return a list of groups in the CloudBees CI system.  
  
API to Fetch Users in a Group  
  
To fetch all users associated with a specific group:  
  
Endpoint:  
  
GET /group/GROUP\_NAME/members/api/json  
  
Example cURL Command:  
  
curl -X GET "https://cloudbees-ci-url/group/GROUP\_NAME/members/api/json" -u "admin:password"  
  
This will return all the users that are part of the specified group (GROUP\_NAME).  
  
  
---  
  
5. Adding Users to Internal Groups  
  
To add users directly to an internal group in CloudBees CI:  
  
API to Add User to Group  
  
To add a user to a specific group, you can use the following API:  
  
Endpoint:  
  
POST /group/GROUP\_NAME/addUser  
  
Example cURL Command:  
  
curl -X POST "https://cloudbees-ci-url/group/GROUP\_NAME/addUser" -u "admin:password" -d 'userName=USERNAME'  
  
This API adds the specified user (USERNAME) to the specified group (GROUP\_NAME).  
  
  
---  
  
6. Mapping CloudBees CI Roles to SIAM Roles  
  
DevOps Internal Controller  
  
1. System Administrator:  
  
SIAM Role: CloudBees CI System Administrator  
  
Permissions: Full access to configure and manage CloudBees CI settings, including user management and system configurations.  
  
2. Administrator:  
  
SIAM Role: CloudBees CI Administrator  
  
Permissions: Ability to configure pipelines and manage users, with limited system settings access.  
  
3. DevOps Run:  
  
SIAM Role: CloudBees CI DevOps Run  
  
Permissions: Manage and execute releases, deployments, and build pipelines.  
  
4. DevOps Build:  
  
SIAM Role: CloudBees CI DevOps Build  
  
Permissions: Create, manage, and execute build jobs.  
  
Other Controllers (e.g., CloudBees CD)  
  
1. Administrator:  
  
SIAM Role: CloudBees CI Administrator  
  
Permissions: Full access to configure CloudBees CI settings, including user management and system configurations.  
  
2. ReadOnly:  
  
SIAM Role: CloudBees CI ReadOnly  
  
Permissions: Limited access to view configurations, jobs, and builds, without any ability to modify them.  
  
  
---  
  
7. SIAM Workflow for User Access  
  
Step 1: User Request  
  
Users raise a Request Item (RITM) in SIAM to request access to CloudBees CI.  
  
The request should specify the required role (e.g., Administrator, DevOps Run, etc.).  
  
Step 2: Approval Process  
  
The SIAM system will route the request to the relevant approvers.  
  
Upon approval, the user will be granted the corresponding SIAM role.  
  
Step 3: Mapping Role in CloudBees CI  
  
After the role is assigned in SIAM, the corresponding CloudBees CI role will be mapped to the user.  
  
The user is added to the appropriate role in CloudBees CI, granting them the necessary permissions.  
  
Step 4: User Access  
  
The user can now access CloudBees CI according to the permissions associated with their role.  
  
  
---  
  
8. Removing Access for Users  
  
To remove access from a user:  
  
1. Revoke Role in CloudBees CI: Use the following API to remove the user from the assigned role:  
  
Endpoint:  
  
POST /role-strategy/roles/ROLE\_NAME/revokeUser  
  
Example cURL Command:  
  
curl -X POST "https://cloudbees-ci-url/role-strategy/roles/ROLE\_NAME/revokeUser" -u "admin:password" -d 'userName=USERNAME'  
  
2. Revoke SIAM Role: Ensure the user's SIAM role is also removed or disabled.  
  
  
---  
  
9. Auditing and Logging  
  
Ensure that all access requests, approvals, and changes are logged both in SIAM and CloudBees CI for auditing purposes. This helps track user access and ensure compliance with internal security policies.  
  
  
---  
  
Conclusion  
  
This process ensures that CloudBees CI (Jenkins) is properly integrated with the SIAM system for access management. By mapping roles between CloudBees CI and SIAM, access control is centralized and managed securely. Users must raise an RITM for role approval before being granted access to CloudBees CI, and the necessary permissions will be enforced for each role.