Predict | Protect | Prevent

ARCON|PAM

Cloud Governance

arcon

Table of Contents

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.
Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Sales Contact
You can directly contact us with sales-related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Introduction

Using cloud infrastructure is crucial to a company's success, but securing access to cloud platforms comes with its own set of issues that put your business at risk.

Managing rapidly growing, increasingly complex cloud infrastructure entitlements is already difficult. This is exacerbated by the adoption of multi-cloud infrastructure as a service (IaaS) offers. Each cloud platform has its own set of access management tools, but they are limited to managing their own environments and do not scale to include others. This forces your team to jump from console to console, attempting to handle rights for each cloud platform independently, with different methods for applying for roles from one platform to the next.

The **ARCON | Cloud Governance module** is a SaaS solution that can assist in gaining total insight and control over your cloud infrastructure and workload. It offers visibility into unnecessary rights, modifies regulations without affecting developer processes, detects potential abnormalities, and enforces access regulations across all users.

1.1 Features

- **Centralized Dashboard:** Key measurements and recommendations on a single screen across several cloud environments.
- **Entitlement Visualization:** Various entitlements like users, groups, roles, etc are continuously discovered across all supported platforms.
- **Granular Recommendations:** Use a single interface to apply policies across many cloud platforms.
- **Access Inspection:** Assess for unwanted or underused access across cloud platforms.

2 Integrations

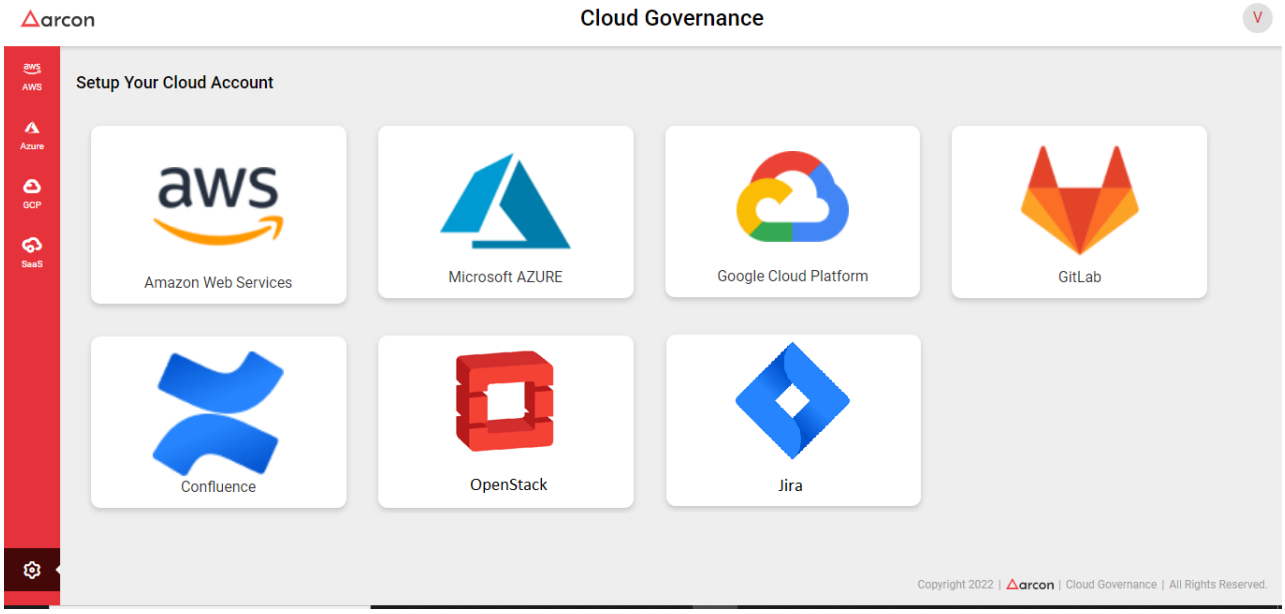
Currently, the Cloud Governance Module integrates with the topmost cloud service providers:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- OpenStack
- SaaS platforms like Gitlab, Confluence, Jira, Salesforce, etc

*ARCON Cloud Governance has the capability to integrate with private cloud (like OpenStack) etc for permissions management and governance.

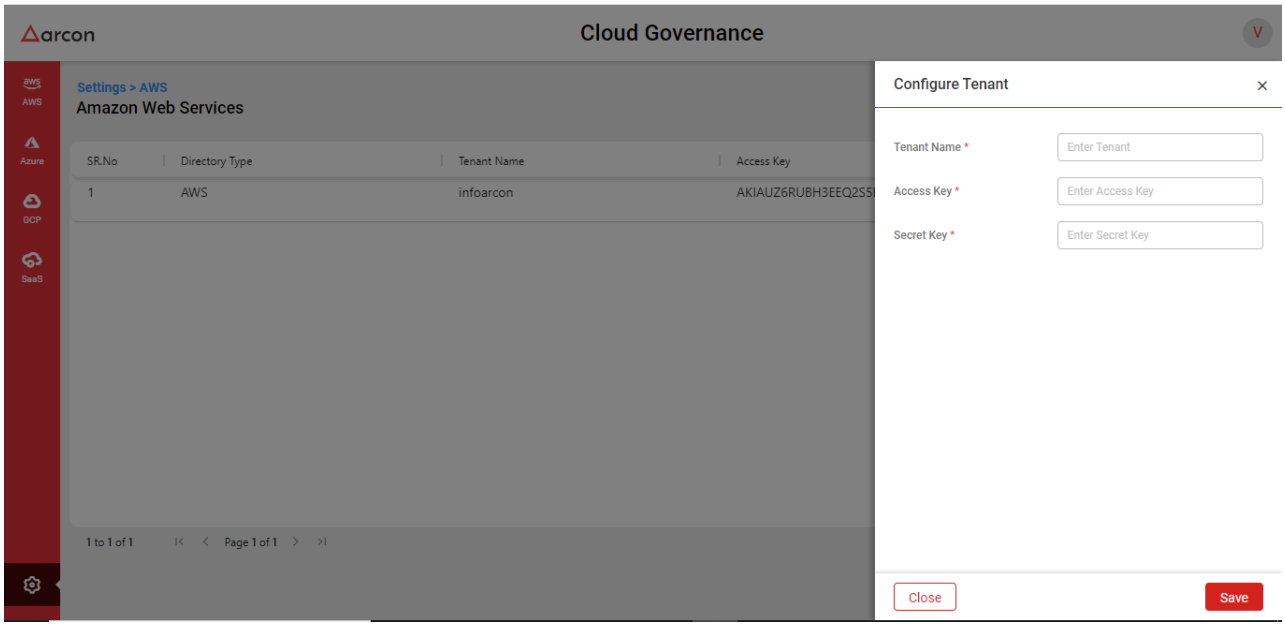
3 Setting up your Cloud Platform

In order to access the features, the administrator first needs to configure their AWS, Azure, or GCP Tenant in Cloud Governance.



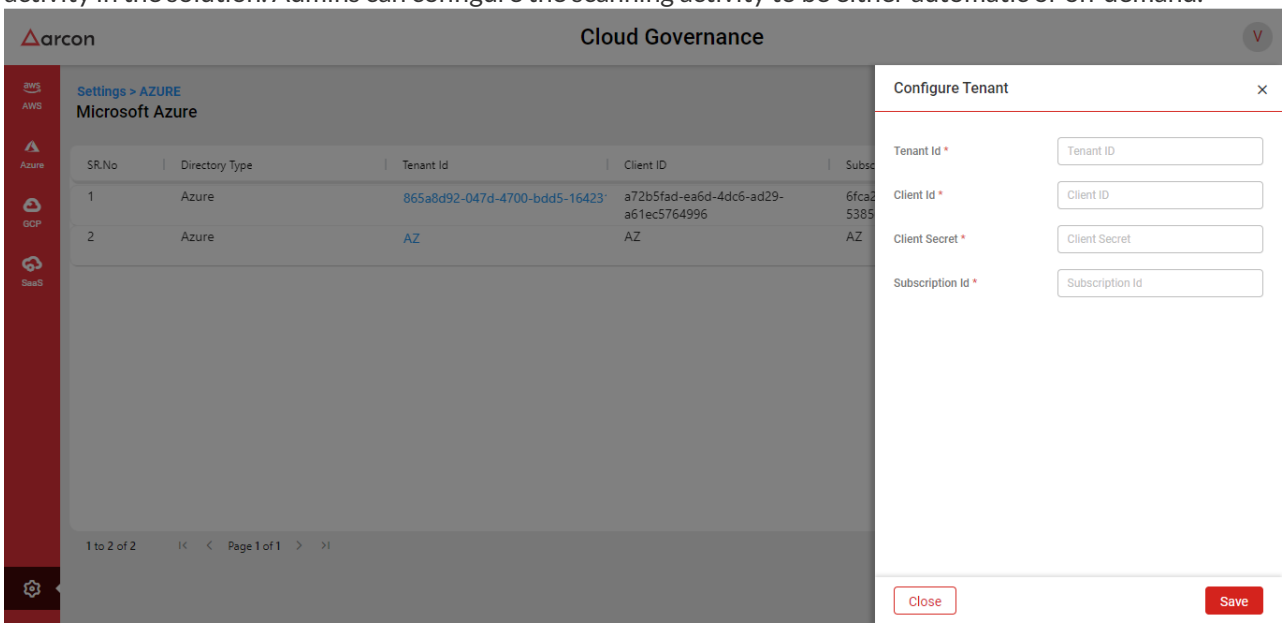
3.1 Set up your AWS Tenant

Admin can configure multiple tenants supporting your AWS infrastructure by adding the tenant IDs of the AWS accounts. For each of the tenants, the admin can configure multiple AWS access keys with different policies. The policies required for Cloud Governance are IAMFullAccess, AmazonEC2FullAccess, AmazonS3ReadOnlyAccess, AmazonVPCReadOnlyAccess, AmazonRDSReadOnlyAccess, and AmazonECS_FullAccess. Cloud Governance scans the AWS platform, gathers, and analyses data from linked workspaces, and updates entity activity in the solution. Admins can configure the scanning activity to be either automatic or on-demand.



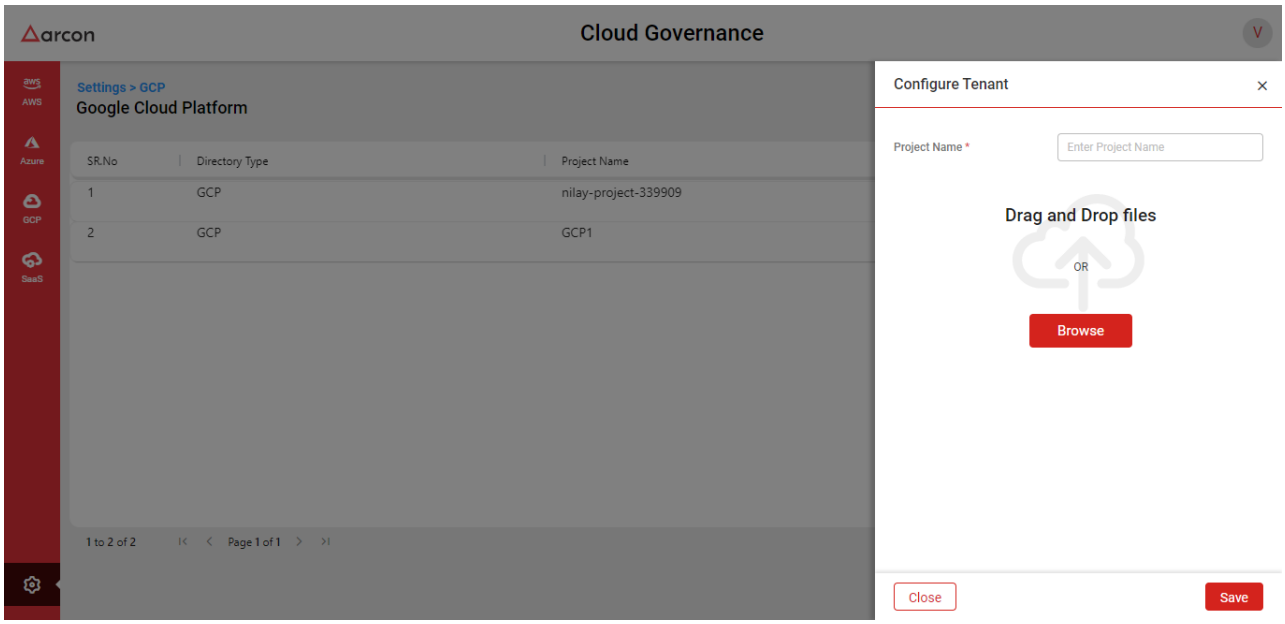
3.2 Set up your Azure Tenant

You can configure multiple tenants supporting your Azure infrastructure by adding the tenant IDs of the AWS accounts. For each of the tenants, the admin can configure Azure Active Directory and multiple subscriptions. For Azure AD, add the credentials of an App Registration with the User Administrator AD role assigned. For Subscriptions, add the credentials of an App Registration with the Azure owner role of the Subscription. Cloud Governance scans the Azure platform, gathers, and analyses data from linked workspaces, and updates entity activity in the solution. Admins can configure the scanning activity to be either automatic or on-demand.



3.3 Set up your Google Project

Admin can configure multiple GCP projects by adding the Project ID of the GCP Project. For each of the projects, the admin can configure multiple service accounts with different roles by uploading their credentials. The policies required for Cloud Governance are iam.securityAdmin, compute.viewer, cloudsql.viewer, vpcaccess.viewer, storage.admin and containeranalysis.admin. Cloud Governance scans the GCP platform, gathers, and analyses data from linked workspaces, and updates entity activity in the solution. Admins can configure the scanning activity to be either automatic or on-demand.

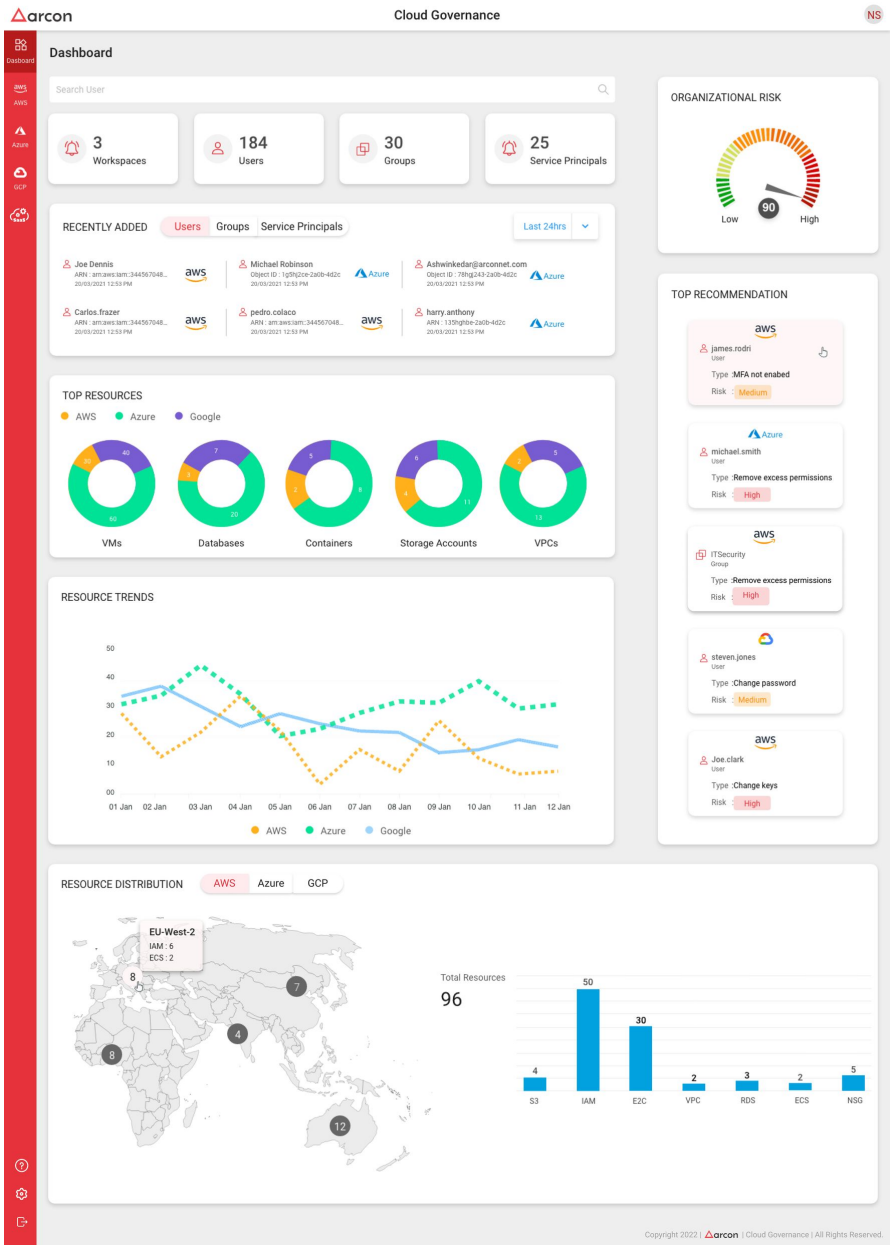


Similar steps are to be followed for setting up an OpenStack and Saas (Gitlab, Confluence, Jira, Salesforce, etc) accounts.

Cloud Governance scanner runs in the background which scans tenants across the cloud platforms and gathers/analyses data from linked workspaces, and updates entity activity in the solution. Admins can configure the scanning activity to be either automatic or on-demand. If the scan type is selected as automatic, then the admins can select timer intervals to schedule the scan process and if the scan type is selected as manual then the admin can initiate the scan according to their convenience.

4 All Cloud Dashboard

The dashboard contains information about various entitlements across multiple clouds which helps in identifying the risky nature of entities. It provides the administrator with various visualizations that give them a direct view of the various resources and identities across the cloud platforms.

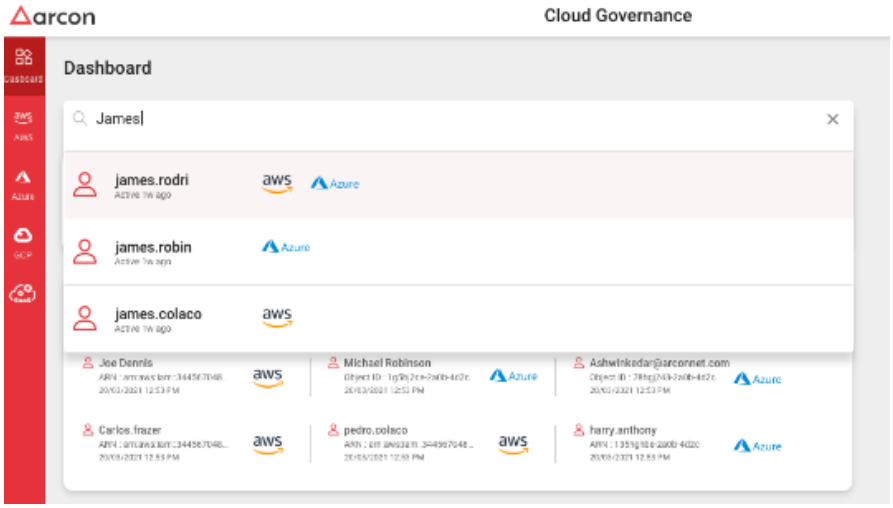


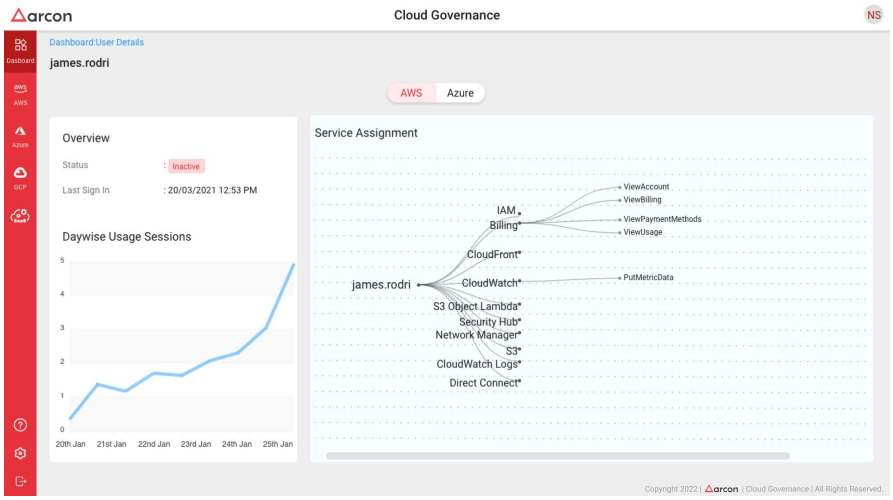
The following information is available on the Cloud Governance dashboard:

- Total workspaces connected - Total tenants configured across AWS, Azure, Google Cloud, and OpenStack
- Total Users scanned - IAM Users in AWS, GCP, AD Users in Azure, and users and roles in OpenStack

- Total Groups discovered - IAM Groups in AWS, AD Groups in Azure, GCP groups, and OpenStack groups.
- Total Service principals discovered - IAM Roles in AWS, App Registrations in Azure AD, Service accounts in GCP
- Organizational Risk score signals the total risk of all the cloud environments
- Recently Added Users, Groups and Service principals across cloud platforms
- Total Resources (VM's, databases, containers, storage accounts) configured across the cloud platforms
- Recommendations for risk reduction of the riskiest entities across different cloud platforms
- Resource trends show the number of resources added to various cloud platforms over time
- For different cloud platforms, track resource distribution around the globe and the resource distribution within each cloud platform

Additionally, there is also a search user option, that performs a fuzzy search across the various cloud platforms configured. This view helps the administrator to clearly visualize all the cloud entitlements of a single user in their organization.





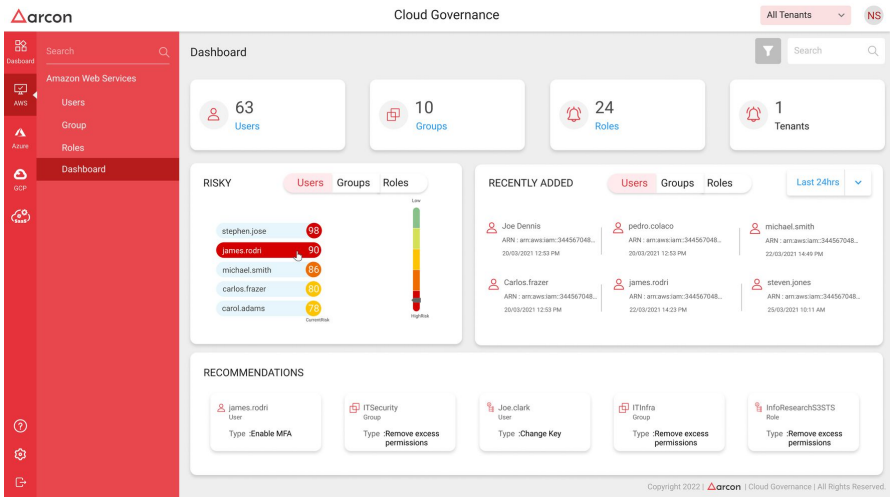
5 Risk Score

A risk score is calculated at all levels, from the individual entity to the overall organization. The module is capable of determining the utilization of permissions issued to various services/resources at the lowest action level. The action is categorized as used/unused based on the latest access information of these activities. It can also detect shadow-admin rights and excessive permissions using AI and machine learning approaches by studying the permission patterns of each cloud platform. Based on all these factors, the risk score is computed.

6 Each Cloud Dashboard

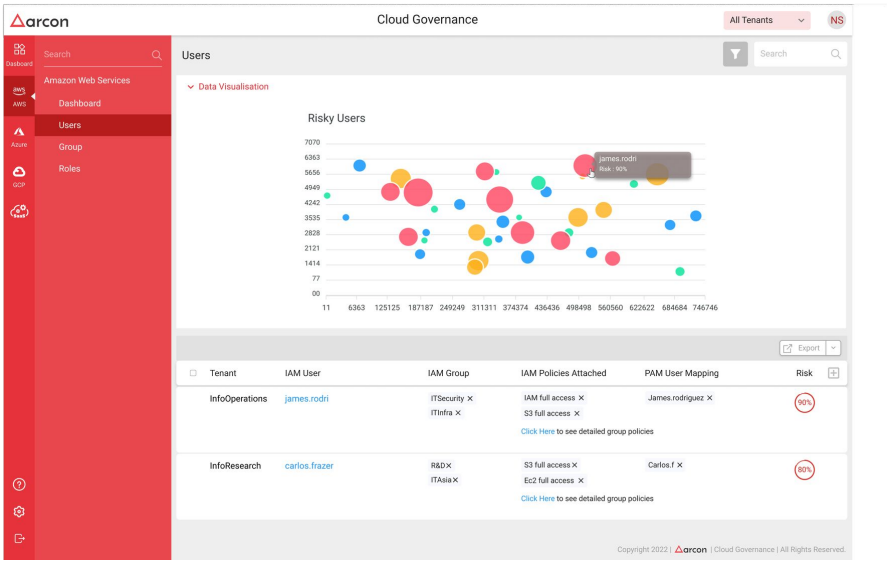
This dashboard helps the administrator visualize a single cloud platform in detail. It presents the administrator with the following information:

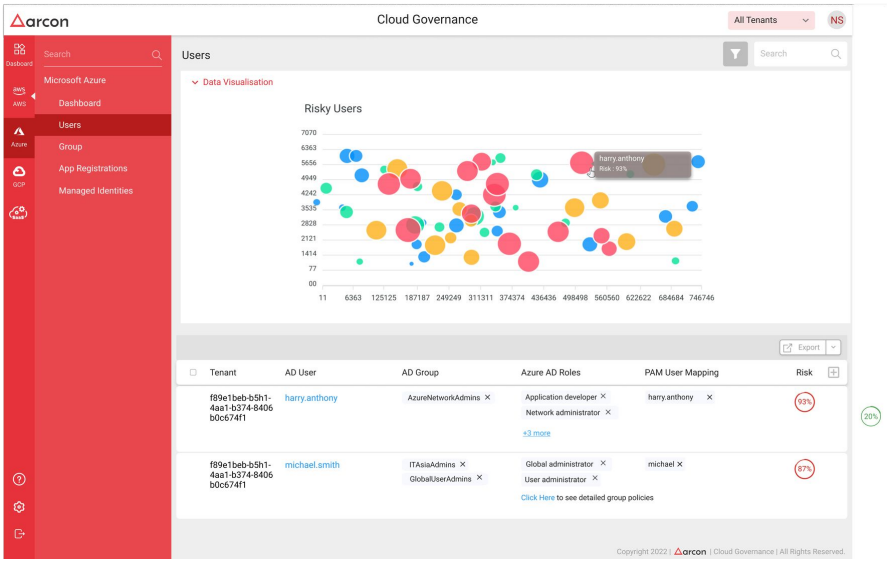
- Total Risk across all tenants on the cloud Platform
- Information on various entities like users, groups, roles, and tenants
- Analyze exposure of cloud assets - riskiness for more exposed users, groups, and roles across tenants
- Overview of recently added cloud assets
- Recommendations that have been identified in the recent past for lowering the risk exposure



7 Users

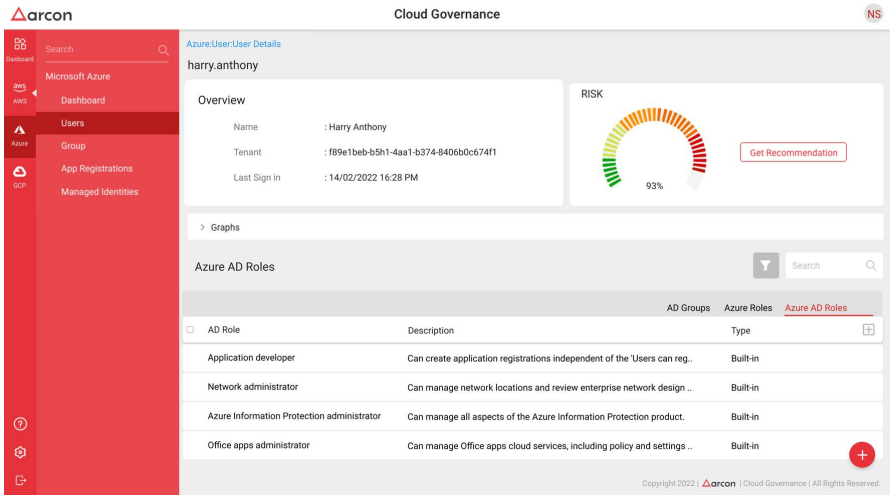
The Users screen displays all the users of your selected cloud platform. For AWS, it scans all the IAM users in your selected tenant. On the top, there is an interactive chart indicating the risky nature of various users, where each bubble represents a user. The size of the bubble indicates the risk score of the user, its color is based on the usage of the actions of its policies. Below the graph is a grid showing the list of IAM users with their attached policies, IAM groups, Tenant name, and Risk score. Additionally, if the PAM Integration feature is enabled, a PAM User Mapping column is also displayed in the grid, which indicates which PAM user has been assigned a console service of this IAM User. The administrator can also directly remove the user from a particular IAM group, detach an IAM Policy or remove the service mapping from PAM. For Azure, it scans your Azure AD and gets all the users in your directory. The grid shows the list of Azure AD users with their assigned AD Groups, AD assigned roles, PAM Mappings, and the Risk score.





7.1 Detailed User information

Clicking on a user in the grid or a bubble in the graph will open up detailed information for the user. It shows the overview of the user and the Risk Score of that user.

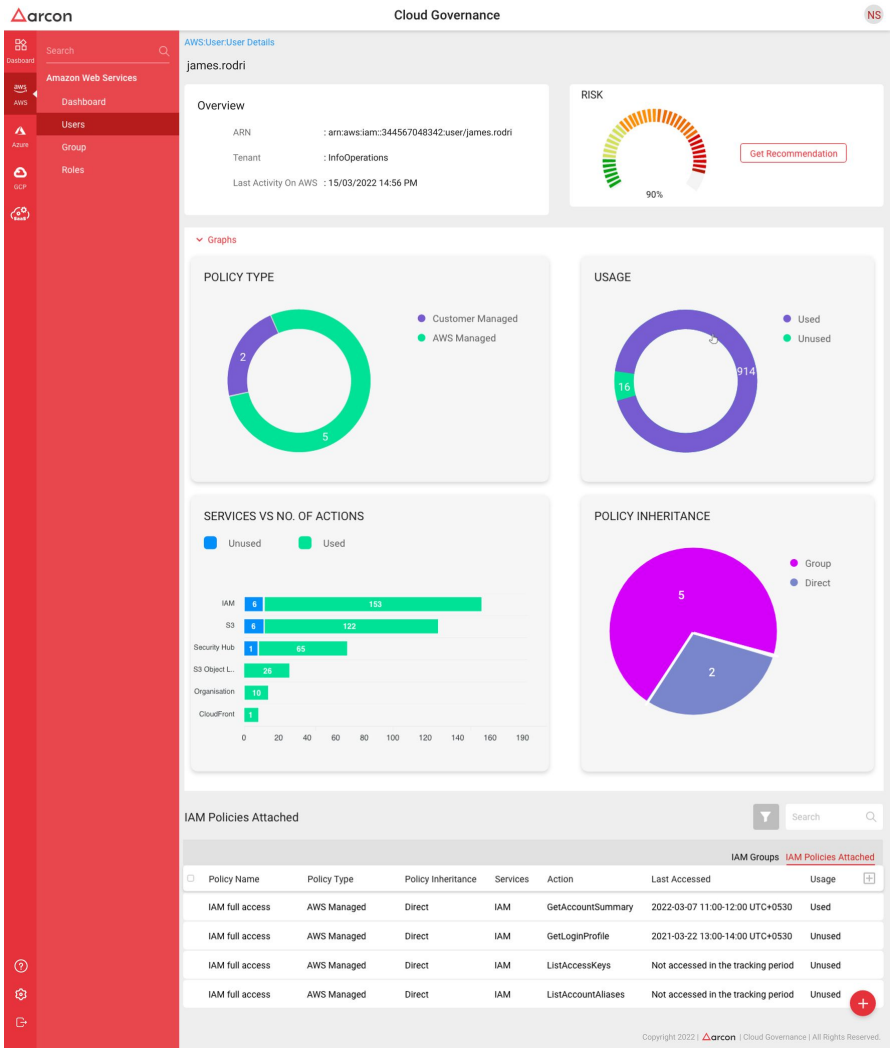


7.1.1 Data Visualization

There are 4 types of graphs that depict different visualizations to analyze the permissions attached to the user.

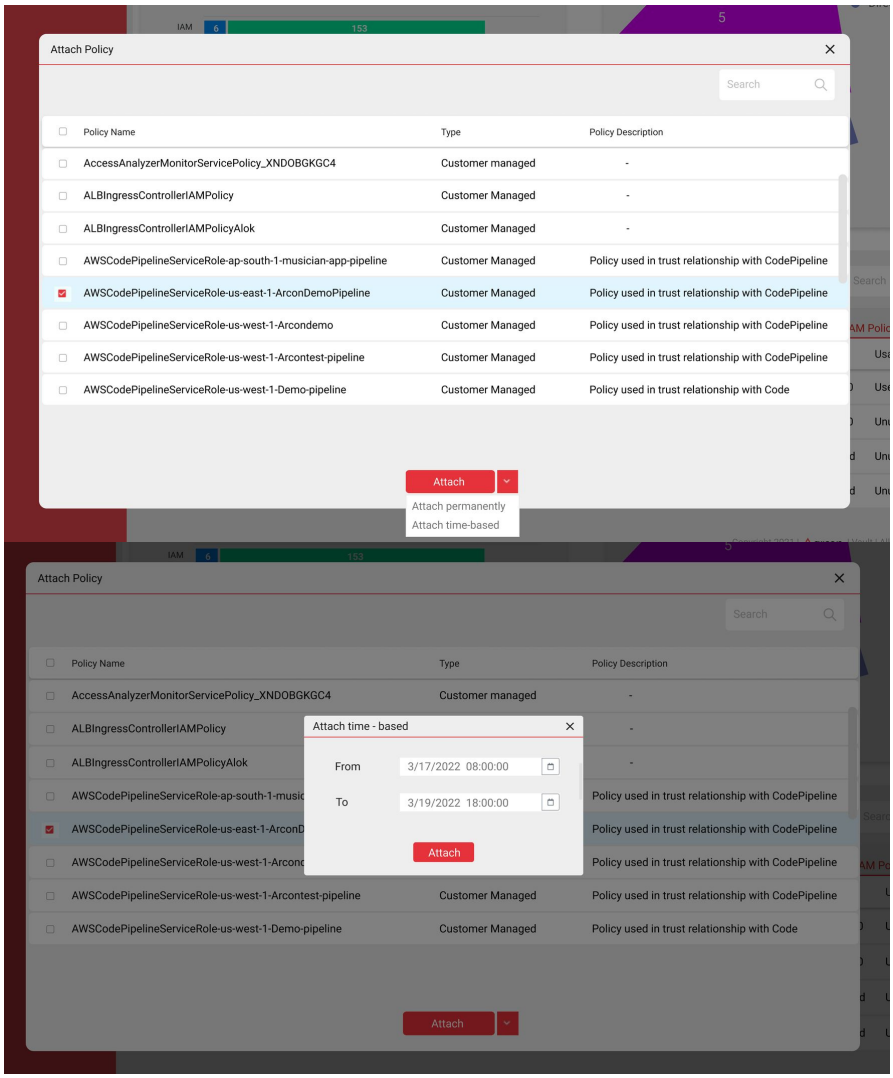
- **Policy Type:** A distribution for the type of policies attached
- **Usage:** Based on the User's actual use of a permission
- **Services Vs No of Actions:** Shows all the services that the user has been assigned through the policies attached and the number of permissions that have been assigned for that service
- **Policy Inheritance:** Shows how many policies that are attached to the user are Direct assignments or assigned through a group

Each of these graphs is interactive and on clicking, similar filters are applied on the IAM policies grid below.



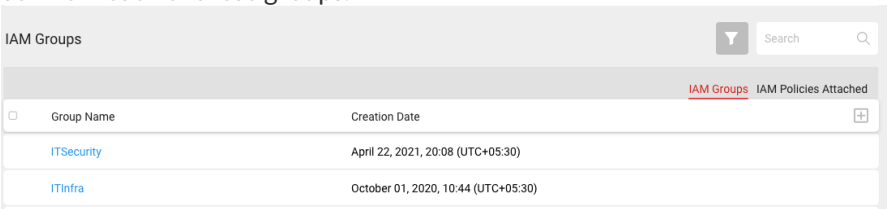
7.1.2 IAM Policies Attached

This tab shows all the Service and Action information of the IAM Policies that are attached to the user and indicates the usage of each action. If the last accessed time is more than the Unused Permissions Period configured in Settings, then the Usage for that action is indicated as Unused. The administrator can also attach new IAM Policies by clicking on the + icon at the bottom. Here the admin can attach the policy as both time-based and permanent. If a time-based policy is attached, the policy will be detached from the entity (user, group, or role) once the validity period expires.



7.1.3 IAM Groups

This tab shows all the IAM Groups that the IAM user is a part of. The administrator can select the group entries and remove the user from each of these groups.



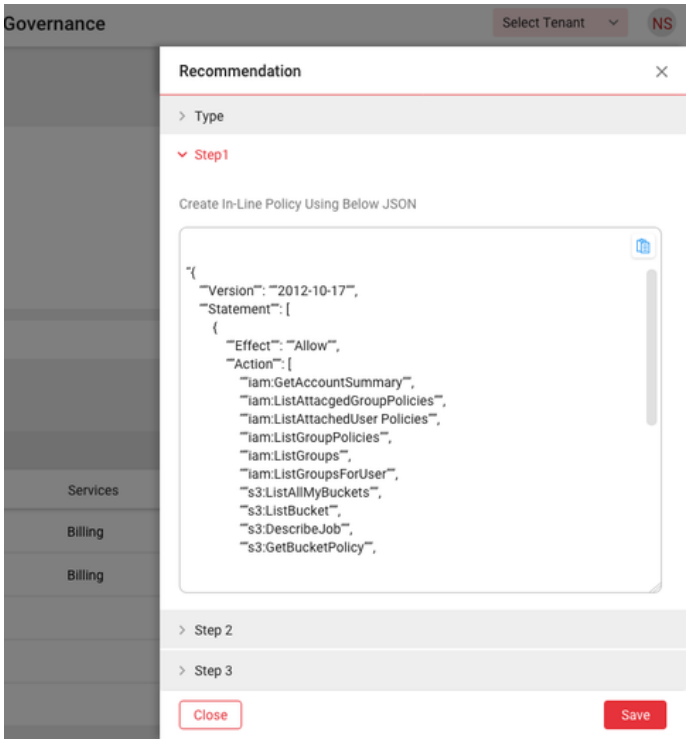
7.1.4 Recommendations

Click on **Get Recommendation** in order to reduce the risk score of the IAM user. There are 2 types of recommendations that are suggested for the IAM user.

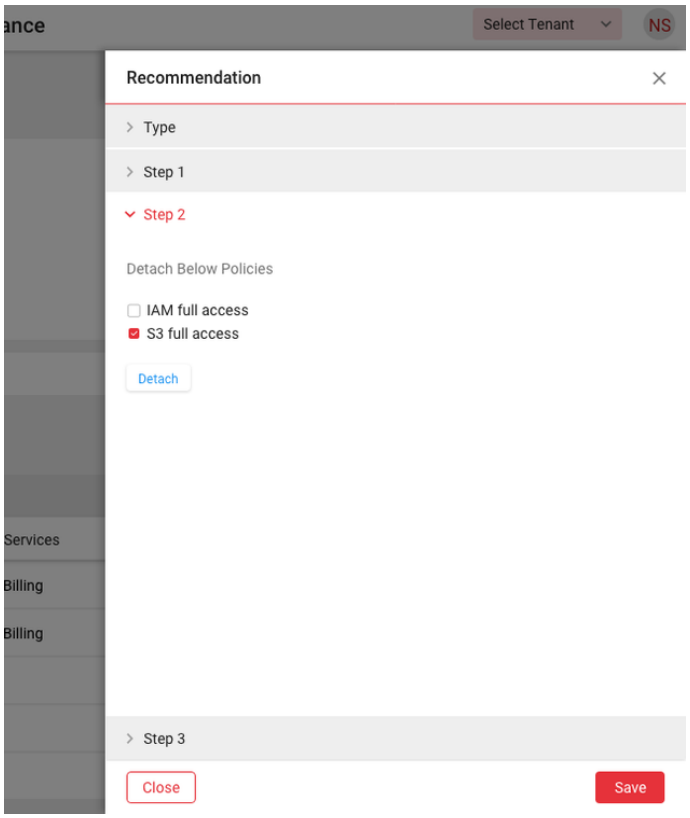
7.1.4.1 Reduce Policy Exposure

The suggestions are based on the principle of Minimal Rights and take into account the particular risks of each platform.

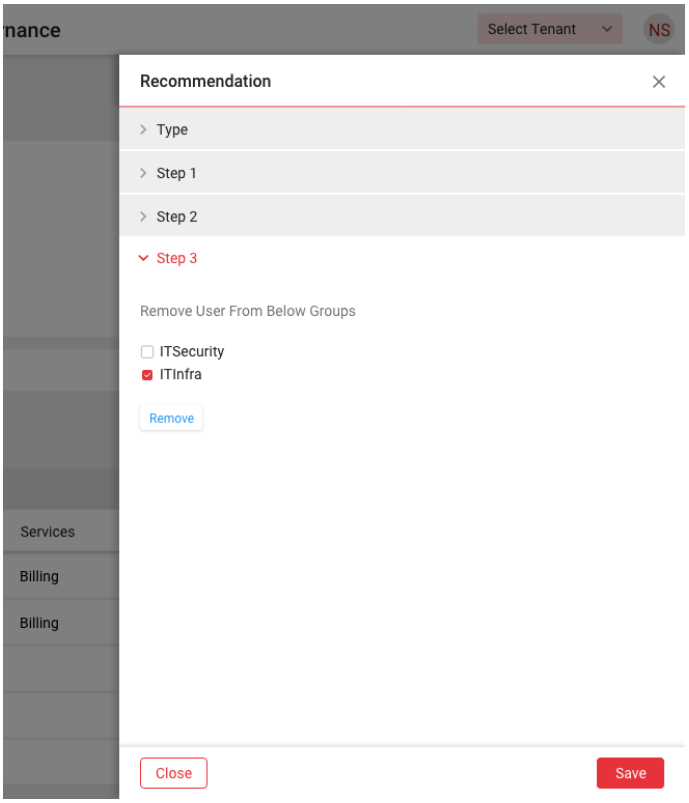
- **Step 1:** A policy JSON is created for the IAM user based on the actual Action usage. The Admin can copy the policy JSON and create a new custom policy on AWS and attach it to the user.



- **Step 2:** Admin to detach the existing policies attached to the IAM user since these policies expose the user to a lot of unused actions.

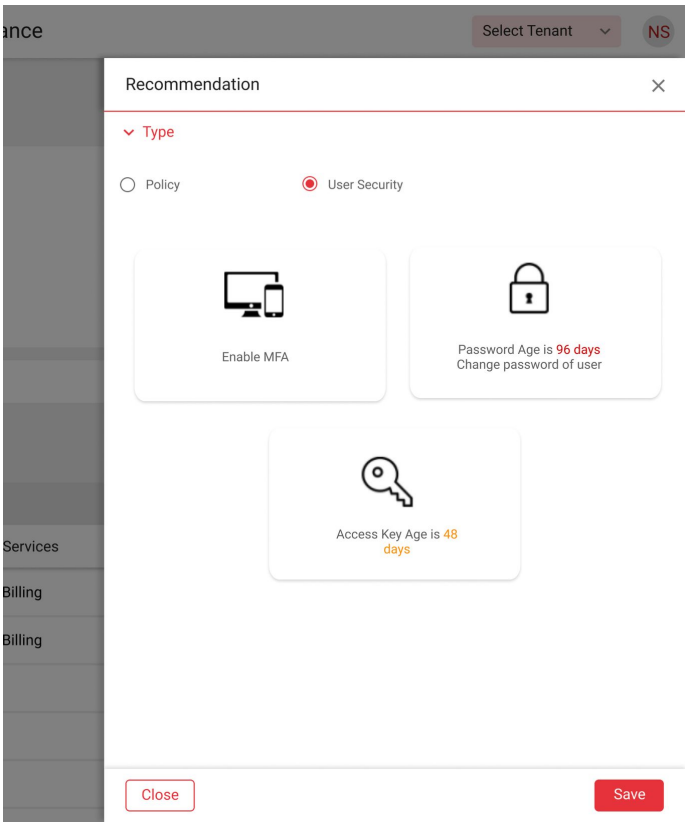


- **Step 3:** Admin to remove the user from all the assigned groups so that the policies inherited through the group are detached.



7.1.4.2 User Security

These are additional recommendations for an IAM user based on MFA, password age, and access key age.

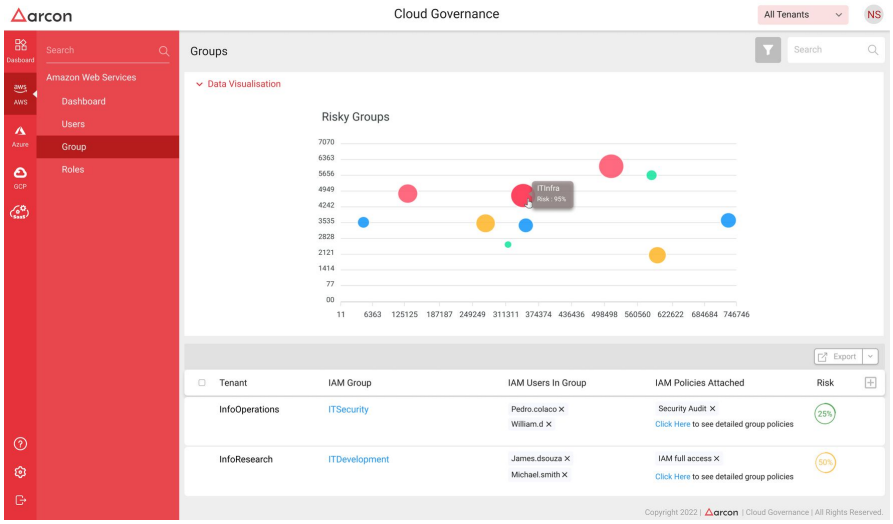


7.1.5 Anomaly Detection

Anomalies are detected depending on entity behavior on the cloud platform which is determined by a number of factors. For instance, If a shadow-admin user is discovered who does not have MFA enabled or whose password/access keys have not been changed in a long period are flagged as anomalous. Additionally, irregular number of user sessions per day, the uncommon originating IP address of the cloud platform login, varied geolocation of logged-in users, and unusual login activity time are some of the parameters on which the anomaly detection algorithm works.

8 Group

The Groups screen displays all the groups of your selected cloud platform. For AWS, it scans all the IAM groups in your selected tenant. On the top, there is an interactive chart indicating the risky nature of various groups, where each bubble represents a group. The size of the bubble indicates the risk score of the user, its color is based on the usage of the actions of its policies. Below the graph is a grid showing the list of IAM groups with their attached policies, IAM users in the group, Tenant name, and Risk score. The administrator can also directly remove an IAM user from the group or detach an IAM Policy. For Azure, it scans your Azure AD and gets all the groups in your directory. The grid shows the list of Azure AD groups with their assigned AD users, assigned AD groups, the group type, and the Risk score.



8.1 Detailed Group Information

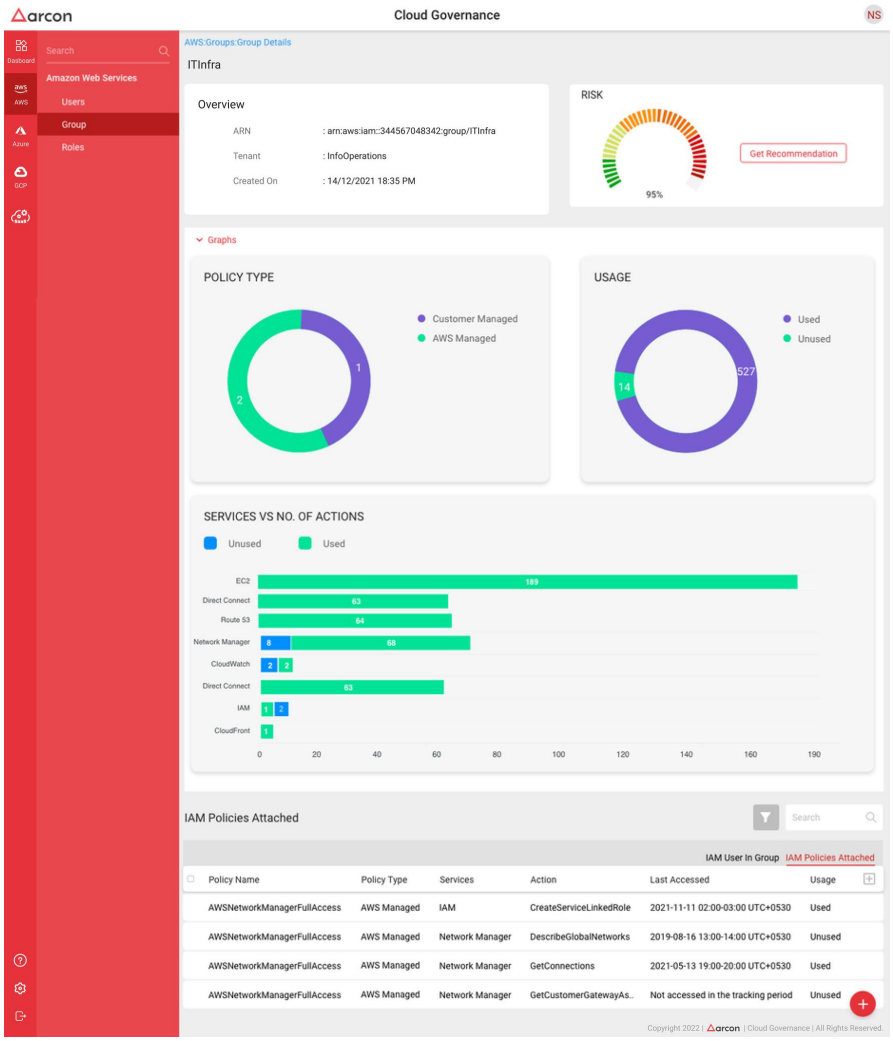
Clicking on a group in the grid or a bubble in the graph will open up detailed information for the group. It shows the overview of the group and the Risk Score of that group.

8.1.1 Data Visualization

There are 3 types of graphs that depict different visualizations to analyze the permissions attached to the group.

- **Policy Type:** A distribution for the type of policies attached
- **Usage:** Based on the group members' actual use of a permission
- **Services Vs No of Actions:** Shows all the services that the group has been assigned through the policies attached and the number of permissions that have been assigned for that service

Each of these graphs is interactive and on clicking, similar filters are applied on the IAM policies grid below.

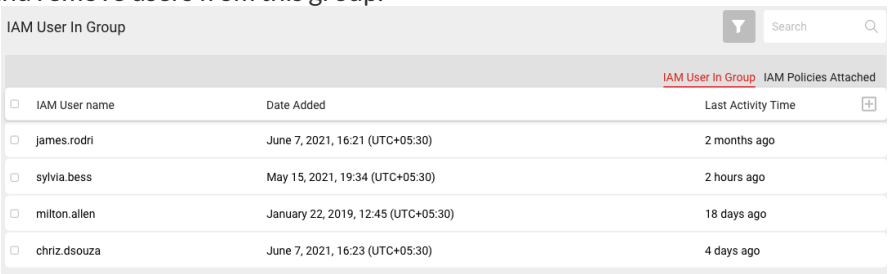


8.1.2 IAM Policies Attached

This tab shows all the Service and Action information of the IAM Policies that are attached to the group and indicates the usage of each action. If the last accessed time is more than the Unused Permissions Period configured in Settings, then the Usage for that action is indicated as Unused. The administrator can also attach new IAM Policies by clicking on the + icon at the bottom.

8.1.3 IAM Users

This tab shows all the IAM Users that have been added to the selected IAM group. The administrator can select the user entries and remove users from this group.



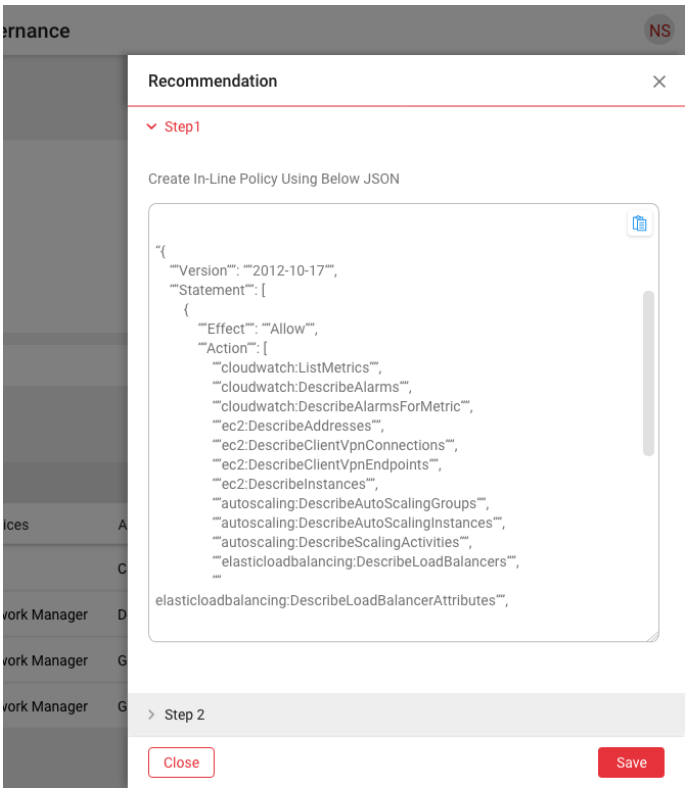
8.1.4 Recommendations

Click on Get Recommendation in order to reduce the risk score of the IAM group.

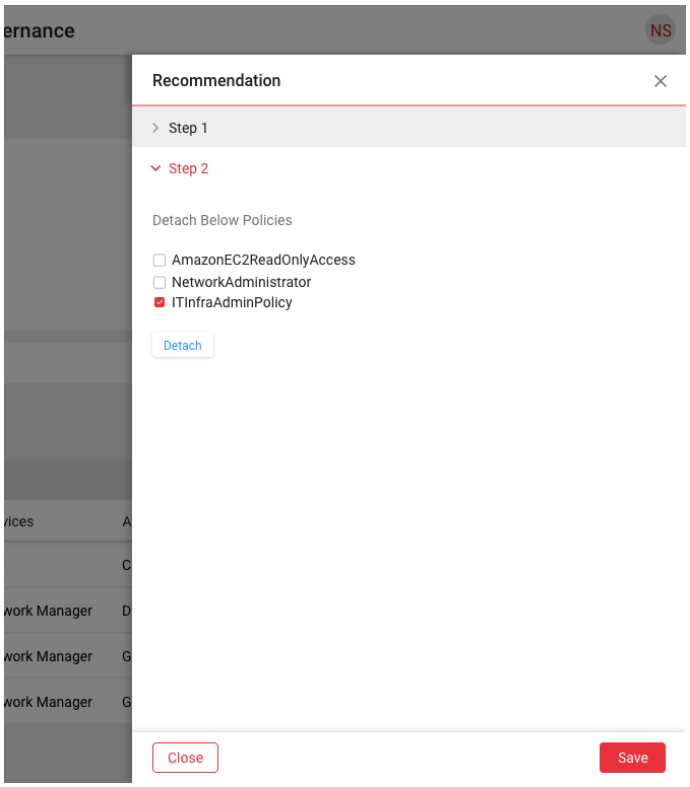
8.1.4.1 Reduce Policy Exposure

The suggestions are based on the principle of Minimal Rights and take into account the particular risks of each platform.

- **Step 1:** A policy JSON is created for the IAM group based on the actual Action usage. The Admin can copy the policy JSON and create a new custom policy on AWS and attach it to the group.

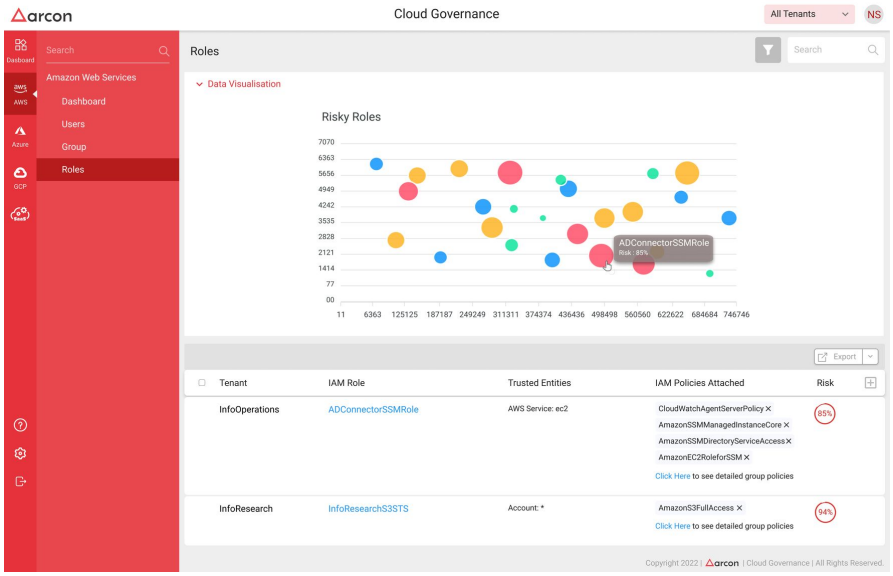


- **Step 2:** Admin to detach the existing policies attached to the IAM group since these policies expose the group to a lot of unused actions.


ernance
NS
Recommendation
Step 1
Step 2
Detach Below Policies
AmazonEC2ReadOnlyAccess
NetworkAdministrator
ITInfraAdminPolicy
Detach
Close
Save

9 Service Principals

The Service Principal screen displays all the service principals of your selected cloud platform. For AWS, it scans all the IAM roles in your selected tenant. On the top, there is an interactive chart indicating the risky nature of various roles, where each bubble represents a role. The size of the bubble indicates the risk score of the user, its color is based on the usage of the actions of its policies. Below the graph is a grid showing the list of IAM roles with their attached policies, Trusted Entities, Tenant name, and Risk score. The administrator can also directly detach an IAM Policy. For Azure, it scans your Azure AD and gets all the App Registrations in your directory and Managed Identities in your subscriptions. The grid shows the list of Azure AD groups with their assigned AD users, assigned AD groups, the group type, and the Risk score.



9.1 Detailed Service Principal Information

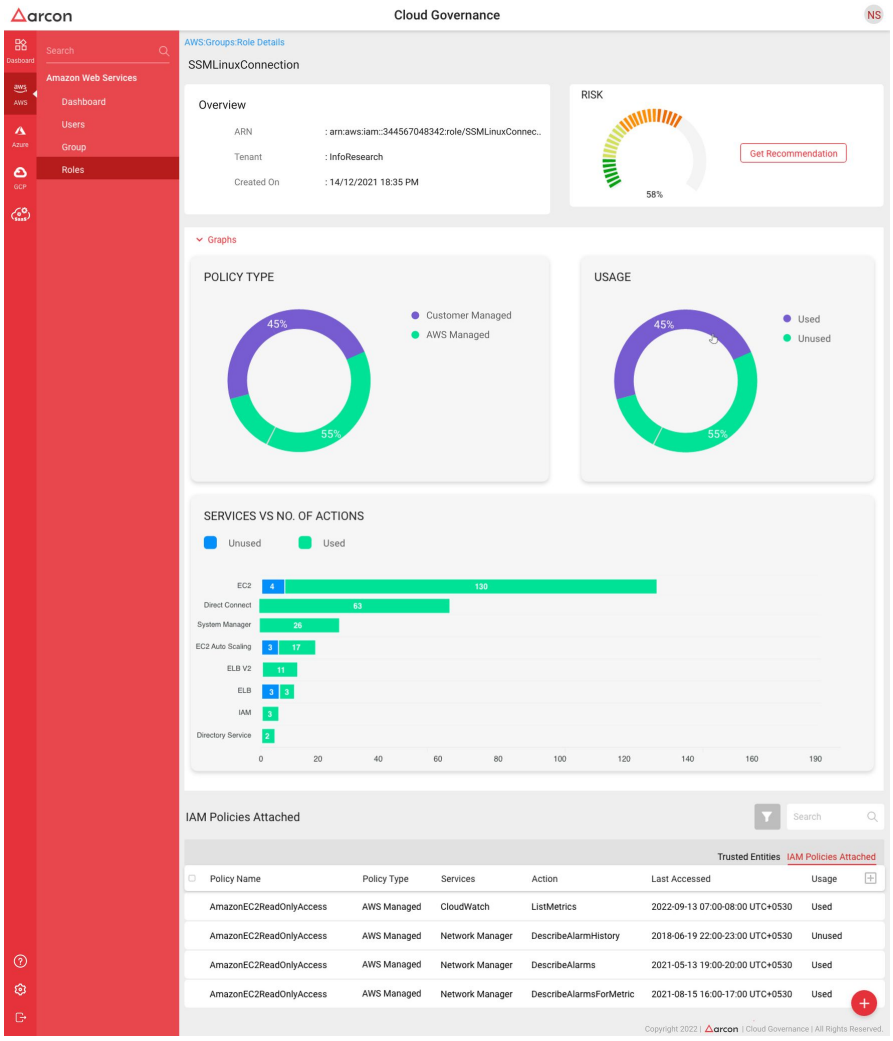
Clicking on a service principal in the grid or a bubble in the graph will open up detailed information for the service principal. It shows the overview of the service principal and the Risk Score of that service principal.

9.1.1 Data Visualization

There are 3 types of graphs that depict different visualizations to analyze the permissions attached to the service principal.

- **Policy Type:** A distribution for the type of policies attached
- **Usage:** Based on the User's actual use of a permission
- **Services Vs No of Actions:** Shows all the services that the role has been assigned through the policies attached and the number of permissions that have been assigned for that service

Each of these graphs is interactive and on clicking, similar filters are applied on the IAM policies grid below.

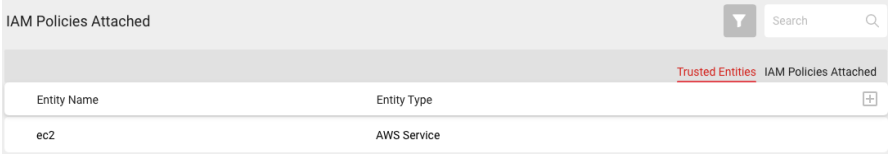


9.1.2 IAM Policies Attached

This tab shows all the Service and Action information of the IAM Policies that are attached to the group and indicates the usage of each action. If the last accessed time is more than the Unused Permissions Period configured in Settings, then the Usage for that action is indicated as Unused. The administrator can also attach new IAM Policies by clicking on the + icon at the bottom.

9.1.3 Trusted Entities

This tab shows all the Trusted Entities that have been assigned to the IAM role and the type of Entity.



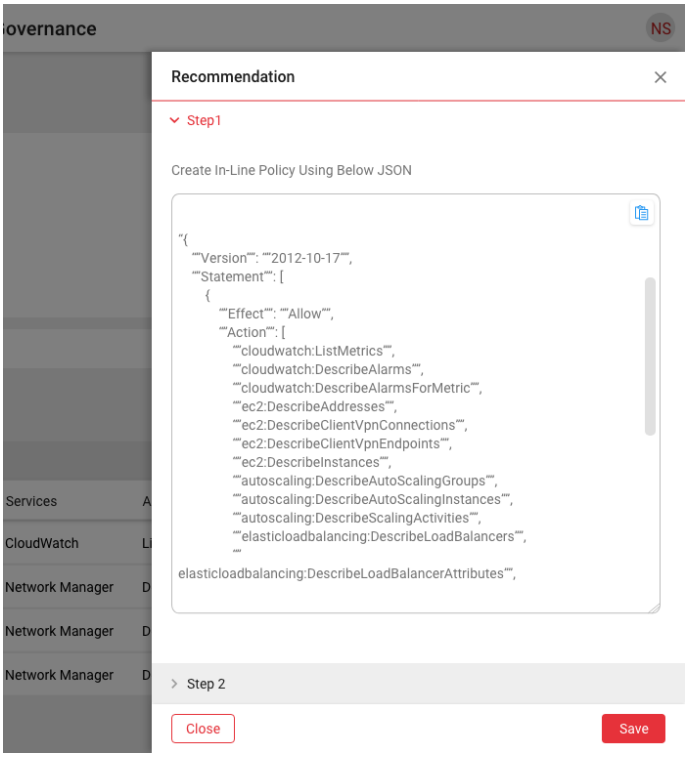
9.1.4 Recommendations

Click on Get Recommendation in order to reduce the risk score of the IAM role.

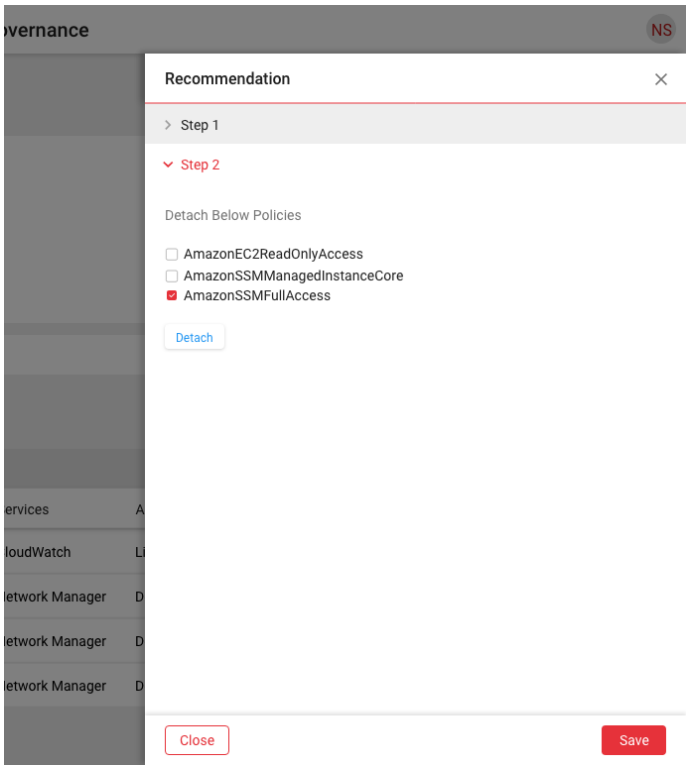
9.1.4.1 Reduce Policy Exposure

The suggestions are based on the principle of Minimal Rights and take into account the particular risks of each platform.

- **Step 1:** A policy JSON is created for the IAM role based on the actual Action usage. The Admin can copy the policy JSON and create a new custom policy on AWS and attach it to the role.

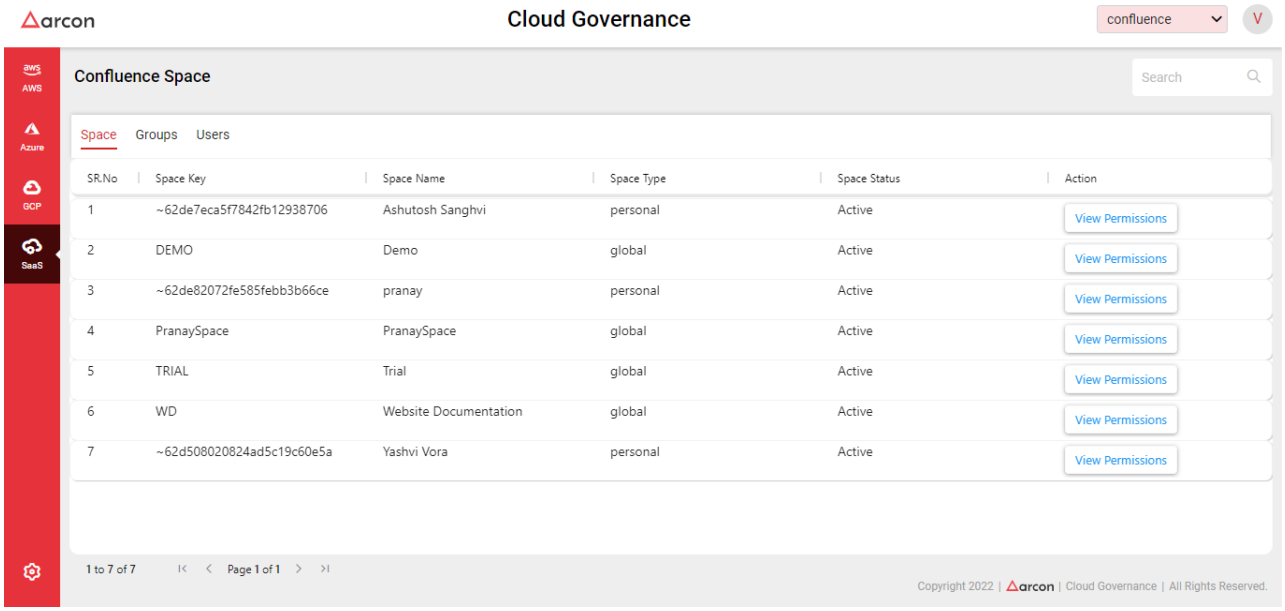


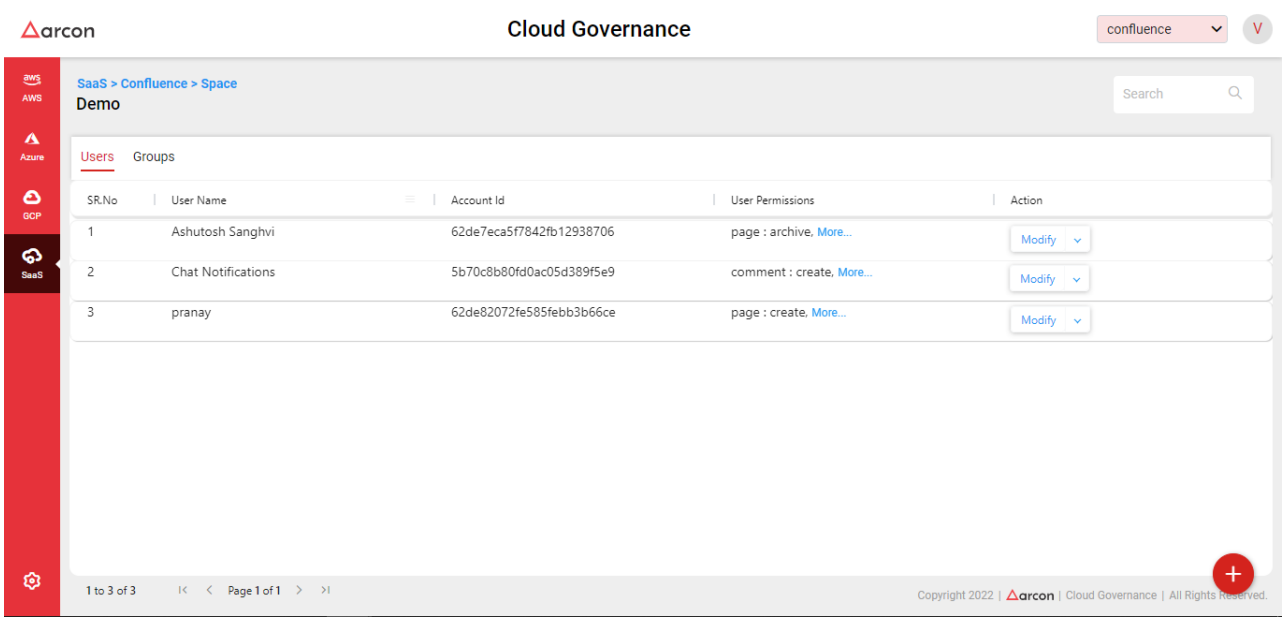
- **Step 2:** Admin to detach the existing policies attached to the IAM role since these policies expose the group to a lot of unused actions.


NS
Recommendation
Step 1
Step 2
Detach Below Policies
AmazonEC2ReadOnlyAccess
AmazonSSMManagedInstanceCore
AmazonSSMFullAccess
Detach
Close
Save

10 Integration with SaaS Applications

Cloud Governance can integrate with SaaS Applications like Atlassian, SalesForce, etc to discover entities like (Users, Groups, Roles, etc). Admin can add/remove an entity from the console. The administrator selects the application from the SaaS section on the left panel and data will be shown in the grid. For instance, in the below screen, the admin can view entities of the confluence application like Confluence Spaces,Users, and Groups. Administrators can get a further idea of the permissions of each entity by clicking the View permissions button.





Privileged Access Management Suite