

### IAM PERMISSIONS EXPLORER

Root IAM user

Account : All Accounts Group: All Groups Last 90 days ⓘ

**Summary cards**

High Risk Roles 8	Unused Roles 2	Over - Privileged 5	Wildcard Access 1
----------------------	-------------------	------------------------	----------------------

**Filters**

Risk :  High  Med  Low Service : All

Click on the role to view detailed view of permissions as depicted in the next page.

Risk calculated based on the group, service access, last use, etc.

Role Name ▾	Group ▾	Risk ▾	Used ▾	Services ▾	Last Used ▾
admin-backup	admin	High	No	EC2, S3, Cloudwatch, Cloudtrail	103 days

Filter based on account, user group and days. The days decide the logs imported from cloudwatch to analyze[AWS]

Summary cards for quick filtering based on factors mentioned

Filtering to select specific risk level or service etc.

Tabular list of roles based on filters set and sorted according to the metric selected.

### ROLE DETAIL - Permissions vs Usage

Root IAM user

Role : admin-backup Group : admin Risk : High Last used : 103 days

**Risk Analysis**

Has Administrator access  
Not used in 103 days  
Accessible by user1212

**Permissions Analysis**

Granted Permissions	Actually used
EC2 : * S3 : * cloudwatch : * cloudtrail : *	EC2 : Describe* - cloudwatch : * -

**Recommended Actions:**

Generate Least-Privilege policy →  
Mark for review  Archive Role

Detailed risk analysis

Role Overview

Permissions used vs granted comparison.

Policy Remediation recommendation based on least privilege principle.

Option to review or archive role entirely.

Policy Remediation recommendation based on least privilege principle.

Option to review or archive role entirely.

Recommended policy changes . Good to keep it editable and option to add more access or remove given accesses.

Impact of the policy update calculated. Also mentions remediation timeline in case of an error.

Options to consider before applying changes.

Option to apply or push to audit by higherups ?

### Policy Recommendation Preview

Root IAM user

Role : admin-backup Group : admin Risk : High Last used : 103 days

**Recommended Policy Updates**

Granted Permissions	Recommended
EC2 : * S3 : * cloudwatch : * cloudtrail : *	EC2 : Describe* - cloudwatch : * -

**Change Impact Assessment :**

No production services affected  
Follows least privilege policy  
Reversible within 24 hrs

**Next Steps :**

Apply policy changes  
 Schedule recheck in 30 days  
 Create review ticket

Apply changes Push to Audit