# Create IAM Role in AWS.

IAM Role creation catalogue is used to provision IAM Role in AWS Environment and also it will do the below functionalities during the provision.

* Attach the Policy to newly created role.
* Add the trusted entities that can assume the role and access conditions for the role.

## Service Now Workflow:

## Sample Payload

### IAM Role Creation

1. {
2. "ScriptFiles": [
3. {
4. "Name": "IAM\_Role.py",
5. "Type": "PY",
6. "Uri": "CE\_Core\_Templates/AWS/IaaS\_Automation/IAM Management/IAM\_Role.py"
7. },
8. {
9. "Name": "IAM\_Role.yml",
10. "Type": "CFT",
11. "Uri": "CE\_Core\_Templates/AWS/IaaS\_Automation/IAM Management/IAM\_Role.yml"
12. }
13. ],
14. "ScriptPayload": {
15. "Region": "us-west-2",
16. "TrustedService": "cloudformation.amazonaws.com",
17. "Rolename": "TestRole",
18. "PolicyArn": "arn:aws:iam::aws:policy/CloudFrontReadOnlyAccess,arn:aws:iam::aws:policy/SecurityAudit,arn:aws:iam::aws:policy/CloudWatchLogsReadOnlyAccess,arn:aws:iam::aws:policy/AmazonDocDBFullAccess,arn:aws:iam::aws:policy/ServiceQuotasFullAccess,arn:aws:iam::957654751236:policy/ALBIngressControllerIAMPolicy,arn:aws:iam::aws:policy/job-function/Billing,arn:aws:iam::aws:policy/AmazonElastiCacheFullAccess,arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess,arn:aws:iam::aws:policy/AmazonAppStreamFullAccess",
19. "Description": "Testing ",
20. "Path": "/test/",
21. "MaxSessionDuration": "10800",
22. "StackName": "SCTASK0013230",
23. "Tags": [
24. {
25. "Key": "Owner",
26. "Value": "Cloud\_Exponence"
27. },
28. {
29. "Key": "Project",
30. "Value": "IT"
31. },
32. {
33. "Key": "BusinessUnit",
34. "Value": "IT IS"
35. },
36. {
37. "Key": "Application",
38. "Value": "Demo"
39. },
40. {
41. "Key": "Environment",
42. "Value": "Non Production"
43. },
44. {
45. "Key": "CreatedBy",
46. "Value": "CloudExponence"
47. },
48. {
49. "Key": "RequestID",
50. "Value": "RITM0012431"
51. }
52. ]
53. }
54. }

### Developer Notes:

IAM Role Creation – Form Design

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Description** | **Validation if any** |
| Role Name | Single Line text | Name of the Role | Validate RoleName |
| Description | Single Line text | Description of the role | None |
| MaxSession Duration | Select Box | Maximum session duration that you want to set for the role | None |
| Path | Single Line text | Path where the role has to be created | Validate Path |
| Policy Name | List Collector | Policies that you want to attach to role | ValidatePolicyCountTo10 |
| Trusted Service | Lookup Select Box | Services of the role | None |
| Role Check | Check Box | To check if all validations are satisfied | OnSubmit |

Default Values

|  |  |  |
| --- | --- | --- |
| **Key Name** | **Default Values** |  |
| Path | / |  |
| MaxSessionDuration | 1 |  |

Internal Mapping in Form

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Name** | **Type** | **Table** |  |
| PolicyName | List Collector | CE IAM Policy[u\_cmdb\_ci\_ce\_iam\_policy] |  |
| Trusted Service | Lookup Select Box | CE Cloud Services[u\_cmdb\_ci\_ce\_cloud\_services] |  |

\*Validate RoleName :

This Script is to validate if given role name is unique and matches the regex pattern provided. The Regex pattern consists of alphanumeric characters and \_+=,.@-' . And this will invoke the backend script “ce\_validate\_role \_aws” which in turn return a list of roles on the fly from aws console via REST API “AWSOAUTHENDPOINT”. This is to avoid the duplicate value of role name.

\*Validate Path :

This script is to validate the path provided using regex pattern. The path should begin and end with ‘/’ and contain alphanumeric characters and \_.

\*Validate PolicyCountTo10 :

This script is to validate the number of policies per role must be 10.

\*OnSubmit:

This script is to validate the variable rolecheck. The request will be processed only if the variable returns true.

Automation Workflow:

The “ScriptFiles” section contains the scripts location in the github repo and ScriptPayload” contains the list of inputs to be passed.

The ResourceDeploymentStepapigateway invokes ResourceDeploymentSingleStepFunction.

The following operations happen in the “ResourceDeploymentSingle”stepfunction:

1. The“ResourceDeploymentStep” lambda is invoked .
2. Lambda will check the input format of payload and verifies it. It also get the credentials through the role associated to it for the below executions.
3. It will get the git repo credentials from the SSM parameter store and then download the IAM\_Role.py and IAM\_Role.yml files in s3.
4. Then the inputs will be passed to the python file where it will trigger the CloudFormation Template file from S3 bucket if the stack has to be created.If there is no stack creation, python file itself will do the required activity.
5. The final activity of the step function is to notify success message to servicenow if the stack is successfully created.
6. If there is no stack creation involved, it will directly notify the servicenow after the python scripts successfully executes

Error Handling:

1. Step function will check if the stack is successfully created. It will notify service now of the status of stack creation if error
2. If there is no stack creation, it will notify servicenow if there are any error from python scripts.
3. Any other runtime error from step function /lambda is also notified to servicenow.