Restricting EC2 Actions using Custom IAM Policy

⚠ Please note a better and more modern approach detailed here: AWS Tagging and IAM Policies

Scenario

Allow a set of target users to login to the AWS console, and allow them to stop or start only their EC2 instances, based on tag values of the instances.

First Pass Solution

This solution allows a single specific user to manage an instance.

1. Create a new role as in Creating Custom Roles to use With Shibboleth.
    a. Name the role "shib-ec2control".
    b. Create the corresponding AD group and add target users as members. (As described in the link, this step needs to be completed by the Cloud Team.)
2. Add the following inline policy to the new role:
    a. Custom JSON for the policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/TargetUser": "${aws:userid}"
                }
            }
        },
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Effect": "Deny",
            "Resource": "*"
        },
        {
            "Effect" : "Allow",
            "Action" : "ec2:Describe*",
            "Resource" : "*"
        }
    ]
}
```

3. Determine the RoleId (aka PrincipalId) of the role.
    a. This is hard to find in the AWS Console. Use the AWS CLI instead:
        i. To get just the RoleId:

```
aws iam get-role --role-name shib-ec2control --query "Role.RoleId" --output text
```

or, to see the entire description of the role:

```
aws iam get-role --role-name shib-ec2control
```

ii. A example RoleId "AROAJRGJOYWPGTTYSJNDS"

4. Label EC2 instances with "TargetUser" tag according to which user should be allowed access to each instance. In order to allow "pea1" to stop /start an instance, give the instance the following tag:
    a. "TargetUser" = "AROAJRGJOYWPGTTYSJNDS:pea1@cornell.edu" The tag value should be "ROLE_ID:NETID@cornell.edu" where
        i. ROLE_ID is the ID of the role determined earlier.
        ii. NETID is the Cornell netid of the user to be allowed control.

Alternative Solution

This solution allows anyone who can login with a given role access to control an EC2 instance.

1. Create a new role as in Creating Custom Roles to use With Shibboleth.
    a. Name the role "shib-example2".
    b. Create the corresponding AD group and add target users as members.
2. Add the following inline policy to the new role:
    a. Custom JSON for the policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/TargetRole": "example2"
                }
            }
        },
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Effect": "Deny",
            "Resource": "*"
        },
        {
            "Effect" : "Allow",
            "Action" : "ec2:Describe*",
            "Resource" : "*"
        }
    ]
}
```

3. Label EC2 instances with "TargetRole" tag according to which role should be allowed access to each instance. In order to allow users from the "shib-example2" role to stop/start an instance, give the instance the following tag:
    a. "TargetRole" = "example2"

References

- https://aws.amazon.com/premiumsupport/knowledge-center/iam-ec2-resource-tags/