sonraí SECURITY

AWS IAM BREAKDOWN

Terms to Know

Organizational units (OUs) to group accounts together to administer as a single unit.

AWS Service Control Policies (SCPs). These are "guardrails" within the AWS organization OU to disable service access on the principals in the account.

AWS Identity and Access Management (IAM) is where you configure "permission policies" and "permission boundaries." These are used to grant more granular permissions on IAM principals, including controlling the maximum they can set.

AWS Security Token Service (STS) is available so you can "scope-down" policies. Reduce the general shared permissions even further from an IAM policy for a limited time frame or to assume a role.

Virtual Private Cloud (VPC) endpoints and endpoint policies are where you control access to services with a VPC endpoint.

Permissions boundaries. They are a way for you to scale and delegate permission management to devs or other groups and gives you (as an administrator) the ability to control the maximum permissions that others can grant.

Specific AWS services and resource-based policies are typically used for cross-account access and to control access from the resource.

How these all work together in a single account

1. You should have an SCP and you should have an IAM policy OR a resource-based policy.
2.
3. If you have an IAM Policy, you will need a permission boundary AND permission policy AND a scope-down policy. Again, this is per account so please keep that in mind.

4. Cloud admins can create exceptions so you can still do what you need to.

Caution! *Default access permission is "DENY" if a policy does not explicitly give access (or "ALLOW"), the default will take precedence.*

Example of AWS Access Policies

You need to specify which IAM principals are allowed to perform which action on a specific AWS resource and under which conditions.

SCPs allow you to define which AWS service APIs can and cannot be executed by AWS Identity and Access Management (IAM) entities (such as IAM users and roles) in your organization's member AWS accounts. SCPs are created and applied from the master account, which is the AWS account that you used when you created your organization.

If you just take that section and put it on a post-it note (good luck fitting it all in) at your desk, you will rock your AWS IAM policy definitions. If you need more help with IAM in the cloud, contact us.

WS IAM policy structure.

Whether you're in the console at the command line, you will need to understand the PARC model:

```
{
 "Statement":[{
   "Effect":"allow or deny",
   "Principal":"principal",  (This is the
entity that is either allowed or denied
access*)
   "Action":"action",  (The type of action
that is allowed or denied)
   "Resource":"arn",   (The AWS arn for
the resource)
   "Condition":"condition",  (And what
conditions need to be met i.e. tags)
   "Key":"value"}
   }
  }
 ]
}
```

To learn more about identity and data protection for AWS contact us at sonraisecurity.com