Building for the future with AWS Identity Services

Karen Haberkorn
Director of Product Management, Identity
AWS
A year like no other
Accelerating identity trends
Accelerating identity trends
Accelerating identity trends
Building for the future means establishing the right foundations today
Agenda

1. Organize your AWS environment
2. Centralize identity management
3. Establish a data perimeter
4. Journey to least privilege
5. Identity specialist panel
Organize your AWS environment
A security boundary for your applications
Planning for growth
Multi-account management with AWS Organizations

- Centrally provision accounts
- Organize accounts and workloads
- Automate infrastructure management
- Share common resources between teams
- Implement security controls
- Organize costs and identify cost savings
- Assign delegates for different functions
Centralize identity management
Come as you are
AWS Single Sign-On – The identity hub for AWS

Centrally manage access to AWS accounts, business applications, or both
Establishing a data perimeter
How do I ensure that only my employees have access to my most important company assets?
How do I make sure an employee doesn’t move important information outside of our corporate environment?
What is a data perimeter?

A set of preventive guardrails that ensures that access to trusted resources is restricted to trusted identities from expected network locations.
Tools for your data perimeter

Service control policies
Permissions guardrails for identities

“Prevent users from copying data to Amazon SNS topics that do not belong to my AWS Organizations organization.”
Tools for your data perimeter

1. **Service control policies**
   Permissions guardrails for identities

2. **VPC endpoint policies**
   Ensure network access only from trusted identities

“Prevent users from outside my organization from moving my customer data through this VPC endpoint to an Amazon S3 bucket that I don’t own.”
Tools for your data perimeter

1. **Service control policies**
   Permissions guardrails for identities

2. **VPC endpoint policies**
   Ensure network access only from trusted identities

3. **Resource-based policies**
   Ensure access only by your identities and AWS services

“Prevent access to this Amazon SQS queue from identities outside my accounts in AWS Organizations unless they are AWS services.”
Tools for your data perimeter

1. Service control policies
   Permissions guardrails for identities

2. VPC endpoint policies
   Ensure network access only from trusted identities

3. Resource-based policies
   Ensure access only by your identities and AWS services

... and more to come
Journey to least privilege
Least privilege is a journey
Getting to the right permissions

Data perimeter
Getting to the right permissions

Data perimeter

Set -> Verify -> Refine
Set permissions: Policy generation with AWS IAM Access Analyzer

Helps you get to the right permissions more quickly by analyzing your access activity
Set permissions: Policy validation with AWS IAM Access Analyzer

Makes it easier to author secure and functional policies with over 100 checks
Verify permissions: Policy preview with AWS IAM Access Analyzer

Verify access to critical resources meets your intent with provable security – before you deploy permissions changes.
Refine permissions: Action last accessed

Identify unused permissions to tighten access

Data perimeter

Set ➔ Verify ➔ Refine

NEW

Access Advisor shows the services that this role can access and when those services were last accessed. Review this list to identify unused and update access.

Allowed management actions for Amazon EC2 (440)

Access Advisor reports management action activity that is logged by CloudTrail for this service. Recent activity usually appears within 4 hours.

<table>
<thead>
<tr>
<th>Action</th>
<th>Last accessed</th>
<th>Region accessed</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateCarrierGateway</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateClientVpnEndpoint</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateClientVpnRoute</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateCustomerGateway</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateDefaultSubnet</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateDefaultVpc</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateDhcpOptions</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateEgressOnlyInternetGateway</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateFleet</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
<tr>
<td>CreateFlowLogs</td>
<td>Not accessed in the tracking period</td>
<td></td>
</tr>
</tbody>
</table>
Identity specialist panel
Coming up next

Brigid Johnson
Sr. Software Development Manager
AWS Identity

Jesse Fuchs
Sr. Security Solutions Architect
AWS Identity
Thank you!