AXIOMATICS

Applying ABAC to your cloud migration

As enterprises continue to rapidly adopt and migrate data, applications and assets to the cloud, new challenges and opportunities arise. A significant challenge that has emerged is how to protect enterprise resources in an open, cloud environment while still meeting increasingly stringent security regulations and controls. While this balance is a challenge, it does present an opportunity to rethink how your organization manages identity and access management (IAM) and how to ensure your cloud enterprise is prepared for future security challenges.

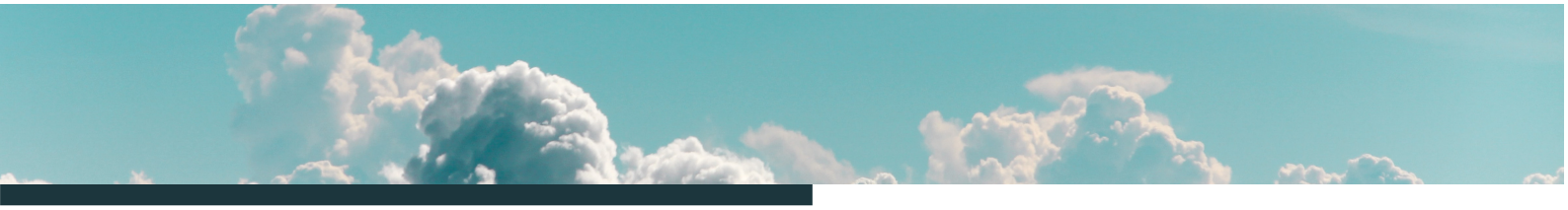
Dynamic authorization delivered through Attribute Based Access Control (ABAC) is the new model for performing access control. ABAC takes advantage of attribute values from subjects, resources and the environment to make access control decisions based on digital policies that define how resources may be accessed. As software-as-a-service (SaaS) and cloud-based applications become predominant in your organization's cloud infrastructure, a dynamic authorization model leveraging ABAC ensures your policies are uniformly enforced across all cloud resources.

A cloud migration use case in action

Cloud migration and other modernization efforts are challenging for the modern enterprise. As legacy applications and services are transitioned to the cloud, efforts must be made to ensure the new services are certified against new sets of cloud-based security standards. Access control and authorization approaches are scrutinized against this new model.

By outsourcing application access control to a centralized service, a consistent means of authorization can be applied uniformly to all applications and cloud resources. This is achieved by transforming an enterprise's natural language policies into digital policies and then enforcing those policies through an Externalized Access Management (EAM) service, which contains a centralized digital policy management (DPM) store.

Commercially available cloud offerings include built-in security features such as IAM. However, these services are typically associated with an identity that has been authenticated by the cloud infrastructure security.



While these services are invaluable, using an ABAC implementation extends access control beyond the cloud offering. ABAC allows for consideration of subject (e.g. identity), resource (e.g. metadata), and environment (e.g. geographic location) and the relationship between these values when performing an access control decision. This enables a much finer-grained access than would be possible when only considering identity.

Another benefit to ABAC in the cloud is taking advantage of having a central location where all cloud access control decisions take place. By integrating an EAM service with existing cloud & network monitoring services (e.g. Amazon's CloudWatch), you can collect and track metrics on virtually every access control request and decision made in the cloud. Triggers and alerts can then be implemented as well to notify someone if, for example, too many access request denials are issued within a given period. This could extend your existing intrusion detection capabilities.

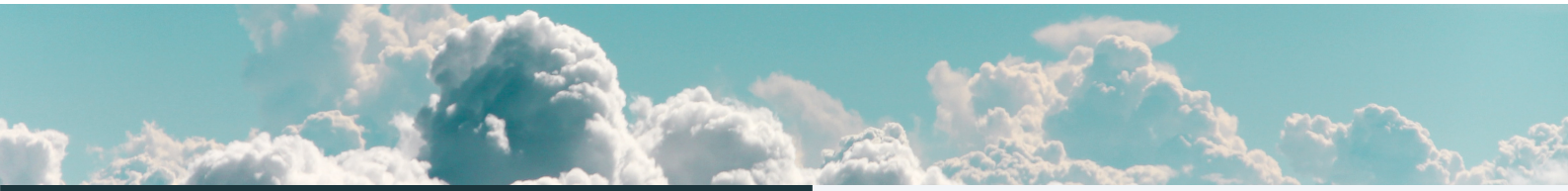
Finally, an ABAC-approach is especially well-suited during an enterprise's transition to the cloud. During this transition there is a mix of on-premise applications and cloud services. While applications are moving to the cloud, an ABAC service can apply policies and enforce decisions within both environments while only having to manage policies in one location. This will help ease the transition of applications into the cloud as the authorization service already exists in the cloud.

In summary, when migrating to a cloud infrastructure, implementing an EAM system to extend your cloud's IAM services will provide fine-grained access control, tighter control of your cloud resources and a central authorization service to log, monitor, and analyze your cloud's access control decisions. Digital policies can be constructed to reflect enterprise-wide security policies and can be uniformly applied throughout your cloud infrastructure to ensure you know who is accessing which cloud resources and when.

About Axiomatics

Axiomatics is the originator and leading provider of runtime, fine-grained, dynamic authorization delivered with Attribute Based Access Control (ABAC) for applications, data, APIs and microservices. The world's largest enterprises and government agencies use the Axiomatics Dynamic Authorization Suite to enable digital transformation, share and safeguard sensitive information, meet compliance requirements and minimize data fraud. Our innovative solutions enable enterprises to share sensitive, valuable and regulated digital assets – but only to authorized users and in the right context.

AXIOMATICS



The specifics

What

Large enterprises can take the opportunity during modernization and cloud migration to address access control challenges by managing access to sensitive data with dynamic authorization.

Who

There are many internal stakeholders who benefit from a dynamic approach. ABAC helps assure CISOs that access security controls are completed in accordance with the organization's security plan.

Compliance officers and auditors also take an active interest in how ABAC helps the enterprise meet, prove and govern compliance requirements.

Why

Axiomatics is the leader in fine-grained, externalized authorization management (EAM): the most adaptable and scalable way to solve data security concerns. Today, leading global automotive, pharmaceutical, banking, and defense manufacturers use our solutions to ensure secure collaboration and data sharing while leveraging the advantages offered by fine-grained access control.

How

Axiomatics provides a suite of solutions that enforce dynamic authorization at the application, API, and data layers from one centrally managed point. We consider the full context under which a user wishes to access data and permit or deny access accordingly. With a centralized authorization service, advanced auditing and reporting tools also ensure compliance is met on an ongoing basis, while real-time controls allow policy changes to be instantly enforced to meet rapidly changing regulatory environments.

Get more info and resources

- **Check out our blog**
- **Connect with our experts**
- **Visit us at axiomatics.com**

Follow and subscribe