THE COMPLETE GUIDE TO AUTHORIZATION

A PlainID Publication

plainID
THE AUTHORIZATION COMPANY

September 2019

Table of Contents

Authorization: A Company's Gatekeeper

Authorization is an essential part of an enterprise's IAM solution. As a company's "gatekeeper," it is the process that determines who can access which company data and resources. Authorization solutions have evolved from simple user access lists, which match users to resources, to multidimensional policy-making algorithms that can use features such as time of day or user location as factors in deciding whether or not to grant access to resources or even determine what subset of resources should be made accessible and in what format.

All Authorization systems share a common purpose: helping an organization protect its greatest non-human asset, its data.

THE COSTS AND RISKS OF INADEQUATE AUTHORIZATION SOLUTIONS

Inadequate or incomplete Authorization solutions cost companies directly and indirectly. These costs include fines for lax data security, potential jail time, and liability compensation. Additionally, companies can easily run afoul of privacy regulations such as the GDPR. Ultimately, companies with poorly defined Authorization policies spend a lot of time and effort fixing problems that could have been avoided for a fraction of the cost. The issue has indeed made its way to the top of the ranks, and is often a regular boardroom topic.

And just as important are the everyday costs and risks from inadequate authorization solutions. The inability to adjust policies to market drivers, or the inability to adjust policies to regulatory drivers, or simply the fact that an organization becomes handcuffed by aging systems that are slowing their time to market can be a dark spot on a company's bottom line. Popular models such as Zero Trust or CARTA encourage the use of context-aware, adaptive and programmable security platforms.In addition to these new models, the ability to make decisions based on dynamic data is crucial for limiting risk - a major concern for any enterprise.

Keeping data safe and avoiding breaches is what Authorization is all about. Ensuring the right people have the right access dynamically, at the right time is fundamental. This eBook discusses four of the most important Authorization management methods: Access Control Lists, Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and the best approach for the present and the future, Policy-Based Access Control (PBAC).

EARLIER SOLUTIONS: FROM ACCESS CONTROL TO RBAC

ACCESS CONTROL LISTS (ACL)

Access Control Lists were the original Authorization/Identity Management solution and at first, this solution was enough for most companies. It involves stating exactly which users can work with each directory, file or application. This approach is still adequate for small organizations, but it doesn't work for even medium-sized ones, to say nothing of enterprises. Every new user must be matched to each resource separately, and likewise any new resource must be matched to each authorized user. This is a cumbersome approach; keeping up with all the changes in an organization can easily overburden an IT department, leading to mistakes and other disruptions.

THE NEXT STEPS: RBAC AND ABAC

The next major Authorization models to appear were RBAC and ABAC.

Role Based Access Control (RBAC)

Developed in the early 1990s, RBAC has remained one of the most popular approaches since. In RBAC, roles are created with specific permissions per resource (e.g. file, application, security group), and users are then matched to one or more roles. For example, a call center might need two roles: customer service representative (with read-only privileges), and supervisor (with modify privileges). Each employee is thus limited to certain predefined roles and the privileges assigned to them. Roles are constant no matter the circumstances, such as the time of day or the user's location. RBAC is used primarily for a "coarse-grained" Authorization solution, as it supported the usage of entitlements or security groups, opposed to "fine-grained" solutions which do support a more in-depth control of the application and data.

Limitations of RBAC

While some businesses don't require fine-grained Authorization, RBAC has several limitations and drawbacks. Many enterprises using this solution suffer from "role explosion". This occurs when there are many similar but slightly different roles being administered within any given enterprise. Whenever a new resource is added, each of these roles must be modified accordingly, adding to maintenance costs and increasing the possibility of error. Additionally, as InfoSec Institute notes, one problem with RBAC is that "roles are only associated with the position." So, if a user legitimately needs access to data or files that were not associated with their role when it was defined, an RBAC solution will prevent that user from accessing the data they need to do their work. Since many workers do need this kind of "extra permission" from time to time, RBAC's model lags behind the dynamism of the modern workplace.

Moreover, RBAC's static nature creates additional system management overhead for IT teams to ensure that employees have the most current permission set. TechTarget observes that with RBAC, system admins must "periodically conduct audits of the roles, the employees who are assigned to them, and the access that's permitted for each role." Thus, managing these roles, users, and their interrelationships is a formidable task that requires continuous maintenance and management of hundreds or thousands of roles across multiple applications.

Finally, it's a serious risk for companies that do not have the ability to manage their growing number of roles. For example, when employees change jobs, more often than not, their past roles and access remain unchanged, and new access is likely 'rubber stamped,' instead of being carefully evaluated. It's not too hard to imagine this: An employee who has changed positions multiple times over the years might have layers upon layers of access rights, and if their credentials are ever compromised, a major breach is sitting there like a time bomb.

ABAC

ABAC was the first major attempt to go beyond RBAC. ABAC takes a different approach to Authorization by using attributes such as an employee's location, time of day, or the data classification to determine access rights. For example, an ABAC system might authorize an employee with the proper security clearance level access to a sensitive document during work hours, but not at 2 AM. This gives ABAC more flexibility than RBAC, which doesn't have that level of granularity.

ABAC makes Authorization decisions by applying rules written in computer languages such as: eXtensible Access Control Markup Language (XACML), or the later, more advanced Next Generation Access Control (NGAC). These rules apply Boolean logic to combinations of users and attributes to grant or deny access to a given resource.

Limitations of ABAC

Although ABAC offers more flexibility than RBAC, ABAC has an important limitation: It provides a localized solution for apps that can be customized to its end-points and it requires full reliance on attributes, which are not always properly defined.

A BETTER SOLUTION: POLICY BASED ACCESS CONTROL

ENTER PBAC

Policy-Based Access Control, or PBAC, combines the best features of RBAC and ABAC. Complexity can easily be reduced by adding an attribute "dimension" to the traditional role. For example - the role of country managers can now have multiple attributes such as the name of the country he is manager of. In addition, it goes one step further by adding in support for working across the enterprise, account managers will have the ability to access only the accounts in their region, both from the data portal or when searching in the archive. **PBAC also allows for contextual decisions that can be based on anything - from what device you're on to your IP address, and then making decisions based on that person's context. This means PBAC provides both *adaptive* and *contextual* access.**

When implemented on a graph database technology interface, PBAC enables the greatest flexibility, by supporting complex policies and advanced data structures. Additionally, graph technology offers the ability to ask the authorization question from different angles. For example: Can John access this account? What accounts can John access? Who can access this account?

According to KuppingerCole, PBAC is "the harmonization and standardization of the ABAC and RBAC models at an enterprise level in support of specific governance objectives."

Like RBAC, PBAC supports roles, although it does not require them. So, PBAC can easily support a rule such as "Stockbrokers can access a certain database during working hours but not afterwards." Since companies generally want to connect access rights with jobs, it's useful to support "roles", in some form, as a criterion for Authorization decisions. But, unlike the roles in RBAC, roles in PBAC don't have rigid definitions, specifying access rights for every resource for every role. If a new resource is added, the policy automatically assigns it to the relevant roles.

PBAC supports both dynamic run-time Authorization and admin-time authorization.

- **Run-time authorizations** are access decisions based on current attributes and conditions that are calculated during the user access request. Run-time authorization provides the flexibility to consider current status and events as part of the making the access decision, therefore are typically more accurate.
- **Admin-time authorizations** are pre-authorized decisions, access decisions made in advance to the user access, and typically provisioned to the application repository. Authorizations in this case are typically set during the user on-boarding, role changing events, or as part of a request process.

PBAC'S ADVANTAGES

In addition to supporting a wide variety of flexible, authorization languages, ranging from coarse to fine-grained, PBAC offers businesses a number of advantages. First, because it makes it possible to articulate access control rules in natural language, it enables business owners to be involved and gain control of access policies rather than leaving Authorization to IT. This is important, because in the end, decisions about corporate data and access to it must make business sense. What PBAC enables is flexibility - these decisions can be made by IT, by business application owners, or both. This gives the application owners a level of visibility that they've never had before.

Second, PBAC reduces the amount of access decisions to manage and govern, supporting a much more efficient audit and compliance process. In many cases, PBAC can reduce the amount of decisions to govern by more than 50%.

Third, PBAC allows enterprises to fully embrace recent industry standards such as Zero Trust and CARTA. By enabling fine grained access control 'on the fly', a policy based approach is the only way to always know who has access to what, and when.

And finally, PBAC provides a virtualization layer between business and technology, enabling the access decisions to be managed regardless, or with limited reliance on the underlying technology. This is the primary reason PBAC is highly recommended for organizations who wish to modernize their data center. PBAC will support current access rules, and enable the transition to a modernized approach.

THE FINANCIAL BENEFITS OF PBAC

In addition to being an excellent Authorization solution for a wide variety of businesses, PBAC offers important financial benefits in a number of areas:

- Improved customer retention rate due to reduction/elimination of data breaches
- Cost improvements:
  - The simplicity of creating Authorization rules reduces IT costs and time to market for new services
  - PBAC's fine-grained Authorization and transparency helps businesses identify and eliminate malicious intent and/or manipulation of access controls
  - Reduces the amount of time and money that your IAM team must spend reinstating authorizations
  - Increased security results in avoidance of data breach-related expenses, fines and compensation (including illegal further processing or use due to lack of consent)
- Productivity gains:
  - Your IAM team can spend less resources on Authorization and more on other important assignments
  - Less tickets filed with IT means they're under less strain, allowing them to focus their time on other critical issues
  - Less user downtime since fewer of their authorizations need to be reinstituted
  - Better Authorization supports safely, enabling more self-service provisioning through a workflow system
  - Support for comprehensive global policies to control resource authorizations
  - Faster and comprehensive IAM Control Effectiveness/Audit Attestation processes
  - Cost reduction in replicating and maintaining identities across the application portfolio
  - Having a single process for all resources reduces the complexity of requesting additional authorizations
- Reduced business risk and improved compliance with regulations:
  - Reliable, comprehensive and complete termination of incorrect user entitlements
  - Improved application of policies and accounting for information barriers and segregation of duties
  - improved compliance with regulatory policies such as GDPR, SOX, and HIPPA

Overall, PBAC offers cost saving benefits that other Authorization models simply cannot provide. When implemented on an intuitive, user-friendly interface, PBAC allows you to spend your time focusing on what you do best, rather than be preoccupied with Authorization.

THE PLAINID PBAC ADVANTAGE

PlainID's SmartAuthorization platform offers an innovative, business-friendly PBAC Solution, providing:

- **Business-oriented approach** - Providing the business owner control and visibility to their assets, apps and data.
- **Policy lifecycle management**- Enable the policies to be built in a studio environment, tested, validated, and then sent to an approval process in a higher environment before deployed
- **Delegated Administration** - Creating hierarchical management areas for policies, each having its own policy admins and approvers.
- **In-depth Analytics and Insights** - providing visibility to the access decisions, including the effect of the policies on the identities, assets and apps.
- **Compliance and SOD** - presenting complaint violations and part of the approval process or enforcing SOD policies at run-time.
- **Universal Authorization support** - supporting multiple authorization languages and standards.
- **Contextual access** - Access is calculated in real-time, based on the context in which the user is accessing.
- **Fine-grained Authorization** - Access decision can be provided to any level of granularity, up to row and column level access.
- **Virtual identities and assets** - Identities and assets are modeled using a virtualization layer, that can be tied to one or more sources of truth.
- **Limiting risk** - the ability to make decisions based on dynamic data is a must when limiting risk and ensuring compliance with relevant regulations.

PlainID can tell you who has access, when they have access, and how they have access. By letting you change these on the fly, PlainID's Policy Based Access Control solution offers the most fine grained approach possible.

PLAINID IN ACTION: A CASE STUDY

Nothing tells an Authorization company's story better than a case study. We recently helped a large US global bank that had tens of thousands of users, over 5,000 different roles, and strict compliance requirements for network, data, and applications service.

The bank was suffering from significant Authorization management overhead that was time-consuming and left potential security holes that were hard to detect. Change requests took time, audits were difficult, and access control was left to multiple systems with business stakeholders finding it difficult to track access to resources, apps, and data. For the IT staff, all of this was controlled and deployed manually, creating a growing overhead and expense.

After deploying PlainID's SmartAuthorization solution, the bank was able to reduce the 5,000 roles into 251 coherent policies. This led to a tangible reduction in IT costs, faster go-to-market time, and an advanced analytics tool that helped them manage these policies as well as the entry points into the system, giving business stakeholders control over access to resources. In short, PlainID made Authorization one of the bank's assets, instead of one of its liabilities.

INTERESTED IN LEARNING MORE?
SCHEDULE A DEMO WITH THE PLAINID TEAM.

REQUEST A DEMO

plainID
THE AUTHORIZATION COMPANY