NEXTLABS®

White Paper

Managing Role and Group Explosion with Dynamic Authorization

Current Trends Driving Access Management Requirements

We see several major trends that have recently been driving enterprise access management requirements and expect that they will continue exert influence in the future. Organizations must plan for how their access management needs are impacted, including the impact to roles assigned to users within applications and the groups to which they are assigned through user management technologies such as Active Directory (AD) or LDAP.

Move to Zero-Trust Security Models

The National Institute of Standards and Technology (NIST) has adopted as a recommendation (NIST 800-207) that organizations implement a Zero-Trust approach to their security. This means that authentication and authorization are being pushed down to the more granular level where access is being requested to specific resources or specific data. Users are no longer assumed to be trusted if they have access to a network or system, as the principle of "Never Trust, Always Verify" is applied to access requests. As part of adopting NIST's recommendations, enterprises have updated their security models to be more data-centric, where the specific data that is sensitive or valuable is protected, instead of the network or system where it is located. With the increase in the number of requests, and access controls being applied at a more fine-grained level, managing access with users and groups can be too rigid and does not allow for the flexibility to dynamically adapt to the changes that are necessary.

Globalization

Large enterprises are increasingly expanding internationally to drive revenue growth, with the rise in global platforms making this a more attractive strategy than ever before. The barriers to global trade are much reduced when compared to the past, and the ease of communication and information sharing across international borders has lowered the investment required to operate in multiple countries. This has allowed enterprises to globalize their workforce, production, and distribution to maximize the local advantages of each region and improve profitability.

Allowing Access from Anywhere and Any Device

With the globalization of workforces and their distribution across wide geographic areas, organizations are finding that employees need to access shared resources from a much more varied range of devices, networks, and time zones. It is no longer possible for an organization to assume that all employees will be accessing resources from the same type of systems, from the same network, or even during the same working hours. Some organizations have even taken the approach of allowing employees to use their own devices, known as 'Bring Your Own Device' or BYOD, to access corporate resources. This means that sensitive resources may be accessed from a wide range of device types, from many different locations, and at many times of the day. Many of these environments are increasingly out of the control of the organization.

Industry Consolidation

As more companies are operating on a global scale there is pressure for their smaller competitors in each industry to grow as well. Companies can face pressure to become more vertically integrated, both as a way of having more control over their entire customer experience, as well as their supply chains, so can expand both up and down the value chain from their current position. There is also pressure from competitors who are in adjacent industries, and companies may choose to expand horizontally as well to protect themselves from competitors doing the same. New consumer, technology, and business trends can even create new markets that companies need to enter quickly to take advantage of a time-limited opportunity. Finally, even companies that already dominate their industry can face pressure from investors to maintain high growth rates and must expand into additional markets to do so.

Although some organizations will grow organically, many will expand through mergers, acquisitions, or establishing joint ventures as the pathway to growth, and therefore need to integrate existing operations at the acquired company into their own business processes. This needs to be done in a way that does not disrupt ongoing operations at either the parent or newly acquired company but does ensure that the best aspects of both are incorporated across the entire enterprise.

Global IT Consolidation

Even though it may make IT operations more complicated, organizations have many incentives to consolidate their IT resources. One obvious benefit is that fewer but more wide-reaching systems take fewer resources than more numerous but smaller systems. Fewer employees are needed to set up and maintain one large system because it can be managed by a single IT team. There are also economies of scale in procuring and maintaining a single large system versus multiple smaller systems because that larger system can be used more efficiently. This is especially true for organizations that have globally distributed operations. If teams using the systems are spread across different time zones, the number of concurrent licenses and system capacity can be more efficiently used than if usage is concentrated into only a few hours each day. Organizations can also locate their IT operations in the geographic locations that provide the best access to the employees and IT assets that IT depends on. This includes the options that are now available to host systems in the cloud, and to incorporate SaaS solutions instead of on-premises software.

Why Role and Group Explosion is a Challenge

Although there are the clear benefits to the trends described above, a specific access management challenge that comes with all, and especially the combination of, these trends is that of role and group explosion. This refers to the exponential increase in complexity of the access that needs to be granted to controlled resources and data. This is especially true when implementing the fine-grained controls as part of a Zero-Trust approach. In traditional Role-Based Access Control (RBAC), each access combination would be specified by a specific role, and users of a system would be members of all the roles that cover the access that they require. In globally consolidated systems, which are used by multiple users in multiple locations to access different types of data through different applications, the number of required roles "explodes" and becomes unmanageable.

Here is a simple example of how just a small number of combinations can quickly result in a much larger number of roles or groups that would need to be created to implement role-based security.

Attributes	Possible Values	# of Roles/Groups
Project Membership	PR01, PR02..	10
US Citizen	No/Yes	2
Location	US, China	5
Export License	NR, ITAR, EAR	5
NDA	No, NDA-01	5
Usage	View, Change, Copy, Send	4
		10,000

As you can see, even this small number of combinations of attributes results in many security roles or user groups required.

One way in which Role Base Access Control has been expanded is to separate functional authorizations and organizational authorizations. Within SAP, for example, this concept is referred to as Enabler Roles. To gain access within SAP, both functional and organizational authorization objects are required.

This does help reduce the challenge of Role Explosion, but as you can see in the example below, it does not completely solve the problem of exponential growth.

Scenario	Derived Role	Enabler Group	Functional Role +ABAC Policy
5 Company Codes per Company 50 Functional Roles in the Company	300 roles: • 50 * 5 = 250 • 50 • 300 Roles	56 roles: • 50 Functional Roles • 1 Enabler Template Role • 5 Enabler Roles Values (CC)	• 50 Functional Roles • 1 ABAC Policy • 1 Data Attribute
7 Plants/Company Code (35 plants)	2050 roles • 50 * 5 * 7 = 1750 • 50 * 5 =250 • 50 • 2050 Roles	87 Roles • 50 Functional Roles • 2 Enabler Role Templates • 35 Enabler Role Value Pairs (CC, Plant) • 50 + 2 + 35 = 87	• 50 Functional Roles • 1 ABAC Policy • 2 Data Attributes
10 Storage Locations	19,550 roles • 50 * 5 * 7 * 10 = 17,500 • 50 * 5 * 7 = 1,750 • 50 * 5 = 250 • 50 • 19,550 Roles	403 Roles • 50 Functional Roles • 3 Enabler Role Templates • 350 Enabler Role Value Pairs (CC, Plant, Storage Location) • 403	• 50 Functional Roles • 1 ABAC Policy • 3 Data Attributes
100 Programs	1,769,550 roles • 50 * 5 * 7 * 10 * 100=17,500 • 50 * 5 * & * 10 = 17,500 • 50 * 5 * 7 = 1,750 • 50 * 5 = 250 • 50 • 1,769,550 Roles	35,054 Roles • 50 Functional Roles • 4 Enabler Role Templates • 35,000 Enabler Role Value Pairs (CC, Plant, Storage Location, program) • 35,054	• 50 Functional Roles • 1 ABAC Policy • 4 Data Attributes

As you can see in this example, although Enabler Roles reduce the number of roles that need to be defined, they are still growing exponentially as more attributes are incorporated into the security model. On the other hand, as we will cover in detail in the next section, if an organization is using ABAC policies, the additional attributes can be added to the policy, but the number of policies stays the same.

Enhancing Role-Based Access Control (RBAC) with ABAC

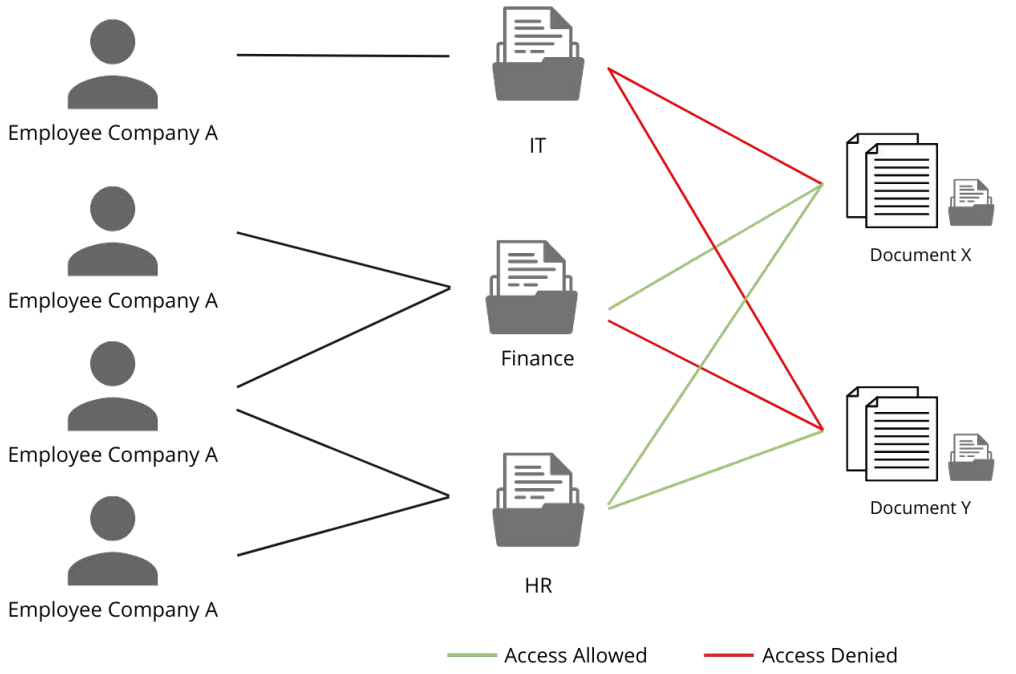
ABAC allows an enterprise to extend existing roles using attributes and policies. Combining RBAC and ABAC into a single hybrid ABAC / RBAC (ARBAC) solution can provide a future-ready identity and access management solution capable of designing and enforcing rules based on individual profiles and business environment parameters. By adding context, authorization decisions can be made based not only on a user's role, but also by taking into account who or what that user is related to, what that user needs access to, where that user needs access from, when that user needs access, and how that user is accessing the requested information.

ABAC does this by using policies built upon the individual attributes using natural language. For example, a policy may be written as follows: "Doctors can view medical records of any patient in their department and update any patient record that is directly assigned to them, during working hours, and from an approved device." By creating a policy that is easy to understand, with context around a user and what they should have access to, access control becomes far more robust. This functionality expands the scope of RBAC significantly. We no longer need hundreds of overloaded roles, and administrators can add, remove, or reorganize departments and other attributes without having to rewrite the policy. At the end of the day, fewer roles mean simpler role management and easier identity management. Moreover, ABAC enables the execution of business initiatives not previously possible via RBAC alone.

How Attribute-Based Access Control Addresses Challenge of Role and Group Explosion

An example of how hybrid ARBAC policies can be used to reduce the number of roles and groups required is to supplement a user's functional role(s) and assigned group(s) with user, environment, and data attributes. For instance, access to regulated information (data attribute) could be limited to users that are members of a specific group and role (user attributes) but only if they are accessing the data from their designated office and during normal business hours (environmental attributes). Defining access policies in this manner requires a much smaller number of policies to be defined and allows for policies to meet the Zero-Trust goals of being more fine-grained and data-centric.

As an example, here is how access to HR and confidential classified documents might be controlled using Role Based Access Control (RBAC) without ABAC.

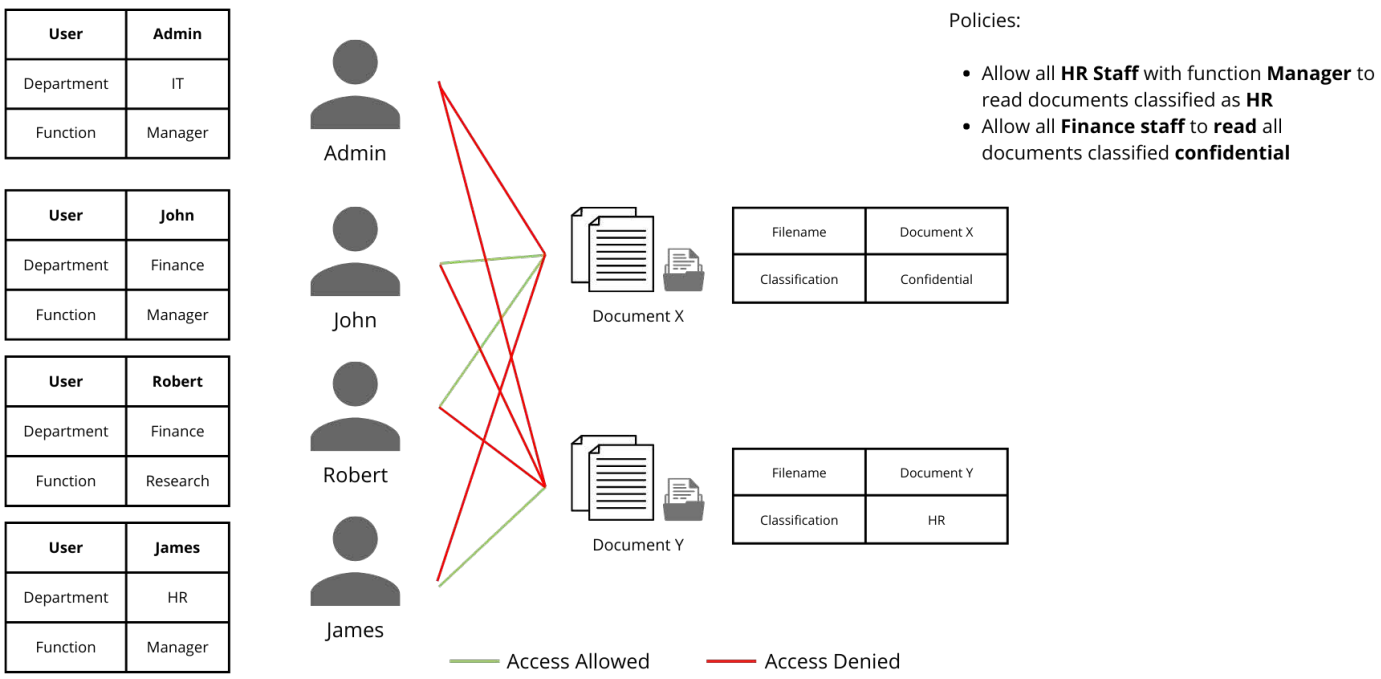


ROLE	ACCESS
IT	Deny
Finance	Full Access
HR	Read Only

ROLE	ACCESS
IT	Deny
Finance	Deny
HR	Read Only

Three roles, of IT, Finance, and HR would be created and access to the documents would be based on the role of the user.

And here is an example of how two ARBAC policies can be defined to control access to those same documents and provide it in a much more fine-grained manner.



In this example, the policies incorporate attributes such as the user's department, title, and the classification of the documents they are accessing. By using attributes, these two policies replace 24 roles that would need to be defined for RBAC enforcement for an equivalent level of access.

- 3 Departments (HR, Finance, IT)
- 2 Titles (Manager/Non-Manager)
- 2 HR Classifications (Yes/No)
- 2 Confidential Classifications (Yes/No)

This would require the definition of 3 x 2 x 2 x 2 = 24 roles.

Using Dynamic Authorization to Implement Attribute-Based Access Control

A key part of making the most of ABAC access policies is to dynamically evaluate them at the time of the access request to determine whether access should be granted and if they are granted access what the requestor is authorized to do. This is a key component to implementing Zero-Trust security, every access request is evaluated at the time of the request, regardless of whether that user has previously been granted access to the requested resource or data. By using dynamic authorization, any changes in attributes or authorization levels relevant to the request are automatically incorporated in the evaluation and enforcement of the policy. This both reduces the effort required to keep policies up to date as well as reduces the latency in any changes taking effect. For instance, if there are changes in restrictions on handling data, whether for additional classifications of data that are restricted or new regulations that prevent data from being accessed by users in certain countries, the policies that govern access to that data can be updated with those changes and then since they are being dynamically evaluated and enforced the changes in access and authorization are immediate.

Using NextLabs' Zero-Trust Policy Platform to Prevent Role and Group Explosion

Dynamic authorization is the foundation upon which NextLabs' Zero-Trust policy platform rests. This is done through the definition and enforcement of ABAC policies utilizing attribute values, such as the user's clearance level and assigned role, data type and classifications, and environmental attributes such as time of day and IP address. By evaluating ABAC policies dynamically at the time of access request, NextLabs allows organizations to grant fine-grained access and entitlement to resources, allowing users access to only hat they need, and granting them the entitlements to only do what they should be authorized to do once they have that access.

NextLabs' data-centric dynamic authorization system with ABAC significantly streamlines the authorization management process. It removes the need to individually administer thousands or even hundreds of thousands of access-control groups and/or role and role assignments on a daily basis. Additionally, organizations do not need to deploy expensive and complex identity governance solutions. With ABAC, hundreds of roles can be replaced by just a few policies. These policies are managed centrally across all sensitive applications and systems, providing a single pane of glass over the "who, what, where, when, and why." Centralized management makes it easy to add or update policies and quickly deploy them across the enterprise.
NextLabs' data-centric dynamic authorization allows organizations to implement Zero-Trust and manage role and group explosion and is integrated into all NextLabs product lines, including:

- CloudAz, a unified policy platform that centralizes administration and utilizes the "never trust, always verify" principle, ensuring data is protected at any access point.
- Data Access Enforcer (DAE) helps enterprises protect data access from anywhere, by securing access and protecting critical data stored in databases and data lakes.
- SkyDRM ensures persistent protection of critical files and documents to protect data on the move and at rest.
- Entitlement Management / Externalized Authorization Management which can be used to secure applications, enforce data security controls, and simplify role management.

Key Takeaways

- The move to Zero-Trust security models, as well as the business trends of globalization, distributed access, industry consolidation, and global IT consolidation all increase the challenges of managing role and group explosion. Traditional Role-Based Access Control (RBAC) approaches require an exponential number of roles or user groups to be defined, and do not scale when authorization management is implemented on a more granular level.
- Moving towards an Attribute-Based Access Control (ABAC) security model and away from the traditional Role-Based Access Control (RBAC) allows organizations to avoid role explosion by defining data access and authorization policies in terms of attributes of the user, data, and environment.
- Implementing ABAC using dynamic authorization allows organizations to realize the Zero-Trust principle of "Never Trust, Always Verify", evaluating and enforcing policies at a fine-grained level at the time of the access request.

To learn more about how NextLabs helps organizations manage the challenges of role and group explosion by incorporating Dynamic Authorization and ABAC into all our products, please visit our Technology page.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.