Rights Over Roles: The Advantages of Role-Based Access Control (RBAC)

MATESO
PASSWORD SAFE

Preface

Defining and granting rights can present IT teams with various challenges. For example, when new employees join the company, they should be given access to all the access they need for their work as quickly as possible. Also, ongoing operations should not be disrupted by unnecessary restrictions. Again, employees should not be given too broad rights or access for too long in order to keep the potential for attack as low as possible.

After all, in digital times, it is more important than ever to keep authorizations for data access as low as possible. In line with the least-knowledge principle, a user should therefore only be given the minimum rights necessary to perform his or her tasks.

Role-based access control (RBAC) has therefore become a popular methodology for assigning permissions in enterprise IT infrastructure. Although the importance of RBAC is growing in enterprises, many are still reluctant to realize this – often out of concern for a costly and complex implementation.

This white paper therefore explains the different authorization models in comparison to RBAC as well as its advantages and areas of application in password management and provides valuable tips for practical implementation with Password Safe in organizations.

„What rights should the role have? And who should it be assigned to?“

If a company loses track of data access, it only exposes itself to unnecessary dangers that could have been prevented in advance by professional authorization management.

Initial Situation

If companies do not have a holistic concept for granting access rights to data and services, various risks and problems arise for them. On the one hand, authorizing each employee individually is extremely time-consuming for IT. It also increases the risk of overauthorization or that user rights are not revoked after use, resulting in superfluous rights that lead to accumulations of them. If there is no way of logging and tracking the assignment of rights, there is an additional risk of unauthorized access. When deciding on professional rights management, companies can draw on various principles. The most important three models are presented and explained below.

Presentation of Different Authorization Models

Identity Based Access Control (IBAC)

In Identity Based Access Control (IBAC), access rights are defined directly in relation to the identity of the subject, which makes this approach very easy to understand in application. However, this method is less suitable for large and highly networked enterprise architectures: It is difficult to scale as the number of users increases and the identity of the user is not related to their position or functionality.

As a result, it is easy to lose track of authorizations. In the event of a department or position change, where the user is assigned new activities and also accesses, all associated accesses would also have to be changed separately, which would be enormously time-consuming. In addition, the risk of incorrect and excessive authorizations increases, since it cannot be guaranteed that the user only receives the exact rights that he needs for his work.

Atribute Based Access Control (ABAC)

Attribute based access control (ABAC) uses attributes (characteristics) rather than roles to assign access rights. ABAC is a subcategory of RBAC, which enables even more detailed assignment of rights. With ABAC, specific characteristics are checked in order to make an access decision. Characteristics can be related to the person (user name, ID, age, ...), resources (what should be accessed?), actions (read, move, edit, delete, ...) or the environment (location, time, device, ...).

From these characteristics, rules are derived that define which of them must be met in order to either approve or deny access. For example, access to certain data outside business hours and without a company location could be prevented. So, compared to RBAC, this approach is more dynamic and offers even more options for assigning rights. On the other hand, the implementation and maintenance of ABAC is also a lot more time-consuming because of these: Defining all the necessary policies can mean checking and defining several thousand characteristics for IT.

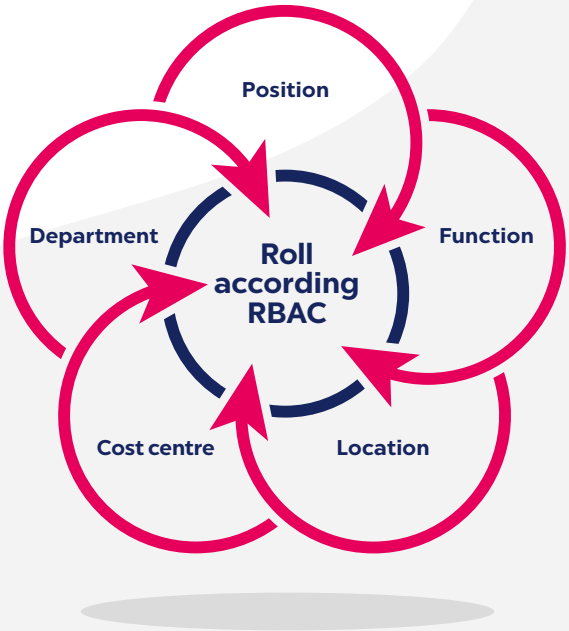
Role Based Access Control (RBAC)

Roles represent the linchpin between IT and business in companies, which is why the organization of these requires close cooperation and also prior planning. The goal should always be to define roles in a comprehensible and transparent manner and to keep their number manageable.

Role-based access control (RBAC) grants and revokes access rights to data and services not individually and directly to the user, but on the basis of the assigned role – in accordance with the least privilege principle. A user can be assigned to multiple user roles. Common permissions on data according to RBAC are „read“, „write“ and „delete“. Microsoft and Oracle Solaris also build on the RBAC principle, for example for permissions via AD groups on file server resources.

Definition of a Role

In companies, every employee has a special function that is reflected by his or her position and is assigned to a department, a location or even a cost center. If the employee is now assigned to a role according to these criteria, he automatically receives the respective authorizations to data that this role requires. In this way, roles can represent the complete hierarchy of a company in detail through the role concept.



„According to the least knowledge principle, employees only have access to the data set they need to work according to their role – and only for the period of time they need it.“

Technically, a role is nothing more than several users with the same permissions. For example, the role „Administration“ with extensive authorizations or the role „Marketing Assistance“ with authorizations limited to the department and function can be created. By working with roles, employees no longer need to be authorized individually, but are more easily assigned to their corresponding role.

With RBAC permissions, instead of direct permissions to each individual record, permissions are only managed through role memberships.

NIST recommendation for role definition: 4 levels

1. **Flat:** Assignment to a role directly gives users the rights associated with it. Thus, a user can be a member of several roles and a role can contain several users.

   Example: The role „IT“ is assigned to all users who require administrative rights.

2. **Hierarchical:** By inserting levels, roles can be set in relation to each other and rules can be defined as to how permissions are inherited. In Password Safe, this is mapped using organizational units.

   Example: In Active Directory, the group „Inside Sales Manager“ inherits rights from the organizational unit „Sales“, to which it is subordinate.

3. **Restricted:** Depending on the assigned role, actions of users can be restricted. In Password Safe, this is mapped by restrictive users or additional protection mechanisms such as the multiple-eyes principle, temporary release limits or password masking.

   Example: A user can only use passwords for login by the role assigned to him, but cannot reveal them.

4. **Symmetrical:** Regardless of other factors, the authorization of the role remains constant in order to comply with the standard.

   Example: The role „Regional Sales Manager“ has the same authorizations to access data regardless of its location.

Benefits With RBAC

In the following, we will discuss the advantages of the RBAC model in terms of security, efficiency and transparency.

Simple and Flexible Management

Collaboration in companies is becoming increasingly agile. Flexible project teams are emerging across departments to collaborate. Employees join at short notice, join other teams in parallel, and new temporary groups emerge. In addition, employee turnover has increased: Employees are changing jobs and employers faster and more frequently. This makes it all the more important to keep track of who is authorized to do what and when, and also to keep authorizations up to date so that former employees are effectively excluded and no longer have access to data.

RBAC enables companies to respond more flexibly to employee changes and turnover according to the Joiner, Mover Leaver (JML) process. Especially when employees join, change departments or leave the company, RBAC makes work much easier and more secure. Rights can be granted and revoked at any time via role memberships, be defined only temporarily from the outset, or access data can be provided with an expiration date, making RBAC highly adaptable and dynamic.

Role-Based Access Control also makes the time-consuming assignment of individual authorizations obsolete, as authorizations to roles can be predefined once and then rolled out to several people or withdrawn again in one go. If the roles are named in a way that is easy to understand, this also strengthens transparency and traceability on the user side.

Joiner: New Employees Join the Company

A new employee receives permissions to over 1,000 passwords via his role. With RBAC, these permissions of 1,000 passwords no longer have to be authorized individually, since only one role membership is processed. The authorizations are already predefined and only need to be adapted to current requirements.

Mover: Employees Change Department

The employee is simply removed from the old role and added to the new one. For a temporary transition phase – for example, when he is still training his successor – both roles can also be retained in parallel until the onboarding process is complete. This ensures a smooth and secure transition of credentials.

Leaver: Employees Leave the Company

If an employee leaves the company, they are only removed from the role and in one fell swoop no longer have permissions or access to any of their 1,000 passwords. This means that no unresolved user IDs remain. This applies not only to former employees, but also to collaboration with external parties or employees who go on parental leave or take a sabbatical.

Resolving the Trainee Effect

The trainee effect is the phenomenon whereby trainees pass through various departments in the company during their training and are given access rights for these departments that are not revoked after a change of department. As a result, employees who have completed their training have more and more access rights to company data – even if they have already left the company. This effect can occur not only with trainees, but in general when employees change – for example, when they are promote or move to a new branch.

Through temporary membership in a role and a general temporary limitation of authorizations that are not permanent, RBAC can ensure that the trainee effect is prevented and can even be dissolved.

Increased Safety and Efficiency

Assigning individual authorizations without RBAC is not only more time-consuming. It also means less control and overview of who has access to what. It also leaves room for errors and overauthorization. For example, security vulnerabilities can arise if individual permissions are not revoked or are retained longer than necessary. If users are granted too many rights, this can lead to errors that would not have occurred in the first place without the individually granted rights.

With a preconceived and predefined authorization concept, the company not only saves work, but is also on the safe side: Access rights are defined exclusively via role concept. Overauthorization of individual employees is thus avoided in accordance with the Principle of Least Privilege (PoLP), in order to also meet compliance requirements. Individual authorizations, which are error-prone and confusing, are also excluded in the best possible way.

In this way, RBAC helps to noticeably increase efficiency and security in IT as well as in the entire company. Changes are made automatically, rights no longer have to be applied for and assigned individually, and there is no longer any waiting time for approval. This not only makes the administration of access rights easier, but also, and above all, more error-resistant.

Distributed Responsibilities

In order to relieve users on the one hand and save resources on the other, responsibilities can be reallocated using the RBAC concept so that real processes from the working world can also be mapped digitally. The advantages of these distributed responsibilities are illustrated using practical examples.

Process Approval

According to the multiple eye principle, certain processes or decisions must be controlled by more than one person. In practice, this can mean in terms of segregation of duties (SOD) that money may only be counted in the presence of an additional person, for example, or that orders may not be approved by the same person who submitted them.

With RBAC, this process can be represented by requiring an additional role to approve access to credentials. In Password Safe, this is represented by the „multi-eye principle by seal“ feature, which can be used to specify exactly how many and which role(s) are required for approval and which role may request approval in the first place.

Delegation of Rights

A cashier should not check his own cash register. RBAC maps this principle in that the „administrator“ role can, for example, authorize other users to access data records, but without being able to view them themselves. This also relieves IT of the burden of ignorance in the event of a potential suspicious case.

Rights Transfer

In the event of illness or vacation, a substitute is named for the employee who can approve processes and access data on his behalf. The fact that several people can be members of a role in RBAC means that data can be accessed regardless of a person‘s absence, and further operations are not held up by a lack of rights. In addition, rights can only be granted temporarily for a certain period of time.

All Advantages at a Glance: IT and Corporate Structure Cleverly Combined

- granular access to data without increasing complexity
- better organization and overview of all access profiles with less administrative effort and error-proneness
- easier onboarding and offboarding of employees and department changes
- no business interruptions: Employees already have all necessary rights in advance
- less potential for attacks from inside and outside the company by excluding overauthorization
- more transparency and traceability for operation and audits

Implementation

In order to apply the RBAC authorization principle in the best possible way and to keep the effort as low as possible in the long term, security precautions must be taken in advance. Therefore, for the effective implementation of RBAC using Password Safe as an example, it is advised to proceed in the following three steps:

1. Actual Comparison: Requirements Assessment

First, a list of all access data (accounts, websites, applications, tools, programs) should be created. Then an overview is obtained of which persons have which access rights to them. In this way, an actual comparison is made of who currently has access to this access data in order to obtain an up-to-date status of the security situation.

Authorization Analysis

- What do individual employees have access to?
- How did these permissions come about?
- How are the permissions for an individual user structured?

2. Target Alignment: Create Roles and Organizational Units

Now the target comparison is made as to who in the company should have access to this access data. For this purpose, organizational units are defined that reflect the structure and hierarchy of the company like an organization chart. Now AD users and groups can be imported and authorized to access objects. The groups become roles. If such a directory service does not yet exist, the roles must be defined manually.

Roles can be thought globally or applied to specific organizational units. This preconceived and predefined authorization concept not only saves an enormous amount of time, but is also much more secure: Individual employees are not overauthorized because the authorization concept is based on the Principle of Least Knowledge.

To ensure that RBAC is able to correctly map all functions in an organization, all departments should be involved. For sustainable authorization management that will also last in the company in the future, roles that do not yet exist, such as trainees with restricted rights or audit officers with comprehensive reading rights, can be „preconceived“.

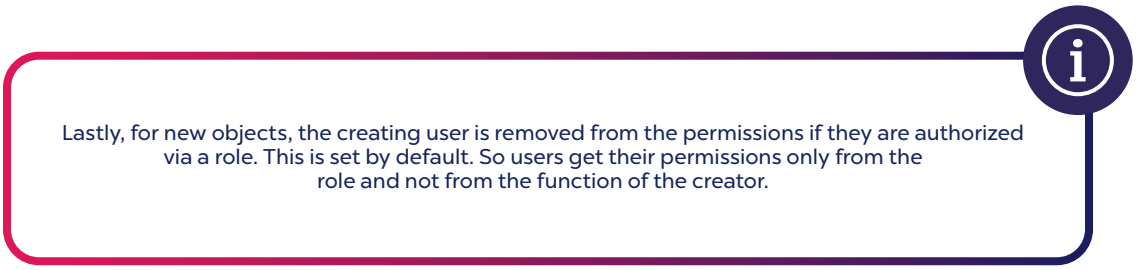
Create Authorizations

Finally, each user is assigned to at least one role according to his or her function. The assignment is made according to the least privilege principle. This involves determining which resources they need to access in order to perform their daily work.

1. Predefine Rights

Since it is very time-consuming to authorize each data record individually, it is advisable to predefine all rights in advance if possible. This involves defining which types of access rights are required – be it „read“, „write“, „move“ or even the „authorize“ right of access data.

The assignment of authorizations is made immensely easier by various automatic mechanisms. Authorizations should also be kept as narrow as possible in advance. A department head, for example, should only be granted the rights „read“ and „add“ to an organizational unit, but should not be able to add sub-organizational units or users.



Lastly, for new objects, the creating user is removed from the permissions if they are authorized via a role. This is set by default. So users get their permissions only from the role and not from the function of the creator.

2. Inherit Rights

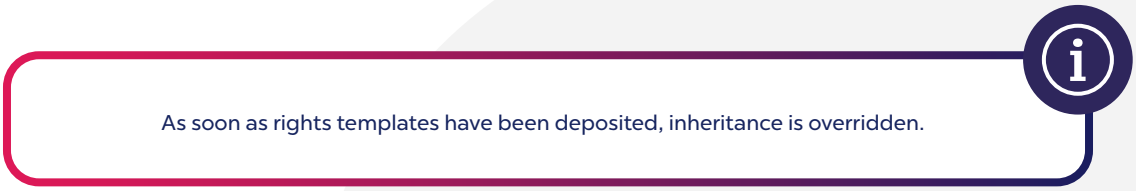
Rights sets can also be inherited from organizational structures: If a new record is created in an organizational unit, it also automatically receives the permissions defined in it. However, there is a risk here that an employee could also delete the organizational unit if one wanted to inherit the delete right. Therefore, the use of rights templates is more appropriate.

As long as no rights template has been defined, rights are inherited.

3. Use Rights Templates

To make working with RBAC efficient, it is advisable to use templates for assigning rights. A rights template maps the typical tasks of a role in an organizational unit using a preassembled authorization set. In this way, roles can also be conceptually authorized, for example, the role „trainee“ or „infrastructure management“. It is important that the rights template is only applied at the role level and not the user level.

Rights templates can also be set as default: This way, the correct rights template is automatically selected in advance when a new password is created in the respective organizational unit.



As soon as rights templates have been deposited, inheritance is overridden.

3. Security & Audits

To ensure that authorization management is always up to date and secure, and that each role has exactly the right authorizations for its function (and no more), regular security checks should be carried out. Especially when projects are completed, collaboration with employees or external parties ends, or new tools replace the previous ones, adjustments should be made. Afterwards, it is always important to comprehensively document the implemented RBAC policies as well as changes to them in order to work in a compliance-compliant manner.

Changes should never be made once for individual employees. If changes are required, the authorization for the entire role should be adjusted or a new role created if necessary.

Conclusion

RBAC enables companies to flexibly design access authorizations entirely according to their individual requirements and needs. Role-based access control can simplify various IT administration tasks, such as adding and removing users in the event of employee turnover or adjusting rights in the event of a change of position or department. In addition, purely from a security perspective, RBAC is ideal for keeping access as low as possible and avoiding superfluous authorizations.

This is the only way to effectively prevent possible security incidents and cyber attacks. And should an incident actually occur, it is possible to act quickly and prevent a major incident by immediately revoking access to data and, in the case of Password Safe, automatically exchanging passwords.

Authorization management in Password Safe is the key to secure management of passwords throughout the company. It means less effort, less error-proneness, more security and efficiency in IT and thus also for all other employees. Manual changes, error handling, waiting times or the individual application for rights: All of this is eliminated, making it the ideal concept for any company.

Author:
Kristina Kaya
Product
Marketing
Manager

MATESO
PASSWORD SAFE

MATESO is a leading German IT company, which has successfully established in the DACH region since the company was founded in 2006. The developed password security solution Password Safe is distributed internationally by its worldwide partner network. Well-known references testify to the technological and know-how advantage of the IT software.

Today the constantly growing enterprise registers over 10,000 corporate customers with several million users worldwide - including 21 Dax 40 companies.

Pioneer in Enterprise Password Management

Password Safe serves companies as a central digital safe for securing, managing and monitoring sensitive data such as passwords, documents and secrets.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE