NASSTAR

ROLE-BASED ACCESS CONTROL: A COMPLETE OVERVIEW

Role-based access control grants and restricts networks access within a specific company. Often seen in large organisations, this is a vital security component being rolled out across the board.

Rather than be susceptible to attacks or rely on higher level vulnerability protocols, role-based access control allows deeper control (and therefore deeper security) throughout your business.

IN THIS GUIDE, WE INTRODUCE YOU TO THE FOLLOWING COMPONENTS OF ROLE-BASED ACCESS CONTROL

WHAT IS ROLE-BASED ACCESS CONTROL?

Role-based access control is the process wherein you can grant different network access levels based on a user's "role".

Role is typically defined by job function or title which defines an authority level. For example, roles might be viewer, commenter, and editor, like in Google Docs.

Based on the role granted by the document owner, any person with access to this document will have different permissions:

\\ A viewer will only be able to read the document. No annotations can be added and no changes can be made.

\\ A commenter can leave notes outside of the document. Anyone with editor access can then make the suggested changes or take the necessary actions.

\\ An editor can make changes to the document as they have been granted full access.

An example more specific to network access is within a typical IT team. Let's split the team into four roles and see if you can guess which roles have access to the network...

IT Helpdesk
Fields tickets and provides first-line support to internal teams.

IT Manager
Handles escalations and raises suggested network changes.

Network Manager
Solely deals with planned and reactive networks changes.

IT Director
Responsible for the performance of the entire IT and networking operation.

If you guessed the Network Manager and IT Director would have access to the network then you are correct.

While the IT Helpdesk and IT Manager may have knowledge of your network, there is no need for them to have direct access. Without appropriate training and knowledge, granting these roles access could lead to incorrect changes or additions.

While it may only take one minute to change something on your network, the repercussions could take weeks or months to undo.

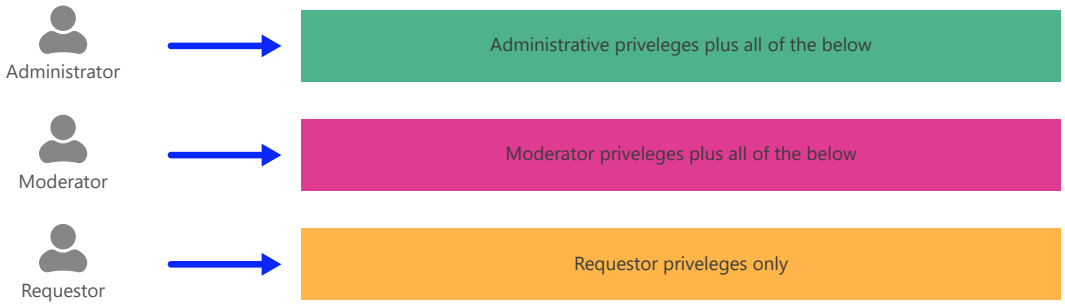
Limiting access to certain employees in the right role is crucial for IT departments to remain secure. Role-based access control is one of the most important threat defences an organisation can use.

WHAT IS HIERARCHICAL ROLE-BASED ACCESS CONTROL?

A common method of assigning controls when dealing with networks and IT systems is hierarchical role-based access control.

The underlying principle here is that roles can inherit permissions from other roles.

For example, a user with complete administration access (the administrator role) would also have privileges granted in all roles below this. So, the administrator can also be a moderator or a requestor.



WHAT IS THE BENEFIT OF ROLE-BASED ACCESS CONTROL?

The two high-level benefits of role-based access control are less risk of leaking sensitive data and more advanced control over who can access which information and applications on your network.

In turn, these both provide wider benefits to your organisation.

Improve operational efficiency
When the right people have the right access to network elements, places where changes can be made, or even documentation, your business is streamlined. There's less time spent granting and revoking access when it is pre-defined by role.

Adhere to and prepare for compliance standards
When you know users can only access the files and systems defined, it's easier to ready your business for accreditations and audits.

Reduction in costs
When access is restricted to certain users, you can reduce the amount of network bandwidth, memory and storage needed. There is also less over expenditure on unnecessary licenses.

WHY IS ROLE BASED ACCESS CONTROL IMPORTANT?

Role-based access control is important for optimum cybersecurity in your business. It's one thing creating an organisation-wide policy for user control, but defining permissions by role ensures *only the right people have access to the right systems at the right time.*

HOW DO YOU PLAN ROLE-BASED ACCESS CONTROL?

When planning role-based access control, it's first important to understand the following conventions

Acronym	Convention	Definition
S	Subject	A person or automated agent
R	Role	Job function or title which defines an authority level
P	Permissions	An approval of a mode of access to a resource
SE	Session	A mapping involving S, R and/or P
SA	Subject Assignment	The task or role assigned to a specific subject
PA	Permissions Assignment	The task or role of a specific permission
RH	Partially ordered Role Hierarchy	The process of assigning subjects multiple roles, roles multiple permissions, permissions multiple roles, operations multiple permissions, or permissions many operations

BEST PRACTICES FOR ROLE-BASED ACCESS CONTROL

The most important thing when implementing role-based access control is to start simple. Taking a big bang approach or starting with your most complex areas makes the first task the hardest.

When large efforts are required to take the first step, it can be demoralising for staff - and the end goal seems further away than ever.

The very first thing you must do is communicate why you're implementing RBAC. By now, you've got a great idea of what you can achieve. But you can also refer to the benefits section on page 6 too.

Start simple
With simplicity in mind, start by targeting roles in areas that are more familiar in your business. This removes the education section where you must get buy in and determine what access might be needed.

Focus on areas of high-turnover
In these areas, creating and deleting new user accounts (and associated access) is common. This means the access controls are likely predetermined or at least well known. This is a area you can chalk up as an easy win for RBAC.

Create RBAC champions
If you're going to change existing access for some users, it's important to get everyone on side. Educating users is one thing but having champions in each department is better.

Make sure you have someone from each team as your cheerleader for RBAC from day one.

Enforce least privilege
If you enforce least privilege, you ensure nobody gets unnecessary access. This sets you up for the safest approach from the very beginning.

Testing and verification
Each time a new role is created, conduct comprehensive testing before signing off that a role is complete. You may assign these as the sole responsibility of someone in your team. A staff member with experience in quality assurance or penetration is the perfect candidate

Schedule role-based access control reviews
When you create your role-based access control plan on day one, what's to say the requirements will be the same in 6, 12, or 18 months time?

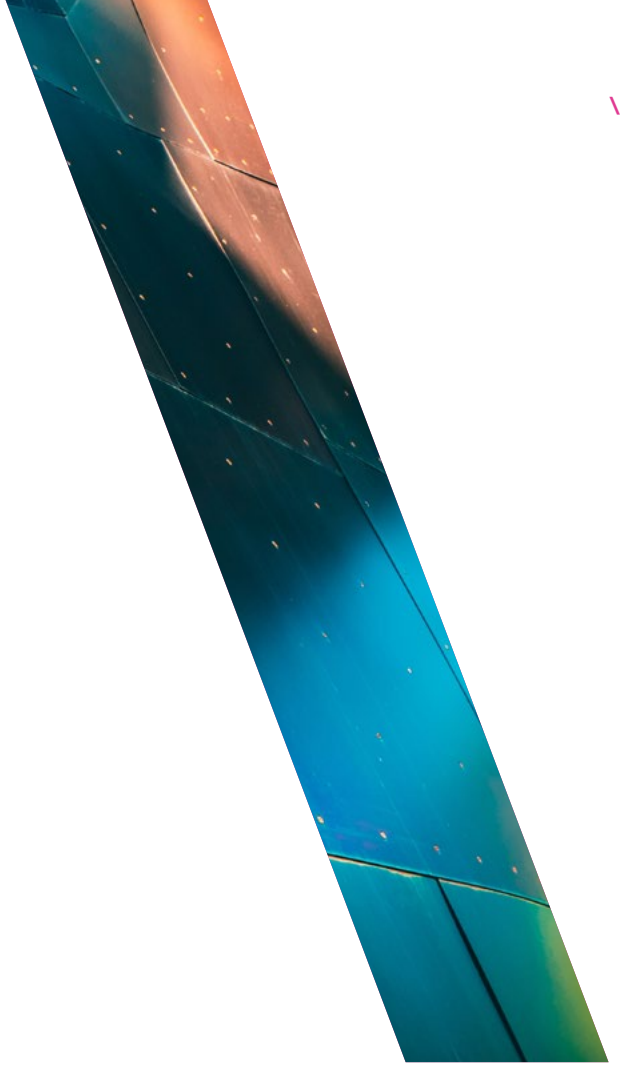
Plan for regular reviews of your RBAC implementation to ensure everyone has the right access. More importantly, you're checking people don't have the wrong access.

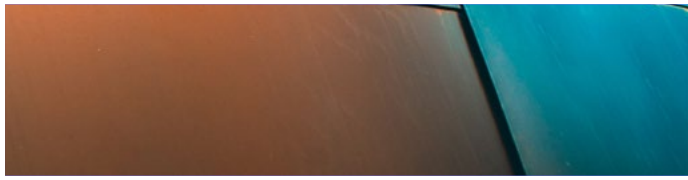
Or it may have become the case where RBAC is no longer suitable and you need to look at attribution-based access control (ABAC).

WHAT IS THE DIFFERENCE BETWEEN RBAC AND ABAC?

RBAC stands for role-based access control and ABAC stands for attribute-based access control. The table below highlights the key differences between the two.

RBAC	ABAC
Role-based access control.	Attribute based access control.
Can be roles based on security clearance, level in company, job type, etc.	Can be attributes per user, per environment, or per resource.
Include role types like teacher, non-teaching staff, student, IT staff, and IT management.	Includes attributes like name, country, organisation, ID number, role, security clearance, data creation date, owner, time of access and threat level.
Ideal for company-wide access like allowing email for all teachers or blocking Facebook for all students.	Ideal for detailed access like only allowing email for teachers when on campus, during working hours, and from an approved PC.
Often referred to as a high-level approach.	Often referred to as a “fine-grain” approach.





WHAT ARE THE THREE PRIMARY RULES FOR RBAC?

Wikipedia defines the three primary rules for RBAC as

1. **Role assignment**
   A subject can exercise a permission only if the subject has selected or been assigned a role.

2. **Role authorisation**
   A subject's active role must be authorised for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorised.

3. **Permission authorisation**
   A subject can exercise a permission only if the permission is authorised for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorised

NASSTAR

nasstar.com
+44 345 003 0000
enquiries@nasstar.com