Analysing Role-Based Permission Models

Prepare for Simpler Access Control & Claims-Based Authentication in AD & Beyond

A white paper for CIOs, IT Directors, Operations Directors & Compliance Managers

From Critical Action Limited

www.criticalaction.co.uk

0845 116 2364

Why Role-Based Permissions?

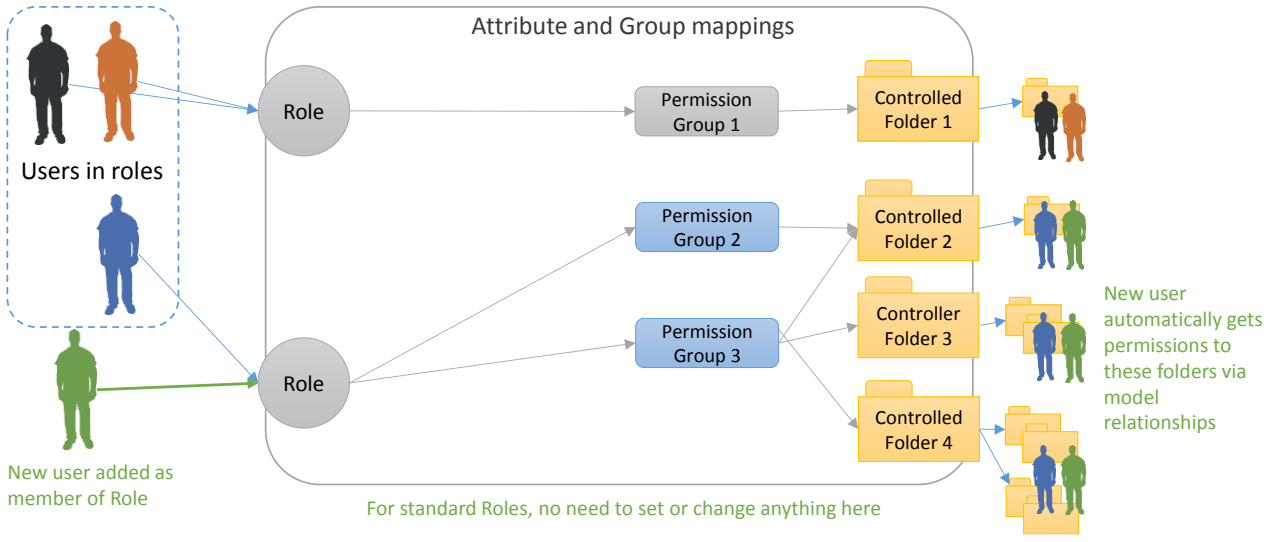
Claims-Based Authentication in Windows Server 2012 can simplify the adoption of Role Based permissions and security within Active Directory, but works best when the model is designed alongside business stakeholders. Role Based permissions can also be put in place without Claims in earlier Active Directories.

Although both Claims-Based Authentication and Active Directory have been around for many years, recent changes to Active Directory introduced in Windows Server 2012 mean that Claims are now consumed directly from AD (as opposed to security groups and LDAP queries). Much of this is being driven by increased use of cloud services in corporate and enterprise environments, and the security, compliance and clarity needs this brings. Claims-Based Authentication brings the promise of being able to manage users' permissions based on attributes already in Active Directory as well as using Security Groups, leading to the potential for clearer AD designs.

Role-based designs in general do two important things – speed up day-to day granting and revoking of permissions, and make the design and operation of the security access model more transparent.

How Roles Work in Active Directory

In operation, a user is given membership of the correct Role security group. In turn, this Role security group is mapped to a number of other Permission groups which serve to grant access to defined resources (folders, files, machines, etc.). When someone changes job in the business, the IT admin changes the user's Role security group membership. Through the mappings between Roles and Permissions the changes to resource permissions result. Temporary cover for roles can be dealt with through adding membership to a second Role for the period of cover needed. Crucially, removing a user from a Role group revokes related permissions.



Key Requirements for Design

When designing such a hybrid Claims-Based and/or Security Groups role-based model, what is very important is creating a technical solution that reflects how the Business actually uses, shares and protects its information assets – files, folders, and so on.

This means understanding what lies behind the job titles, and digging into who works with whom, why, on what, when and where. It also means understanding what layers of access or security are used (or needed) around documents, and what impacts on when and who can get access. For example, does a user get access to a folder when they are above a level of seniority, when they work on a given project, or when the information itself passes some sort of gateway status? Control needs to be exercised over both the mappings between Roles and Permissions and also the application of Permission groups to resources like files and folders. This can be approached in a number of ways, but the idea is to protect the integrity of the mapping model, aiding with auditing, reporting and management of security and access.

One of the biggest challenges typically seen in a mature AD implementation is a lack of revocation of historic rights when they are no longer needed. New groups tend to be created quickly to grant permissions to new folders or resources; but often, groups or group memberships are not removed or disabled when permission is no longer required. Sometimes, this doesn't matter, but depending on the compliance or commercial nature of the information, this might well represent a risk or threat vector to your business.

Building the Roles-Groups-Permissions Model

To help infrastructure teams to move towards role-based access (whether Claims-Based or purely Security Group based design prior to Server 2012), it is important to start designing from a clear, consistent and extensible logical model of the business, which shows the current state of access needed, but which also allows for the inevitable flex and change that happens over time.

We have worked with businesses of various sizes and complexities to explore business needs around access control, where the common thread is protection of valuable intellectual property.

The approach we use brings both business and IT stakeholders together to map out the high-level catalogue and flow of information classes. We look for the patterns of access that show when different roles need to collaborate easily, with a minimum of restriction. We look for the limits to collaboration so that information is protected, and we look for the information that is "mastered" in one area, but shared with controlled groups of other roles based on functional need or expert input.

Ideally, models should self-describe, so that it is more likely that correct permissions will be applied to new resourced, and that new or changed roles will be mapped to sensible permission groups, based on the business function of the role. This is the approach we take to naming the groups in a structured way, as a result of the analysis of role and information sharing/protection data we gather.

Implementing Role Based Access in Active Directory

As a result of the engagement model we use, technical design authorities and infrastructure teams can design their Active Directory implementations on the bases of a number of defined roles, a set of permissions groups, and logical mappings between roles & permissions, and permissions & groups. Projects can also be defined to migrate folders and documents to the new permissions model – it is usually preferable to create a "new world" into which data is migrated, as that means historical permissions don't need to be unpicked. Care (or

an alternative approach) may be needed though if there are interlinked documents, or hard-coded or absolute paths and so on are used in files.

The technical design defines AD OUs, Policies and Security Groups, and if Claims-Based Authentication is being used, which attributes will be used to provide/consume claims, and what values map to what Access Control List permission entries for folders. The attributes could be things like the user's (or computer's) location, department, address, account expiry date and so on.

The model tends to be fairly static – essentially only changing when job roles change what information they work with. The people in jobs can change frequently however, with a minimum impact on IT operations, since the changes of security group membership are restricted only to the role groups, not the more numerous permission groups – the permission groups' membership of role groups sees to that.

Getting Started With Role-Based Permissions

If you:

- Work with Active Directory in your business
- Are preparing to migrate to Windows Server 2012
- Are preparing for or using software or cloud services that use a role-based model
- Want to save time managing changes of job role and resource access
- Want improved transparency and auditability over "who can access what, and why?" or
- Can see the benefit of investing in analysing requirements to create your role-based model

Then please get in touch to talk through what we could do for you and your technical team.

Our analysis services start with one day workshops and run through to multi-month, managed programmes of stakeholder identification, interview and analysis. We often work alongside technical staff too, feeding into technical design and implementation. This means we can help you from the early days of brainstorming approaches for small proofs of concept, through to full model designs and specifications for thousands of users.

w: www.criticalaction.co.uk
e: information@criticalaction.co.uk
t: 0845 116 2364

About Critical Action Limited

Critical Action was founded to help organisations capitalise on ideas, opinions, questions, information and capabilities that they usually already have, but need to organise, nurture & act on to turn them into real results.

We aim to achieve a lot of discussion, debate, exploration and if possible decision, when people are face to face, whether one-to-one or in groups. We then assemble the information and conclusions from this "people time" into real deliverable documents which have a purpose to them.

Our goal is for you to be able to trace a route through the raw data in people's heads, and the first tentative debates, right through to considered plans of actions, and visible results that make a difference; to make your organisation more successful, more differentiated, and better for both customers and staff.

We work with CIOs, IT Directors, Operations Directors and similar roles in small, medium and large organisations where information and intellectual property are at the heart of operations and business value.