Realtime publishers

The Essentials Series: Enterprise Identity and Access Management

Administration Challenges

sponsored by

QUEST SOFTWARE®

by Richard Siddaway

Copyright Statement

Administration Challenges

The administration of identity and access can be a significant effort in an enterprise. The challenge is to reduce the administrator effort and ensure that an organization remains secure and compliant. The first major challenge that many organizations face is that of administering identity in a heterogeneous environment.

Heterogeneous Environments

Heterogeneous environments require multiple directories and multiple, often disparate, identities for any one individual to achieve authentication and authorization. The picture is further complicated by the mixture of protocols required for authentication. It is also possible that for non-Windows systems the authentication data is held locally across a number of systems with no guarantee that the same userid is used to represent the same individual across systems.

Applications can require authentication to control access. Ideally, this is handled through Active Directory (AD) but this is not the case for many applications. Some applications—such as SQL Server, SAP, Oracle, Siebel, and so on—have their own authentication and authorization mechanisms that can be used instead of or in combination with AD-based authentication.

Multiple Directories

The heterogeneity of computing environments leads to multiple directories being present within the infrastructure. Many users will have identities defined in multiple directories. This situation can generate a number of issues:

- Extra, repetitive administrative effort for maintaining identity across multiple directories
- Uncertainty about whether passwords can be synchronized between directories and, if so, the way to do so
- Extra costs for acquisition and operations
- Confusion about which directory is regarded as holding the master data
- Mistakes in granting access permissions due to confusion about identity, which lead to inappropriate access to confidential data

Adoption of AD as the single source for authentication and authorization will resolve or remove these issues.

Account Management

The management of user accounts in AD is fundamental to an organization's security. The life cycle for accounts centers on their creation and deletion, together with the provisioning of access rights.

Provisioning

User provisioning is often performed manually as part of the Help desk function. There is no guarantee that two administrators will create user accounts in exactly the same way. This lack of consistency creates additional administrative effort and can lead to security loopholes. A manual process makes it more difficult to ensure that the user is made a member of the correct groups, leading to problems with access management.

In larger organizations, the number of accounts that need to be created means that automation has to be employed. The ultimate case is a large university where thousands of new users have to be created—and provisioned with mailboxes and access rights—at the beginning of the academic year.

Automation of user account creation enables consistency and the application of rules to ensure that users are given the correct authorization rights. Organizations of all sizes can benefit from automating the process, preferably based on an information feed from the HR department.

AD simplifies user provisioning in that a user has a single account that can be used across all the machines within the domain. In an environment that does not use AD, this level of centralization cannot be achieved. A user account must be created on each individual machine. Automation becomes more difficult, if not impossible, especially in the case of multiple types of non-Windows systems. If multiple administrators, or groups of administrators, are involved, the situation becomes even more complicated as different naming standards may evolve and there is no guarantee that a given userid on two machines actually refers to the same individual.

A user account may be modified during its lifetime. The final act in the life cycle deals with how accounts are removed when they are no longer required.

De-Provisioning

In many organizations, user accounts are not removed. This leaves a growing burden in AD and can also be responsible for security breaches. Imagine the scenario in which an administrator has remote access and then leaves. If that account is still active, that administrator could access confidential data or damage the systems.

At the very least, the accounts should be disabled. One common solution is to move the accounts to a holding organizational unit (OU) and disable the account. If it is determined that account is no longer required, after say 1 month, then it can be deleted. These tasks should be automated based on a feed from the HR department.

Delegation

Separation of duties is a sound security principle. This applies to identity and access management. How do you want your AD to be managed and by whom?

Who and What

There are some administrative tasks within AD that should not be delegated (for example, schema or topology management). It is common to delegate the administration of users, and related computers especially in a distributed environment that spans multiple, disparate, time zones. The rights to manage all user accounts in a given OU can be easily delegated to one or more administrators.

These administrators do not need to be as skilled as your main domain administrators but it is essential that they are trustworthy. The ability to manage, or even create, user accounts and access rights could have serious effects if misused.

How

Having decided what tasks will be delegated and who will perform the work, the next determination is how the delegation will be performed. It is possible to delegate these permissions manually, but this is not easy to administer or to keep track of who has the rights to administer which part of the directory.

The preferred way is to utilize a tool that integrates with AD and can manage the delegation of these administrative roles. Delegation should be treated as role-based access with groups created specifically to manage these permissions. The tool should also provide a reporting function so that it is possible to easily determine the delegated permissions within the directory.

Revoking

One point that is often overlooked is the revoking of rights when they are no longer required. Administrators can change roles, and if they no longer require the rights to manage a specific portion of the directory, their permissions to do so should be revoked. This can be difficult to achieve if the rights have been assigned manually.

The type of management tool discussed in the previous section should be capable of easily revoking permissions. If the rights are based on group membership, removing the administrator from the group will revoke the permissions.

Non-AD

In the non-AD world, is it possible to delegate administrative permissions in this way? The usual answer is no, it is not possible, at least not natively. This leads to the situation where highly skilled, and expensive, administrators are performing tasks that would be better suited to more junior staff which prevents them from applying their skills to the full benefit of the organization.

Password Management

Managing passwords can contribute significantly to administrative costs. A figure of $25 per password reset is commonly quoted. You need to consider password policies and how you will manage those passwords.

Multiple Password Policies

Windows Server 2008 is the first version that allows administrators to create multiple password policies in an AD domain. Prior to this, you required multiple domains to accommodate multiple password policies, which caused a rise in cost of acquisition and operation. Organizations will need to use a third-party tool to manage the multiple password policies, as the only native tool available is ADSIEdit!

Use this functionality to set stronger passwords for privileged accounts and service accounts. With a very long password, considered passphrases instead of passwords, the need to change passwords is radically diminished. Ensure that the password policies are designed to meet your needs. One situation to avoid is the "I can't remember long passwords so create a policy for me with a very short password that never changes!!" That situation will cause problems.

Password Reset

In many organizations, password reset is performed by the Help desk. How many organizations will ratify the identity of the person asking for a password reset? One particular financial services company requires a fax from your manager before the Help desk would reset the password.

Resetting a password is not a technically onerous job. The logical place for this to occur seems to be at the Help desk. However, there are other, more beneficial, things they could be doing. The time for the Help desk to perform these tasks could be found by adopting an alternate strategy for reset. Either delegate the job into the business or adopt a self-service approach.

Allowing password resets to be performed locally has a number of benefits including a quicker response time and the requestor is immediately identified as they are in the same business unit as the person performing the reset. This may not work as well for an organization with a large proportion of mobile users. In this case, think about a self-service portal for password reset. Based on the answers to pre-determined questions, the users can trigger a password reset themselves. This approach has been shown to pay for itself very quickly.

Non-AD Issues

The preceding discussion assumed an AD environment. What about the myriad non-Windows systems and applications with their unique and often disparate password policies? Redundancy of effort and the potential for security breaches rise exponentially as the diversity of the heterogeneous environment increases.

The problem becomes even worse when passwords are considered:

- Is the same password used on all systems?
- Do the same password policies apply on all systems?
- Did the user change all passwords when they expired?

In most situations, the answer to all these questions is no. In this situation, it is inevitable that the number of calls to the Help desk for assistance with password-related problems will rapidly increase—or even worse, that these issues must be handled by highly paid administrators at the OS or application level. At $25 a problem, that can very quickly become a significant cost. In addition, the password reset capability cannot be delegated, so the highly paid administrators are performing these tasks rather than applying their skills more productively.

Fortunately, as has been discussed earlier, the simple process of consolidating identity, authentication, and authorization in AD can bring significant positive impact on the cost of password management in the heterogeneous environment. Fewer identities and fewer directories directly correlate to fewer password resets and more consistent and secure password policy.

Group Management

A well-designed authorization strategy is based on the use of groups in AD. Managing the groups needs to be planned at the same time as the structure of the groups.

Who Is in the Group?

Who needs to be in a particular group? In some instances, this is a business decision, so there is an argument that the business should manage membership of these groups, or at least approve membership. Beware of nested groups. Tracing the membership of a group through several layers is not an easy task with the native tools. Obtain a tool to do so or develop scripts to perform this task.

What Groups Am I In?

The converse question is “How do I know what groups a user is in”? This again can mean traversing nested groups.

Technology, People, and Processes

The challenges of identity and access management can be summed up as people, processes, and technology. Correctly trained people implementing well-designed and tested processes using the types of technology outlined earlier will enable your organization to overcome the challenges of identity and access management.