NetIQ

Active Directory Administration:

Managing Active Directory for Better Data Integrity and Security

Don't Let Your Admin Solution Become a Bigger Problem

As both a data store for confidential information and a gateway to other critical IT systems, Microsoft Active Directory (AD) has become the *de facto* book of record for identities in today's enterprises. This is a convenient solution, as AD is included in most versions of Microsoft Windows Server. But it also creates potential risk because users with administrative access to AD (commonly known as "privileged users") can potentially access the accounts of every user and service connected to that directory. And that creates one of the biggest security challenges that many of today's enterprises are only just beginning to realize: too many people have privileged access to AD.

The risks associated with this problem cannot be understated. The Ponemon Institute report, *Privileged User Abuse & Insider Threat*, reveals that 45% of respondents believe it is likely that social engineers target privileged users to obtain their access rights. Despite this, 49% of respondents have no policy for assigning privileged user access. In fact, only 35% of respondents say company administrative rights or privileged access rights are assigned through well-defined policies that are centrally controlled by corporate IT. This "inside out" activity can bypass many security protocols and precautions because security software typically monitors only the perimeter for unauthorized access, not internal access.

So why has this happened? It's really quite simple. As organizations reach a certain size (typically 1,000+ employees) or have a certain amount of complexity to their environment,

Social engineering is an intrusion that involves tricking people into giving up confidential information in order to gain privileged access or insights.

they need a better way to effectively manage all the identities, servers, desktops, storage space, mailboxes, printers, groups and distribution lists that reside within their infrastructure. What starts as a manual process quickly becomes very time-consuming—trying to manage all these identities and grant the appropriate authority to each one. As a result, people who need access to specific *resources* often get *broad* access because it is expedient and easy.

Flash Point Paper

Why Should a Directory Administrator Be Part of My Company's IT Solutions?

- *AD is your organization's primary identity store or authoritative book of records*
- *Too many people have full rights or are domain administrators in AD*
- *You need to reduce manual or repetitive tasks related to AD or Microsoft Exchange Server administration*
- *You need technical or business-owner approvals during the management of access rights granted through AD*
- *Users require self-service capabilities in AD*
- *Help desk personnel need just enough rights in AD to resolve problems*
- *You need to show full audit trails of all administrative activity in AD*

With an identity management solution at the heart, an active directory administration solution works in tandem to manage day-to-day delegation of privileges.

When the company realizes that it needs a better way to effectively manage all of the identities in its organization, it often puts in an identity management solution. With this type of solution, administrators can automate the task of provisioning access to enterprise resources and assets. This eliminates the risk of human error and provides a layer of security for user identities. But now comes the ultimate irony: the identity data being managed by the identity management solution is actually stored in AD. So unless administrators have already reduced the number of privileged users, adding an identity management solution is like locking the door to the henhouse—with the fox inside.

There has to be a better way.

The Smart Choice: Adding an Active Directory Administration Solution

The use of AD is widespread so you'd think it would be easier to control visibility and administrative rights. But because so many people at different levels in an organization need AD rights to effectively do their jobs, many organizations struggle with effectively delegating appropriate authority. Some simply overlook the risks of escalated AD administration and assume their identity management solution will take care of the problem. This is rarely the case.

There is an effective action to consider: adding an AD administration solution. While having an identity management solution is ideal for most large and highly regulated companies, there

Shortcomings of Microsoft Native Tools:

While Microsoft does provide ways to delegate AD administrative authority, its native AD administration tools are lacking in several key areas:

1. Secure delegation of entitlements. Native controls are not flexible, do not scale well and are difficult to change. Assistant administrators see everything in AD, regardless of whether they can actually manage that information.
2. Reporting of delegated authority. Once you close the delegation wizard, it requires significant work to identify who has access to what.
3. Content control. Because there is no content and context policy enforcement through native tools, you risk directory pollution (invalid, incorrect or improperly formatted information being entered into your directory).
4. Web-based administration. Microsoft does not provide a web-friendly way to do AD administration, which means administrators are forced to use the AD Users and Computers (ADUC) interface.
5. Restoration of deleted information. You can only recover deleted AD objects with significant effort.
6. Automation. There is no way to automate repetitive, manual AD administration tasks, which means the chances of human error dramatically increase.

are several advantages to adding directory administration for AD to an identity-managed environment.

There are several options to consider, including using native tools, but you must choose wisely.

Are Native Tools the Answer?

While Microsoft does provide ways to delegate AD administrative authority, its native AD administration tools fall short in many areas (see sidebar). By adding the combination of an identity management and a dedicated AD administration solution, you should be able to address the shortcomings of these native tools and:

- Easily and securely delegate administrative authority.
- Provide easy auditing of administrative authority and actions.
- Enforce account policies.
- Automate highly manual and highly repetitive administration tasks.

The Advantages of Having Both AD Administration and Identity Management Solutions

Combining a dedicated AD administration solution with an identity management solution has several distinct advantages. First, it reduces your overall security risk by allowing you to easily delegate "just enough" administrative authority in AD without making you manage such fine-grained delegation through your identity management solution. Second, it often simplifies identity management deployments by showing administrators only what they have rights to manage in AD. Adding the AD administration solution also means that there is a single connection point for AD across multiple domains.

Often, the result is that IT work can be more evenly distributed to local or junior administrators because the department can delegate AD authority with fine-grained precision. Identity management specialists can concentrate on your organization's overall identity framework while various individuals perform the day-to-day administration of AD in a secure and standardized way. In addition, adding an AD administration solution can enhance your overall auditing and reporting capabilities because it carefully and securely logs all administrative activity in AD. Running reports and proving compliance regarding all administrative activity done in AD becomes that much easier.

Attributes of a Top-Notch Active Directory Administration Solution

Not all tools that are designed to manage AD administrator rights are created equal. Finding the one that is right for your organization can be complicated, but there are a few things that you should look for. It should enable you to delegate targeted administrative privileges without increasing the burden on your organization's busy IT staff. It should also allow you to capture and store all administrative activity, so you have the comprehensive audit trail needed to produce reports that satisfy management and auditors. Here are a few specific things to look for in your solution:

- **Granular access controls.** Does it allow you to grant precise, tailored access privileges and reduce the number of users with full administrative privileges?
- **Centralized activity logs and reports.** Can it help achieve and maintain regulatory compliance with mandates such as PCI DSS, FISMA, HIPAA and NERC CIP through precise privilege control coupled with centralized logging of all administrative actions and flexible, comprehensive reporting?
- **Controlled self-service tasks.** Does it enable IT administrators to increase efficiency by transferring common user and mailbox management functions to the help desk or, via self-service functionality, to the end user?

Automating Systems Can Keep Out Problems:

1. Automated provisioning/ de-provisioning/re-provisioning of user access rights and privileges
2. Centralized HR source for creation, deletion or updating of rights

This is especially helpful when large groups of users who require privileged access (such as contractors or temporary employees) leave the workforce. Don't leave the door open for them!

- **Automation and secure privilege delegation.** Can it reduce administration costs and enforce policies by automating repetitive and complex tasks and providing use-controlled delegation of common administrative duties?
- **Improved data integrity.** Will it reduce data pollution by consistently enforcing business policies and controlling the format and amount of data entered into your AD and Exchange Server objects?

Combining an identity management and AD administration solution to delegate your AD administration can provide tangible benefits to your organization without increasing complexity or risking security. NetIQ has a range of options that can help. Our Identity-Powered Solutions use identity information intelligently to make your business more responsive and secure. They leverage your existing resources and infrastructure so you don't have to start from scratch. And they deliver sustained business value while driving lower TCO. Specific products that can help with delegating AD administration include:

www.netiq.com

- **NetIQ® Directory and Resource Administrator™.** (**www.netiq.com/products/directory-resource-administrator/**) Improve security, demonstrate compliance and streamline the administration of AD and Exchange Server.
- **NetIQ Group Policy Administrator™.** (**www.netiq.com/products/group-policy-administrator/**) Control and simplify the administration of Microsoft Group Policy.
- **NetIQ Identity Manager.** (**www.netiq.com/products/identity-manager/advanced/**) A complete, yet affordable solution to control who has access to what across your enterprise—both inside the firewall and into the cloud.

Today's hybrid IT infrastructures are creating new challenges for business and IT leaders. IT services are now being delivered across an increasingly fragmented combination of physical, virtual and cloud environments. These services are being accessed from an expanding number of locations, on a growing variety of devices. And the technology environment is changing faster than ever. In the face of this combination of forces, organizations like yours often struggle to balance consumerized user expectations with the need to reduce organizational risk. At the same time, organizations must embrace the business value that can be achieved by leveraging innovations like cloud computing and mobile technologies.

So how do you keep access to IT services simple while preventing unauthorized or risky user activity—all in the context of where and how users are connecting? That's where NetIQ comes in. Our broad portfolio of Identity-Powered Access and Security solutions, combined with our data center management solutions, help you manage the complexity of hybrid environments to ensure that the right people have the right level of access to the IT services they need, whenever they need them. With NetIQ, you can incorporate new technologies and services more securely, faster and with less effort. And our solutions help you understand what is going on in your environment—in real time—so you can mitigate risk while still taking advantage of opportunities.

Quite simply, this means that you can secure, manage and measure what matters most to your organization. Even more important, this new level of clarity will create new opportunities—and competitive advantage—by enabling you to understand, maintain and make sense of the shifting relationships between individuals, devices, behaviors and technology services. That's how you can drive the successful business outcomes that will deliver ongoing value to your organization.

About NetIQ

We are a global enterprise software company that meets the demands of today's IT environments with a wide range of proven solutions for identity and access management, security and data center management.

Learn what you need to do by visiting: **www.netiq.com**

Worldwide Headquarters
515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
+1 713 548 1700
888 323 6768
info@netiq.com
www.netiq.com
www.netiq.com/communities/

For a complete list of our offices
in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit: www.netiq.com/contacts