Top 5 Avoidable Active Directory Administration Mistakes

Abstract

Microsoft's Active Directory (AD) is, and will continue to be for the foreseeable future, the directory of choice for the majority of organizations around the world. Despite the disruption that cloud and mobile technologies have induced, AD remains the most popular user authentication and authorization system available today. And while AD has matured since its introduction, administration mistakes persist primarily due to administrator error. Once made, these errors often result in costly problems such as security breaches, compliance failures or costly fines. It is typically only after a material event or failure that it becomes clear that theses mistakes were most likely avoidable. This white paper will throw a spotlight on five avoidable Active Directory Administrative mistakes so organizations may address these issues before they become a problem.

5 Account deactivation performed improperly

When a user leaves the organization, temporarily or permanently, the access granted by the user's AD account should be revoked. By properly deactivating the user account, the account no longer represents a target for bad-guys or auditors. Many organizations believe that simply disabling a user account makes the account secure – this however, does not leave the account in a state that makes it impervious to exploitation. And those organizations that are only disabling accounts to secure them are leaving accounts one check-box away from causing costly security & compliance failures

To properly secure unused accounts up to nine separate properties and settings should be evaluated and potentially updated. These attributes include cleanup of group membership, updating attributes and possibly changing the object's location. It may appear that deleting a user accounts is an alternative to disabling, but it is not. Deleting users is unacceptable because the account is no longer available when needed for audit or security reviews.

Organizations should look for an account suspension solution that not only allows AD admins to suspend accounts manually, but also on a schedule. When a user's departure date is known in advance, scheduling deactivation of the account will ensure the account is not overlooked when the AD Admin gets busy.

User Deprovisioning Considerations

- Native "Disable" provides only one of the nine critical steps needed to secure accounts; leaving accounts one check-box away from causing costly security & compliance failures
  - SOX, HIPPA, PCI require software controls to revoke access when associates leave the organization
  - Auditors demand demonstrable controls so accounts must be retained for a period of time
- If synchronized to cloud – cloud accounts often continue to consume licenses, incurring additional costs and creating additional security and compliance considerations.
- Automated solutions should enforce best practices and support scheduled, temporary, and permanent user deactivations.

4 Inactive accounts are not remediated

In today's networked environments, Inactive User Accounts are a favorite target of bad guys, compliance auditors, and security staff because. Inactive accounts pose a threat that can compromise business systems, data, or lower the reputation of the business with public breaches. Compliance requirements like SOX 404, PCI, SSAE 16 and HIPPA require software controls be in place to identify and securely deactivate inactive accounts so they are not misused.

Many organizations have a dangerous communications disconnect between the Human Resources Department (HR) and the AD Administrative team. This disconnect leads to the proliferation of inactive accounts. When people leave the organizations HR should, but does not notify the AD team and the departing user's account is not deactivated. These inactive accounts cause two problems. First, they are a targets for misuse and second they slow down day-to-day administration because they are no more than clutter in searches, reports and on-screen.

Every organization should have an automated remediation process in place - to detect and deactivate accounts that are no longer in use. This process should follow proper user account deactivation best practices (as mentioned in number 5 above) and should, at a minimum, be scheduled to execute and report results one time each day.

Inactive Account Considerations

- SOX 404, PCI, SSAE 16 and HIPPA require controls to properly revoke departing user access
- Lack of communication is a leading reason for failing to deactivate accounts
- Constant attention is required to find and remediate inactive accounts (automation is suggested)
- It is not simple to identify inactive accounts, multiple account aspects must be considered
- Inactive accounts put Security, Compliance & Efficiency objectives in jeopardy

3 Active Directory Data left inaccurate

Organizations primarily use AD for authenticating user sign-ons, but others use it for much more. Each user account in AD not only stores a sign-on name and password, but AD can also store organization and geographical attributes of the user. When this data is properly maintained and kept current, the information can be used by applications and administrators as a way of storing information about the organization that can be used in various ways. Microsoft Exchange and Office 365 use AD details for a centralized corporate directory allowing users to view colleagues departments, e-mail addresses, phone numbers or mailing addresses.

"I tried to call you, but your phone number was wrong in the directory…"

"Everyone in LA received the e-mail, why didn't you?"

"An audit found that IT did not apply the retention policy to everyone in Finance."

Two new technologies, Dynamic Access Control and Claim-based Authorization, were made available to customers in Windows Server 2012. When implemented, these technologies can consider a user's AD Data such as country, department or other attributes to determine if the user should be granted access to a particular resource. These technologies enable scenarios such as separation of duty and ethical walls that before were not possible without expensive and complex third party systems. Because both of these technologies rely on AD data, the data must be kept accurate and up-to-date.

The approach for keeping AD data accurate will vary for different organizations. Ideally organizations will setup an automated update from the most likely source; the HR Department. If automated, frequent updates can be made with almost no effort. Another, less efficient path, to AD data validation is to send a list of users and their details to managers and ask the managers to send back corrections.

Active Directory Data Considerations

- Manual updates of employee information (phone, jobs, office locations etc…) will fall behind
- Stale user data impacts both IT and business operations, causing costly productivity delays
- Stale user data prevents automatic assignment of access, retention, and archive policies increasing IT workload and costly errors
- No native solution and Identity Managers or scripting are complex and costly

2 User Access allowed to become out-of-date

Many AD Administrators recognize too late that the number of groups they manage equals or exceeds the number of user accounts they manage. The result is administrators struggling to keep group memberships accurate using manual, time consuming and error prone processes. Because AD groups are the primary mechanism that user access to resources is granted or denied, groups and their out-of-date memberships will eventually lead to costly data leaks, security breaches and outright compliance failures.

When organizations are subject to SOX, HIPPA or PCI requirements, groups that are used to control access to finance, patient, or credit card information become a favorite target of auditors and compliance officers. Compliance regulations were created to protect the public from organizations that may falsify their results or otherwise act in an irresponsible manner. When the wrong user granted access to sensitive information by being included in the wrong group, the consequences can be drastic. Many compliance failures require that organization's official compliance reports may have to be publicly re-stated, IT management may have to be replaced and costly fines may be leveled against by the government.

The security and compliance implications, combined with a cost from $5 to $15 per manual membership change - often justifies investing in automating and cleaning-up group memberships. If the organizational data in Active Directory accurate (See #3 above), then AD data can be used to automate group memberships.

Group Management Considerations

- Group Management is error prone and time consuming leaving groups inaccurate
- Stale data make Dynamic Access Rules worthless
- Often there are more Groups than actual users
- The organization's critical information is put at risk by costly incorrect or missing access grants
- Security, Compliance & Efficiency objectives are in jeopardy
- Automation solution must support inclusion and exclusion rule for granular membership

1 Costly and error prone manual account provisioning process

Account provisioning is the combined process of account creation and the subsequent assignment of settings, policies and resources needed for the job held by the individual that will use the account. While account creation may be a simple task, account provisioning can be complex involving many steps and decisions made along the way. And like all humans, administrators make mistakes that often become evident during account provisioning.

Possibly as important as account provisioning are account updates and account deprovisioning. When a user changes roles or separates from the organization, the user's account must be changed accordingly. So there are actually three separate processes that should be examined in detail when examining account provisioning.

Because there is no out-of-the-box automated accounts provisioning, provisioning remains costly both in terms of time and money. An efficient way of reducing these costs is to introduce automated provisioning. That is not to say that because manual account provisioning is costly every organization should jump to automate provisioning. For example, a custom car maker can build a single car by hand and spend as much time and money to produce that single unique car. A car manufacture, intent on producing many cars, will create an assembly line to produces many similar cars quickly at a much lower cost.

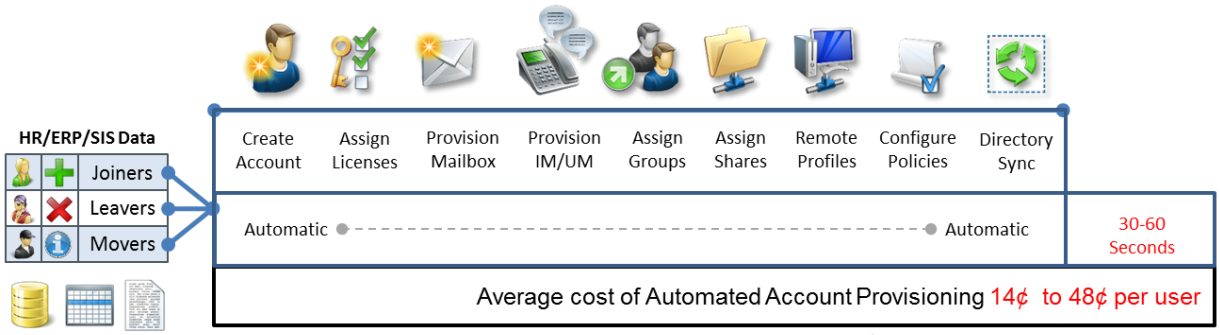
Manual Account Provisioning

Create Account	Assign Licenses	Provision Mailbox	Provision IM/UM	Assign Groups	Assign Shares	Remote Profiles	Enforce Policies	Directory Sync	
2 to 5 minutes	3-10 minute	4-7 minute	2 minute	3-15 minute	3 minute	3 minute	5-15 minute	30-60 minute	25 to 96 minutes
Average cost of Manual Account Provisioning $12 to $46 per user									

*Average Admin Salary from payscale.com

Three factors can be helpful in making the decision to automate, 1) The number of accounts added, removed and updated 2) The workload of IT staff and the size of the organization and 3) the organizations tolerance for cost and delays. The chart above was designed to help illustrate the costs associated with manual provisioning. The chart shows that manual provisioning cost can range widely between $12 and $46 and the associated time delays range between 25 minutes and 96 minutes. While it is not possible to show all of the tasks administrators will need to accomplish, those shown are common across a variety of organizations.

For comparison, the chart below illustrates the cost reduction and time savings of automated account provisioning. An additional benefit to automation is the fact that the chart now covers account provisioning, updates and deprovisioning with no additional costs. It is realistic that automated account provisioning will cost less than $1 per user added, modified or removed and the account will be ready almost immediately.



*Average Admin Salary from payscale.com

Many account provisioning solutions themselves can introduce more of an administrative burden than they solve. Look for solutions with hidden costs such as complex workflow or scripting that will need to be constructed and then maintained. Another consideration is if the account provisioning solution requires additional software like an expensive SQL or Oracle database backend. Without considering these hidden costs the solution may wind up costing more than the loss from manual account provisioning.

Account Provisioning Considerations

- Manual account provisioning is time consuming, error prone and expensive
- Automated provisioning is not needed by everyone
- Items that make provisioning complex
    - Create a unique Logon name and Generate a unique password
    - Enter organizational details such as Office, Address, Manager, Title etc…
    - Set user Profile, Home folder & Remote Services resource settings
    - Add users to the appropriate groups
    - Create or configure mailbox & assign management policies
    - Initiate Sync to other platforms and assign licenses or roles on those systems
- Manual provisioning cost vary widely but are typically between $12 and $46 per user
- New users can be delayed for several hours waiting for new user accounts.

About Cayosoft

Simple and affordable, Cayosoft Administrator Suite is the #1 solution for Office 365 License Management. Cayosoft's unique architecture gives administrators easy to setup rules to define the organizational wide policies for Office 365 License Management.

Active Directory Management – Features

- Account Provisioning
- Automatic Group Management
- Hybrid Administration with Office 365
- On-going Administration & Maintenance
- Real-time Visibility & Reporting

For more information visit:

https://www.cayosoft.com/automate-active-directory-administration/

We are here to help answer any questions you may have so please contact us using one of the following methods:
U.S. Toll Free: +1-866-848-5350
International: +1-614-423-6718
E-mail us: sales@cayosoft.com
Web: http://www.cayosoft.com/contactsales/