Microsoft Active Directory Management to Control Access and Boost Security

Active Directory management tips from Ross Phillips

A small to medium-sized business may include hundreds of employees and thousands of devices. Microsoft Active Directory (AD) provides an indispensable method for identifying those resources and managing access within the system. In organizations with data in the cloud, Azure AD provides a similar service for cloud-based servers and applications such as Office 365 for business.

Active Directory and Azure AD form the core of an organization's information technology (IT) environment. Tapping into the full capabilities of these tools requires Windows PowerShell, a command-line shell and scripting environment. While PowerShell is essential to Active Directory management, it requires a level of expertise not available in many IT departments.

At the same time, because AD determines system access, it represents a treasure trove for hackers. Unauthorized changes to AD, whether nefarious or accidental, can wreak havoc in an organization.

Delegating Management Tasks

User and resource management involves a host of complex tasks, much more than a single system administrator can effectively manage. Consequently, administrators delegate some of those tasks to help desk personnel, team managers and occasionally consultants.

While these employees and consultants need appropriate credentials to perform assigned tasks, administrative privileges typically give them greater system access than they actually need. Every access granted increases the danger. For instance, an employee may accidentally delete a user account or even intentionally sabotage the system.

To protect the organization, you need a way to provide employees and consultants just enough access to complete their assigned tasks, but no more. You also need to be able to quickly determine exactly who has administrative privileges and what changes they have made.

An Eye on Security

For many organizations, AD represents the keys to the castle. Once bad actors have taken over AD, they can mine credentials of individual users or elevate privileges to admin level, thus gaining access throughout the system. Consequently, hackers increasingly target AD.

For example, in March of 2019, Norwegian aluminum giant Norsk Hydro suffered a ransomware attack via AD. The attack forced the shutdown of automated production lines on multiple continents. Recovering from cyber-attacks can prove extremely costly, both to the budget and to the company's reputation.

Individuals within an organization can also cause significant damage to network security through AD. Consider the danger when an employee with administrative access becomes disgruntled. With broad privileges, that employee can easily and quickly cause widespread damage through unauthorized changes to system schema.

Comprehensive Reporting

Because AD and Azure AD control so much of the underpinnings of your organization's IT environment, AD reports play a pivotal role. For example, security reports deliver alerts to possible risks, such as potentially fraudulent sign-in attempts. And usage reports can provide information important in determining the appropriate number of licenses to purchase.

The reporting possibilities are practically endless. With reports, administrators can obtain a complete picture of activity within the system, from passwords and application usage to regulatory compliance.

While the Office 365 Management and Azure portals provide some basic reports, comprehensive reporting requires PowerShell scripts.

Customized Portal for Active Directory Management

Messaging Architects will soon offer a tool to help you get the most out of AD and Azure AD, while limiting exposure within a critical environment. With new hosted AD management options, your organization can benefit from powerful custom scripts for essential tasks and reporting. This new portal protects system security while delivering robust AD management.

For instance, with a customized script, you can quickly grant consultants just the specific access they require for micro tasks within your system. You can also run custom reports to determine license usage or see what users have Admin access to the system.

If you would like to tap into these possibilities, or if you have specific tasks you would like automated, join the conversation. Email your questions or suggestions to Ross Phillips at ross.phillips@messagingarchitects.com.

Ross Phillips began working with Messaging Architects eleven years ago. Currently a solutions architect and implementation consultant, Phillips manages email migrations for companies of all sizes and across multiple industries. A CISSP-certified professional, he is passionate about security.

Bonus Summer Grilling Tip *(because Ross is also passionate about grilling!): If you are going to barbeque brats this summer, remember to parboil them for 10 to 20 minutes before you put them on the grill. This will infuse flavors and ensure a safe, thoroughly cooked sausage prior to placing them on the grill. Safe grilling is happy grilling!*