opentext™ | Cybersecurity

Position Paper

The Challenges of Administering Active Directory

As Active Directory's role in the enterprise has drastically increased, so has the need to secure the data it stores and to which it enables access. The lack of native control makes the secure administration of Active Directory a challenging task for administrators. As a result, organizations need assistance in creating repeatable, enforceable processes that will ultimately reduce administrative overhead while simultaneously helping increase the availability and security of their systems.

This position paper outlines seven common challenges associated with the secure administration of Active Directory and provides some helpful insight into what NetIQ by OpenText™ can do to assist you.

Table of Contents

Active Directory's Central Role in Enterprise Environments

Since its availability with Microsoft Windows (Windows) 2000, organizations have used Microsoft Active Directory (Active Directory) to help administer and secure their Windows environments. Deployment of, and reliance upon, Active Directory in the enterprise continues to grow.

Active Directory's role in the enterprise has drastically expanded, as has the need to secure the data it stores and to which it enables access.

It is becoming more and more the central data store for sensitive user data and the gateway to critical business information. This provides organizations with a consolidated, integrated and distributed directory service, and enables the business to better manage user and administrative access to business applications and services.

Active Directory's role in the enterprise has drastically expanded, as has the need to secure the data it stores and to which it enables access. Unfortunately, native Active Directory administration tools provide little control over user and administrative permissions and access. The lack of control makes the secure administration of Active Directory a challenging task for administrators. In addition to limited control over what users and administrators can do in Active Directory, the database has a limited ability to report on activities performed. This makes it very difficult to meet audit requirements and secure Active Directory. As a result, organizations need assistance in creating repeatable, enforceable processes that will ultimately reduce their administrative overhead while helping increase the availability and security of their systems.

Because Active Directory is an essential part of the IT infrastructure, you must thoughtfully and diligently manage it—that is, control it, secure it and audit it. Not surprisingly, with an application of this importance there are challenges to confront and resolve to reduce risk while deriving maximum value for the business. This paper examines seven of the most challenging administrative tasks related to Active Directory.

Compliance Auditing and Reporting

In the face of diverse regulatory mandates such as HIPAA, Sarbanes-Oxley and PCI-DSS, achieving, demonstrating and maintaining compliance is challenging. To satisfy audit requirements, organizations must demonstrate control over the security of sensitive and business-critical data. However, without additional tools, demonstrating regulatory compliance with Active Directory is time-consuming, tedious and complex.

Auditors and stakeholders require detailed information about privileged-user activity. This level of granular information enables interested parties to troubleshoot problems and also provides information necessary to improve the performance and availability of Active Directory.

Auditing and reporting on Active Directory has always been a challenge. Prior to the release of Windows Server 2008, there were no granular reporting capabilities. There is now limited reporting on some of the details auditors require in Windows Server 2008. While this limited information is a move in the right direction, it is not robust enough to meet stringent auditing requirements or to support business changes or decisions.

Auditors and stakeholders require detailed information about privileged-user activity. This level of granular information enables interested parties to troubleshoot problems and also provides information necessary to improve the performance and availability of Active Directory.

To more easily achieve, demonstrate and maintain compliance, organizations should employ a solution that provides robust, customizable reporting and auditing capabilities. Reporting should provide information on what, when and where changes happen, and who made the changes. Reporting capabilities should be flexible enough to provide graphical trend information for business stakeholders while also providing granular detail necessary for administrators to improve their Active Directory deployment. Solutions should also securely store audit events for as long as necessary to meet data retention requirements and enable the easy search of these events.

Group Policy Management

Microsoft recommends that Group Policy be a cornerstone of Active Directory security. Leveraging the powerful capabilities of Group Policy, IT organizations can manage and configure user and asset settings, applications and operating systems from a central console. It is an indispensable resource for managing user access, permissions and security settings in the Windows environment.

Maintaining a large number of Group Policy Objects (GPOs), which store policy settings, can be a challenging task. For example, one must take special care in large IT environments with many system administrators, because making changes to GPOs can affect every computer or user in a domain in real time. However, Group Policy lacks true change-management and version-control capabilities. Due to the limited native controls available, accomplishing something as simple as deploying a shortcut requires writing a script. Custom scripts are often complex to create and difficult to debug and test. If the script fails or causes disruption in the live environment, there is no way to roll back to the last known setting or configuration. Malicious or unintended changes to Group Policy can have devastating and permanent effects on an IT environment and a business.

To prevent Group Policy changes that can negatively impact the business, IT organizations often restrict administrative privilege to a few highly skilled administrators.

To prevent Group Policy changes that can negatively impact the business, IT organizations often restrict administrative privilege to a few highly skilled administrators. As a result, these staff members are overburdened with administering Group Policy rather than supporting the greater goals of the business.

To leverage the powerful capabilities of Group Policy, it is necessary to have a solution in place that provides a secure offline repository to model and predict the impact of Group Policy changes before they go live. The ability to plan, control and troubleshoot Group Policy changes—coupled with an approved change and release-management process—enables you to improve the security and compliance of your Windows environment without making business-crippling administrative errors. Organizations should also employ a solution for managing Group Policy that enables easy and flexible reporting to demonstrate that they've met audit requirements.

There are no automation or policy enforcement capabilities native to Active Directory. With little control in place, there is no way to ensure that users will receive the access they need when they need it.

User Provisioning, Reprovisioning and Deprovisioning

Most employees require access to several systems and applications, and each program has its own account and login information. Even with today's more advanced processes and systems, employees often find themselves waiting for days for access to the systems they need. This can cost organizations in lost productivity and employee downtime. To minimize workloads and expedite the provisioning process, many organizations look to Active Directory to be the commanding data store for managing user account information and access rights to IT resources and assets.

Provisioning, reprovisioning and deprovisioning access via Active Directory is often a manual process. In a large organization, maintaining appropriate user permissions and access can be a time-consuming activity, especially when the business has significant personnel turnover. Systems administrators often spend hours creating, modifying and removing credentials.

In a large, complex business, manual provisioning can take days. There are no automation or policy enforcement capabilities native to Active Directory. With little control in place, there is no way to ensure that users will receive the access they need when they need it. In addition, there is no system of checks and balances. Administrative errors can easily result in elevated user privileges that can lead to security breaches, malicious activity or unintended errors that can expose the business to significant risk.

Organizations should look for an automated solution to execute provisioning activities. Implementing an automated solution with approval capabilities greatly reduces the burden on administrators, improves adherence to security policies, improves standardization and decreases the time a user must wait for access. It also expedites the removal of user access, which minimizes the ability of a user with malicious intent to access sensitive data.

Secure Delegation of User Privilege

Reducing the number of users with elevated administrative privileges is a constant challenge for the owners of Active Directory. Many user and helpdesk requests require interaction with Active Directory, but these common interactions often result in elevated access for users who do not need it to perform their jobs.

Because there are only two levels of administrative access in Active Directory (Domain Administrator or Enterprise Administrator), it is very difficult to control what users can see and do once they gain administrative privileges. Moreover, once users aquire powerful administrative capabilities, they can easily access sensitive business and user information, further elevate their privileges and even make changes within Active Directory. Elevated administrative privileges, especially when in the hands of someone with malicious intent, dramatically increase the risk exposure of Active Directory and the applications, users and systems that rely upon it (Human Resource (HR) systems or proprietary business information, for example).

It is not uncommon for a business to discover that thousands of users have elevated administrative privileges. Each user with unauthorized administrative privileges presents a unique threat to the security of the IT infrastructure and business. Coupled with Active Directory's latent vulnerabilities, it is very easy for someone to make business-crippling administrative changes. When this occurs, troubleshooting becomes a nightmare, as auditing and reporting limitations mentioned earlier make it nearly impossible to quickly gather a clear picture of the problem.

It is not uncommon for a business to discover that thousands of users have elevated administrative privileges. Each user with unauthorized administrative privileges presents a unique threat to the security of the IT infrastructure and business.

To reduce the risk associated with elevated user privilege and ensure that users only have access to the information they require, organizations should seek a solution that can securely delegate entitlements. This is a requirement to meet separation-of-duties mandates, as well as a way to share the administrative load by securely delegating privileges to subordinates.

For example, an administrator may wish to delegate the ability to reset passwords to the members of the helpdesk in order to more quickly resolve user requests and reduce administrative burden. With granular privilege delegation, the helpdesk would be able to reset passwords but would not have the ability to take other administrative actions in Active Directory, ultimately improving efficiency and reducing business risk.

Change Auditing and Monitoring

To achieve and maintain a secure and compliant environment, you must control change and monitor for unauthorized changes that may negatively impact your business. Active Directory change auditing is an important procedure for identifying and limiting errors and unauthorized changes to your Active Directory configuration. One single change can put your organization at risk, introducing security breaches and compliance issues.

Native Active Directory tools fail to proactively track, audit, report and alert administrators about vital configuration changes. In addition, native real-time auditing and reporting on configuration changes (including GPOs), day-to-day operational changes and critical group changes do not exist. This exposes the business to risk, as your ability to correct and limit damage is dependent on your ability to detect and troubleshoot a change once it has occurred.

A change that goes undetected can have a drastic impact on your organization. For example, users who elevate their privileges and change their identity to that of a senior member of the finance department could potentially access company funds resulting in theft, wire transfers and so forth.

To reduce risk and help prevent security breaches, organizations should employ a solution that provides comprehensive change monitoring. This solution should include real-time change detection, intelligent notification, human-readable events, centralized auditing and detailed reporting. Employing a solution that encompasses all of these elements will enable you to quickly and easily identify unauthorized changes, pinpoint their source and resolve issues before they negatively impact the business.

To reduce risk and help prevent security breaches, organizations should employ a solution that provides comprehensive change monitoring. This solution should include real-time change detection, intelligent notification, human-readable events, centralized auditing and detailed reporting.

Maintaining Data Integrity

It is important for organizations to ensure that the data housed within Active Directory supports the needs of the business, especially as other applications rely on Active Directory for content and information.

Data integrity involves both the consistency of data and the completeness of information. For example, there are multiple ways to enter a phone number:

- +1.713.418.5555
- 713 418-5555
- 7134185555
- 1-713-418-5555
- (713) 418-5555

Entering data in inconsistent formats creates data pollution. Data pollution inhibits the business from efficiently organizing and accessing important information. Another example of data inconsistency is the ability to abbreviate a department name. Think of the various ways to abbreviate “Accounting.” If there are inconsistencies in Active Directory’s data, there is no way to ensure that an administrator can group all the members of accounting together, which is necessary for payroll, communications, systems access and so on.

Another vital aspect of data integrity when working with Active Directory is the completeness of information. For example, if an employee is transferred to a new department in a different city and state, the company’s HR system would leverage Active Directory to update benefits and payroll information. However, the HR system would not know where to send the employee’s paystub if the administrator did not enter the zip code. Active Directory provides no control over content that is entered natively. If no controls are in place, administrators can enter information in any format they wish and leave fields that the business relies upon blank.

To support and provide trustworthy information to all aspects of the business that rely on Active Directory, organizations should employ a solution that controls both the format and completeness of data entered in Active Directory. By putting these controls in place, you can drastically reduce data pollution and significantly improve the uniformity and completeness of the content in Active Directory.

To support and provide trustworthy information to all aspects of the business that rely on Active Directory, organizations should employ a solution that controls both the format and completeness of data entered in Active Directory.

Self-Service Administration

Most requests made by the business or by users require access to and administration of Active Directory. This is often manual work and there are few controls in place to prevent administrative errors. Active Directory's inherent complexity makes these errors common, and just one mistake could do damage to the entire security infrastructure. With the lack of controls, the business cannot have just anyone administering Active Directory.

While it may be practical to employ engineers and consultants to install and maintain Active Directory, organizations cannot afford to have their highly-skilled and valuable employees spending the majority of their time responding to relatively trivial user requests.

Self-service administration and automation are logical solutions for organizations looking to streamline operations, become more efficient and improve compliance. This is achieved by placing controls around common administrative tasks and enabling the system to perform user requests without tasking highly-skilled administrators. Organizations should identify processes that are routine yet hands-on, and consider solutions that provide user self-service and automation of the process. Automation of these processes reduces the workload on highly-skilled administrators and also improves compliance with policies since automation does not allow users to skip steps in the process. Organizations should also look for self-service and automation solutions that allow for approval and provide a comprehensive audit trail of events to help demonstrate policy compliance.

Secure Configuration Manager allows administrators to demonstrate regulatory compliance with USGCB and other standards.

NetIQ Secure Configuration Manager by OpenText also leverages configuration information to identify vulnerabilities, as well as instances in which data is exposed to outside access. To do this, it uses the latest security updates from the National Vulnerability Database.

Customers are further able to easily establish a current policy compliance baseline, download the latest security knowledge and tailor configuration and vulnerability checks across multiple platforms and applications.

Secure Configuration Manager allows administrators to demonstrate regulatory compliance with USGCB and other standards. It also enables them to manage IT risks via scored reporting so they can direct remediation efforts toward issues of highest priority.

Conclusion

Active Directory has found its home as a mission-critical component of the IT infrastructure. As businesses continue to leverage it for its powerful capabilities as a commanding repository, Active Directory is a vital part of enterprise security. Therefore, administrators must be able to control, monitor, administer and protect it with the same degree of discipline currently applied to other high-profile information such as credit card data, customer data and so forth.

Using our solutions, customers and partners can capitalize on the opportunities in today's complex and ever-changing IT landscape.

Because native tools do not enable or support the secure and disciplined administration of Active Directory, organizations must look for solutions that enable its controlled and efficient administration. These solutions help ensure the business information housed in Active Directory is both secure and appropriately serving the needs of the organization.

This paper has explored some of the most challenging aspects of securely administering Active Directory. OpenText provides Active Directory management and security solutions that increase your control over Active Directory administration and improve your ability to achieve and maintain compliance. In addition, solutions from OpenText decrease the cost and complexities associated with administering Active Directory. For more information on how OpenText can help you securely administer Active Directory, visit: **www.microfocus.com/en-us/cyberresilient**

About NetIQ by OpenText
OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

Connect with Us

www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.