Identity management in action

Introduction

The exponential increase in digital interactions and the dispersion of users across various platforms make identity management an imperative aspect of cybersecurity.

Identity management, or IdM, refers to the process of managing individual identifiers, their authentication, authorization, and roles within or across system and enterprise boundaries to increase security and productivity while decreasing cost, downtime, and repetitive tasks. Central to this is Active Directory (AD), a Microsoft technology used for access control and Identity Federation.

This reading explores how AD manages users and computers and the integral role of identity federation.

Active Directory (AD) and access control

AD is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems, providing various network services, including LDAP, Kerberos-based and DNS-based authentication. What's more, AD centralizes the administration and security of an enterprise IT environment.

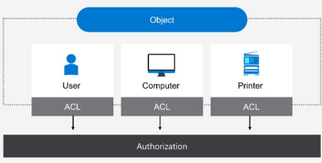
Access control is at the core of AD's functionality, managing who can or cannot access specific resources within a network. This management is handled in two parts: authentication and authorization. Authentication verifies the user's identity attempting to gain access, while authorization determines what authenticated users can or cannot do.

Review the following to learn more:

- Access Control overview: Discover the key concepts and components that make up access control, including permissions, ownership of objects, inheritance of permissions, user rights, and object auditing.

Access control list (ACL)

AD employs a mechanism known as access control lists (ACLs) to implement authorization. Each object in an AD (users, computers, printers, network shares, etc.) has an ACL attached, which defines who has access to the object and what operations they can perform. This structured approach ensures that only authorized individuals can access sensitive information, thereby maintaining security.



AD's approach to access control employs intricate but clear-cut mechanisms to authenticate and authorize users. By making use of access control lists, it effectively dictates who can access what, ensuring network integrity and security.

However, as organizations become more interconnected, accessing resources across multiple domains becomes a frequent necessity. In this context, identity federation, particularly AD's implementation through Active Directory Federation Services, becomes invaluable.

Review the following to learn more:

- Access control lists: Explore the role of ACLs in managing access to securable objects.

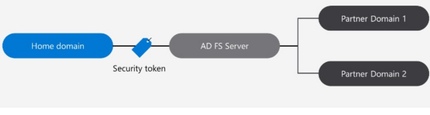
Identity federation and Active Directory Federation Services (AD FS)

It's not uncommon for people to access resources outside of their home domain. Think of the times you've used a single account, like your Microsoft account or a social media profile, to sign into different websites.

Identity federation enables your digital identity, stored in one system (the home domain), to be used by other systems (partner domains), even if those systems use different authentication methods. This facilitates single sign-on (SSO), allowing you to authenticate once and gain access to multiple systems.

Active Directory Federation Services (AD FS) is Microsoft's solution to Identity Federation. AD FS uses a claims-based access-control authorization model. This means it passes identity-based claims on your behalf between an AD FS-secured enterprise and a federation partner.

In this model, your digital identity is encapsulated into a security token, a sort of digital passport, which is issued by the home AD FS server. When you attempt to access a resource in a partner domain, this security token is presented to the partner's AD FS server. Access is granted if the security token is valid and you are authorized. This process allows you to navigate seamlessly across trusted systems, improving the user experience and operational efficiency.



Simply put, identity federation allows you to take your digital identity beyond the boundaries of your home domain, accessing resources in partner domains with the convenience of single sign-on. AD FS facilitates this using a claims-based access control model, issuing security tokens that encapsulate the user's identity and can be trusted across domains.

Active Directory in user and computer management

Active Directory maintains an organized structure of all network components, including users and computers, making managing them easier. Each user account in AD has a unique username and a set of attributes - such as full name, password, and group membership - that define the user's identity and access permissions. Similarly, each computer has a unique name and attributes.

Group Policies, another feature of AD, allow administrators to manage users and computers efficiently. They can define policies for a group of objects, and AD automatically enforces these policies. This means admins can manage settings across many users and computers simultaneously, simplifying administrative tasks.

For example, an admin might want to enforce a policy that all company-owned computers should have specific security software installed. By defining this in Group Policy and applying it to the relevant computer objects in AD, this task can be accomplished without manually configuring each computer.

In terms of managing users and computers, Active Directory provides an organized structure that makes it easier for administrators to navigate and control their network components. Through features like Group Policies, administrators can simultaneously apply settings across a multitude of users and computers, streamlining administrative tasks and promoting consistency.

AD use case for Sam's Scoops

Let's imagine that Sam's Scoops has experienced rapid growth, expanding to three ice cream stores in the city. To effectively manage the user accounts and computers across all locations, Sam decides to use Active Directory (AD).

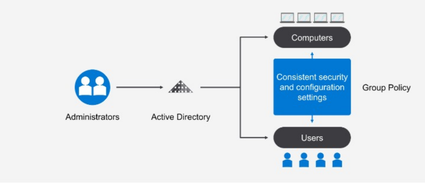
In Active Directory, Sam creates a unique user account for each employee. These accounts are given unique usernames and passwords, while Sam defines specific attributes for each account, such as the employee's role (cashier, store manager, etc.), contact information, and the particular store they work at. These attributes help identify each user's identity and role within the business.

Next, Sam organizes the computers within her stores using Active Directory to streamline computer management. Each computer has its own entry, complete with unique attributes like location and function(Point-of-Sale terminal, back-office computer, etc.).

Now, Sam wants to enforce certain policies to enhance security and operational consistency across her stores. For instance, she wants all Point-of-Sale (POS) computers to run a specific version of the POS software, have antivirus software installed, and lock the screen automatically after 5 minutes of inactivity.

Using the Group Policy feature in Active Directory, Sam easily configures these policies. She creates a Group Policy Object (GPO) for the POS computers and defines the desired settings. She then links this GPO to the group of POS computer objects in AD. From now on, these settings are automatically applied to all POS computers, without manually configuring each computer.

When a new computer is added, or an existing one is replaced, Sam only needs to add it to the relevant group in AD, and the necessary settings and software will be automatically configured based on the group policies.



Through AD, Sam can manage her business's users and computers efficiently and uniformly, ensuring a smooth operation across all her stores.

This example highlights the effectiveness of AD in simplifying administrative tasks, maintaining consistent settings, and elevating a business's overall security.

Conclusion

In conclusion, identity management is a multi-faceted task that demands precision and flexibility. By using technologies like Active Directory, businesses can improve their networks' security, efficiency, and scalability. AD's capabilities for access control, Identity Federation, and user/computer management provide a comprehensive suite of tools to deal with today's challenges in identity management. These elements in action are evidence of how essential and intricate identity management is in the digital world, serving as a cornerstone of cybersecurity, user convenience, and operational efficiency.

Mark as completed