MICROSOFT ACTIVE DIRECTORY

NETWORK MANAGEMENT USING DIRECTORY SERVICES

ITC ADMINISTRATORS MUST QUICKLY RESPOND TO NEW REQUIREMENTS IN THE CONTINUOUSLY CHANGING WORLD OF INFORMATION TECHNOLOGIES. MICROSOFT ACTIVE DIRECTORY SERVICES HELP THEM ACHIEVE THIS GOAL.

Demands on ICT administrators have never been greater. Pressure to increase work efficiency, lower costs and improve employee productivity require that ICT administrators search for solutions to rather difficult problems.

[IDENTITY MANAGEMENT]

Organizations use ever-growing numbers of applications and information systems, and their growing numbers also entail growth in the number of identities that must be managed by administrators and used by employees. This results in a need to consolidate user identities in applications and information systems in a single central location for their administration, including the management of authorization data for user access to computers and network services.

[COMPUTER MANAGEMENT]

ICT administrators must also manage the computers in the network, perform the required modifications in their configurations, install new software, and provide security for the operated computers, applications and information systems.

FEATURES AND BENEFITS

- Central user account and user information management
- Group and group member management
- Single user authentication and authorization for network service access
- Consolidation of computer configurations in a network, of their security settings and installed applications

[MICROSOFT ACTIVE DIRECTORY]

Microsoft Active Directory design and implementation help in:

- Introducing a single directory service providing authentication and authorization services for the whole organization.
- Implementing the available infrastructure of the Active Directory domain controllers, which complies with the requirements for continuity of the organization's services.
- Migrating to a single Microsoft Active Directory service together with consolidation and securing of the ICT operating environment.
- Introducing central management of computer and user desktop lifecycles using group policies, and subsequently lower the costs and improve the efficiency of workstation management.

Benefits include a decrease in computer network complexity, streamlined management and higher efficiency of new technology integrations resulting in lower general costs, higher productivity and greater agility.
The current implementation of the Microsoft Active Directory service can be consolidated to effectively respond to any needs of the organization that have developed since the Microsoft Active Directory service was deployed.

[ACTIVE DIRECTORY CONSOLIDATION]

We build on our long-term experience in using the Active Directory service in largescale networks to ensure their effective utilization:

- Securing of the Active Directory service, Microsoft operating systems and other Microsoft products according to the Microsoft Security Compliance Manager methodology.
- Design of a robust geographic topology for domain controllers and reliable Active Directory replication.
- Design of an effective Active Directory organizational structure and administrator privilege delegation.
- Workstation and user desktop lifecycle management using group policies.
- Integration of infrastructure network services (DNS, DHCP, WINS, NTP, LDAP, Kerberos) in heterogeneous networks.
- Single platform and authentication and authorization and user authorization and Single Sign-On integration in applications and information systems.

[ACTIVE DIRECTORY DOMAIN SECURITY]

A violation of Active Directory and Microsoft Windows operating system security could result in the failure of the computer network and an information leak. We have therefore developed the Trusted Computer Base, designed to secure the directory service and computers with Microsoft Windows operating systems and the services running on these systems.

Active Directory security is based on the Microsoft Compliance Security Manager methodology and is implemented through group policies:

- TCB Domain Policy - basic security configuration for all computers and services in the Active Directory domain.
- TCB Domain Controllers Policy - security configuration for domain controllers.
- TCB Windows Server Policy - security configuration for application servers.
- TCB Windows Workstation Policy - security configuration for workstations.

These group policies are common for computers running Microsoft Windows 2000 and later operating systems.

[EFFECTIVE ORGANIZATIONAL STRUCTURE]

Objects in the Active Directory service can be arranged into an organizational structure according to many aspects and the needs of the applications that use them. An effective organizational structure design must correspond not only to the application and information system requirements, but also to the requirements for the operation and management of the Active Directory service itself.

[ROBUST GEOGRAPHIC TOPOLOGY]

The correct distribution of Active Directory domain controllers into the individual sites and configuration of replication topology provide a reliable directory service supporting Business Continuity Management for the information systems used.

[INTEGRATION AND THE CLOUD]

The integration of information systems with information systems of other organizations and the transfer of parts or the whole ICT of an organization into the cloud represent new fields of work. Here, it is especially important to utilize consolidated identities by means of their synchronization or using a central directory service.

[INTEGRATION OF INFRASTRUCTURE SERVICES]

Active Directory domain controllers can provide all infrastructure network services, such as DNS, DHCP, WINS, NTP, LDAP and Kerberos needed by Active Directory for its operation. In heterogeneous networks, these services are often provided partially or fully on different platforms and it is therefore necessary to integrate them - to decide which platforms and servers will be used to provide the individual services, and how the configurations of computers and other network devices will be modified so they can use these services.

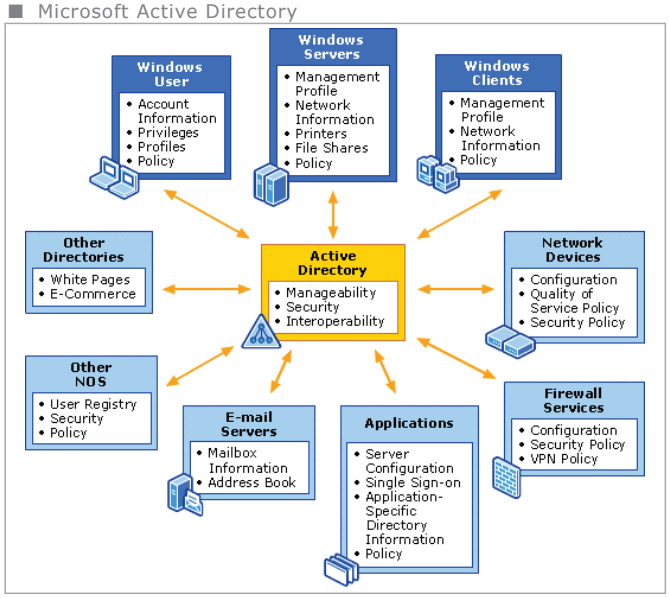
[UNIFIED AUTHENTICATION AND AUTHORIZATION]

Using Active Directory as a unified platform for authentication and authorization of users through LDAP, NTLM, Kerberos, NIS and Radius protocols significantly reduces the need for user identity management in applications and information systems. Kerberos, moreover, provides Single Sign-On user login to network services. Active Directory Federation Services integrates Active Directory with information systems operated via the Internet.

[WORKSTATION AND USER DESKTOP MANAGEMENT]

The unified installation of a Windows operating system using the Windows Deployment Service sand the installation of applications and user desktop management using group policies enable effective application management and user environment control. Using roaming profiles, it is possible to break users' dependence on a specific computer and reliably back up all user data.

■ Microsoft Active Directory



COMMERCIAL CONTACT

ICZ a.s. Na hrebenech II 1718/10
140 00 Prague 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: marketing@i.cz