Information Services & Technology

Windows Server Platforms: Detailed Information on win.mit.edu

Introduction

win.mit.edu, or WIN, is the MIT centrally-maintained Windows Domain.

- General Description
- Prominent Benefits and Disadvantages
- Features Specific to MIT and WIN
- Design Choices Specific to MIT and WIN

General Description

WIN is intended for general use by any and all users, departments, labs, centers, or DLC, and offices. Its structure and features are intended to foster efficiency and collaboration across the Institute by providing a common set of services, data and tools. Many aspects and features within this Domain are customizable by participating DLCs and in certain cases individual users. Although WIN is not intended to meet every specific need on campus as a platform, it is a product and set of associated services intended to meet the needs of most users.

WIN provides not only single sign-on to systems and applications within the domain, but also extends this single sign-on to other Kerberos-enabled systems in use at MIT.

Directory data is fed from other MIT systems into the WIN Domain Active Directory, or AD, database. This includes information from the Data Warehouse and Moira. In the future we also expect to feed some data from the MIT Roles system into AD. This means that users can have access to common and consistent data, names, and access control lists across a variety of computer systems at MIT.

Prominent Benefits

Beyond the features standard to Windows 2000 Professional and Windows XP Professional (on desktops/workstations/notebooks/laptops) and to Windows 2000 Server/Advanced Server and Windows Server 2003 Standard and Enterprise Editions (on servers) in a Domain, WIN users and administrators can take advantage of the following benefits:

For the user:

- Seamless integration into existing MIT infrastructure, including Kerberos, Moira, enterprise management interfaces,

and the Data Warehouse.

- Single sign-on using one's cannonical MIT Kerberos principal, the username and password.
- One "roaming" profile, the user's Windows settings and preferences, persistent in the user's DFS home directory. This home directory is accessible to Windows Explorer and other Windows applications through a drive letter (H:).
- Shared printing to a variety of MIT network printers, including Kerberized Athena print queues, in addition to native Windows printing services and methods.
- An automated problem reporting system, SendBug, runs as an integrated application.
- Potential AD schema extensions enables newer applications and technologies for future growth.

For the DLC container, a group of WIN machines, administrator:

- Centrally installed, maintained, and supported domain controllers, obviating any need to run or maintain domain controllers on a local basis.
- Containers as fundamental organizational units and "islands of control," with scalable Group Policy settings allowing custom configuration all machines similarly, including OS, software, behavior and associated settings.
- Assistance through documentation, central consulting and peer support for container administration through user groups.
- Flexible deployment options, including Remote Installation Services (RIS) images, RIPrep (monolithic) images, or joining existing machines running compatible Windows operating systems.
- Automatic and overridable push deployment of centrally-qualified and approved Windows Service Packs.
- Similarly, automatic push deployment of critical updates and security patches.
- Automatic and customizable periodic self-maintenance routines/scripts which run unattended within the SYSTEM account context.
- Central logging and optional auditing of events to a secure, access-controlled central log server.
- Native Windows as well as alternative Web-based interfaces for many machine and container administration tasks and domain requests.
- Moira (MIT mailing lists, groups, machine information, etc.) propagated to AD and used for security groups, machine memberships an access control lists (ACLs) within the Domain.
- Additional management tools and interfaces, including PERL scripting, Windows Resource Kit, Windows Support Tools, and others.
- Reliable and secure domain controller services and central servers with 24x7 availability (in continuous operation since Spring 2001).

WIN delivers features and significant benefits. These vary by customer, but situations inappropriate to WIN might be:

- Need to run application servers or services that require extensive Active Directory, AD, schema changes, modifications to the domain structure.
- Required compliance with government or private security or auditing policies if they conflict with those of IS&T.

Features Specific to MIT and WIN

Of the features and benefits listed above, the following are unique to MIT and the win.mit.edu domain, and are not normally found in a typical Windows Active Directory domain implementation:

- Username/password integration with MIT's existing Kerberos principals/Athena accounts/email usernames and passwords; associated single sign-on benefits with applications like Kerberos, Eudora, SAP, etc.
- OpenAFS is optional on machines within the domain.
  Note: OpenAFS for Windows is not supported by IS&T.
- DFS Roaming profile that is maintained and accessible.
- Extensions to standard Windows Group Policy settings unique to MIT, allowing for, among others:
  - Centralized distribution of software through MSI (self-repairing, rollback-capable Microsoft installer technology)

technology and Group Policy
    - Centralized distribution of key Microsoft updates normally not available in MSI format through Group Policy without the need for additional technologies such as Software Update Services, including
        - Windows Service Packs
        - Critical Updates
        - Security Patches
        - Peripheral Microsoft technologies, such as Internet Explorer versions
    - Control of machine behavior beyond what Microsoft offers, for needs such as
        - Idle user logoff management
        - Remote domain-wide reboots (overrideable)
- Periodic self-maintenance scripting and behavior (overrideable and partially customizeable).
- Extensive scripting, including:
- - Log-on as well as log-off time scripts
    - Use of PERL and Windows batch commands
- Central logging of system, application, and security events to a secure central log server, allowing for troubleshooting and back-tracking in case of total system failure.
- Integrated problem/bug reporting system.

Note: Some of the functionality above can be implemented in a typical Windows Active directory domain through the use of freely available versions of said software or third-party applications with similar features (e.g. the use of Microsoft DFS for distributed file system access). However, the win.mit.edu implementation of most all these features include additional benefits such as code fixes and developmental patches that allow for better stability and seamless integration. Additionally, all of these services are maintained centrally as part of the domain environment, allowing the users and administrators to focus on using them to address their day-to-day operational needs without worrying about maintenance and upkeep.

Design Choices Specific to MIT and WIN

While WIN provides many features and benefits to its user and the local administrator, there are certain requirements and design limitations that in place to present a standardized and reasonably maintainable infrastructure. These include:

- All domain controllers are centrally maintained by IS&T. End users and local administrators may not deploy domain controllers as part of the win.mit.edu domain, but Windows servers can participate as member servers.
- The win.mit.edu domain consists of a single, flat domain with containers of machines as organizational units available to participating DLCs or offices (beyond those required for central operational purposes). No sub-domains are allowed.
- No Kerberos or other trust relationships to outside Windows domains (within or outside MIT) are allowed due to privacy and security requirements.
- Domain user accounts are the same as existing MIT Kerberos principals/Athena user accounts/standard MIT email user accounts and are maintained by MIT User Accounts. (Local user accounts and groups can always be created on a per-machine basis.)
- Containers (groups of machines) can be nested, however, currently nesting is allowed up to two levels deep (e.g. at most, your container(s) may contain subcontainers that themselves contain only machines).
- Compatible operating systems are Windows 2000/XP Professional on the client side and Windows 2000 Server/Advanced Server or Windows Server 2003 Standard/Enterprise Eds. on the server side.
- User profiles are roaming by default and stored in the user's private DFS home directory. Alternative options are available, e.g. local profiles or stored on a departmental server.
- AD schema changes need to be negotiated and some may not be possible to implement if they conflict with domain requirements due to technical or policy (e.g. privacy) reasons. Proposals for such changes (for instance, if required

by an application a domain participant wishes to deploy) will be considered on a case-by-case basis.