ISM (Information Storage Management) Frame-Work for Companies

[I]**Prateek S,** [II]**Dr. T H Sreenivas**

[I]PG Student, [II]Professor

[I,II]Dept. of Information Science & Engineering, The National Institute of Engineering, Mysuru, India

Abstract

The ISM frame-work requires Active Directory. Active Directory is a special-purpose database. The directory is designed to handle a large number of read and search operations and a significantly smaller number of changes and updates. Active Directory data is hierarchical, replicated, and extensible. Because it is replicated, you do not want to store dynamic data, such as corporate stock prices or CPU performance. If your data is machine-specific, store the data in the registry. Typical examples of data stored in the directory include printer queue data, user contact data, and network/computer configuration data. The Active Directory database consists of objects and attributes. Objects and attribute definitions are stored in the Active Directory schema. The Active Directory is also a directory service included with Windows Server. It extends the features of previous Windows-based directory services and adds entirely new features. The Active Directory is secure, distributed, partitioned, and replicated. It is designed to work well in any size installation, from a single server with a few hundred objects to thousands of servers and millions of objects. The Active Directory adds many new features that make it easy to navigate and manage large amounts of information, generating time savings for both administrators and end users.

Keywords

Active Directory Domain, Organizational Units, power shell

Problem Description

Security has always been a principal issue in society, and this is especially true of modern society. The IT world is no different and data security is a crucial aspect of this information age. Valuable data is stored on many computer systems round the world. Access to information is restricted to those who require it through the use of passwords and encryption. The active directory implementation mainly enables the person to use his/her data in a very high confidential and can use his/her data in outside the same organization with provided legal passwords to each of the individual password. This will be mainly use full in large organizations which have many branches across the country.At the end we have provided the front end site to enable the employees details.

Project Aim

The aim of this project is to research and explore the feasibility of an integrated security system. The new development aims to place many aspects of existing IT and physical security systems into one secure system. The proposed system will attempt to utilize current technologies such as wireless networking, embedded system components and Microsoft's Active Directory to create a package that once deployed within a business or organization, would provide security administration and easeablity of access for all aspects of company

Introduction

Active Directory domain services are used primarily to manage Users and Resource management across Enterprise infrastructures spanning the physical subnets across the globe. Active Directory domain provides distributed database to store and manage application data, user data and computer data respectively. Active directory structure comprises of Single forest, with multiple domains and child domains. Administrator can configure active directory domain based on the physical subnets , it is advisable to install directory server on the physical site.
Active directory provides different security boundaries in the

form of
a) Forest
b) Domain
c) Organizational Units

In a more realistic example, many organizations and businesses use Active Directory to store employee information. Employees that want to use company resources must authenticate to Active Directory before going any further. IT administrators use Active Directory to maintain order in the organization.

In order to provide the entire view of the entire organization we have implemented it through a front end display where all the details of the employees or registered.

To have an efficient ISM Frame-work we have implemented the following features to active directory.

1. Digital Information Security IT or logical security
2. Firewalls(enabling and disabling ports)
3. Intrusion Detection and Anti-virus software Intrusion Detection
4. Authentication
5. Single-Use Password
6. Automatic log off
7. Login and Logout Time: How many hours the person will use the computer. How many persons will use the same computer
8. Antivirus policy: antivirus applications and required to block ports
9. Applications installed policy
10. Antivirus report
11. Blocking of computer if a person retires / transferred at midnight 12AM (after giving resignation)
12. PB number
13. OS Version and OS configuration

Hardware Requirements

Depending on your configuration, we need some or all of the following hardware:
• One or more network adapters with a Network Driver Interface

Specification (NDIS) driver for LAN connectivity
• One or more compatible modems and an available COM port
• ISDN adapter (if you are using an ISDN line)
• DSL adapter
• X.25 adapter or PAD (if you are using X.25)
• Analog telephone line, ISDN line, X.25 line, or DSL line
• Smart card reader
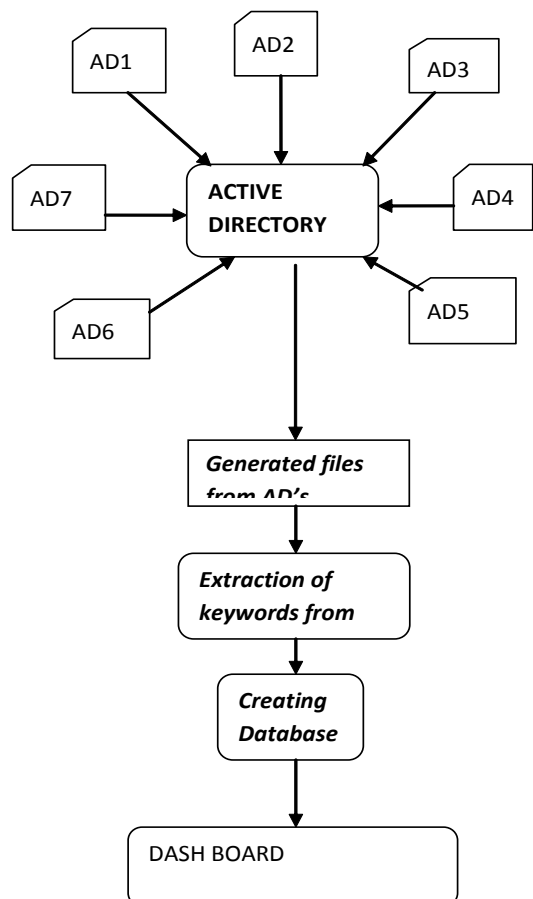• Wireless adapter
• DNS
• Clients
• Servers

Software requirements for data extraction and data storage
• Active Directory
• Power Shell
• C and c++
• Asp.net
• Java
• Php
• Html
• Pl/sql

Implementation Detail
• Planning DNS
• Installing and Configuring Active Directory and DNS
• Configuring DNS Client Settings
• Troubleshooting DNS

System Design

Installing and Configuring Active Directory and DNS
When you create a new domain, the Active Directory Installation Wizard installs DNS on the server by default. This ensures that DNS and Active Directory are configured properly for integration with each other.

Important
Before you install Active Directory and DNS on the first domain controller server in a new domain, ensure that the IP address of the server is static, meaning it is not assigned by Dynamic Host Configuration Protocol (DHCP). DNS servers must have static addresses to ensure that they can be located reliably.

To install DNS with Active Diectory in a new domain:
1. Click **Start**, point to **Administrative tools**, and then click **Configure Your Server Wizard**.
2. On the **Manage Your Server** page, click **Add or remove a role**.
3. On the **Configure Your Server Wizard** page, click **Next**.
4. Click **Domain Controller (Active Directory)** and then click **Next**.
5. On the **Welcome to the Active Directory Installation Wizard** page, click **Next**.
6. On the **Operating System Compatibility** page, read the information and then click **Next**.
   If this is the first time you have installed Active Directory on a server running Windows Server 2003, click **Compatibility Help** for more information.
7. On the **Domain Controller Type** page, click **Domain controller for a new domain** and then click **Next**.
8. On the **Create New Domain** page, click **Domain in a new forest** and then click **Next**.
9. On the **New Domain Name** page, type the full DNS name (such as corp.contoso.com) for the new domain, and then click **Next**.
10. On the **NetBIOS Domain Name** page, verify the NetBIOS name (for example, CORP), and then click **Next**.
11. On the **Database and Log Folders** page, type the location in which you want to install the database and log folders, or click **Browse** to choose a location, and then click **Next**.
12. On the **Shared System Volume** page, type the location in which you want to install the SYSVOL folder, or click **Browse** to choose a location, and then click **Next**.
13. On the **DNS Registration Diagnostics** page, click **Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server**, and then click **Next**.
    On the **Permissions** page, select one of the following:
    Permissions compatible with pre-Windows 2000 Server operating systems Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems
15. On the **Directory Services Restore Mode Administrator Password** page, type a password that will be used to log on to the server in Directory Services Restore Mode, confirm the password, and then click **Next**.
16. Review the **Summary** page, and then click **Next** to begin the installation.
17. After the Active Directory installation completes, click **OK** to restart the computer.

Creating bulk users into Active Directory

We can create useres into active directory through 2 ways
- Mannually through active directory steps (users in min numbers)
- Through power shell scripts (bulk users)

We had a requirement of creating bulk users in Active directory for Test users. Initially we thought of writing .NET code which will communicate to LDAP and creates the users. But we were not aware of that it can be done very-2 quickly using the Powershell with 3-4 line of scripts.

Generation of files from computers added to Domain

We can generate file of users from active directory through 2 ways
- Active Directory CSV generator tool
- Through power shell skripts

The CSV Generator Tool helps you to generate a CSV file that contains a customized array of user specified attributes and the corresponding Active Directory values, all ready for any bulk Active Directory management. This free tool takes a simple CSV file with basic attributes like sAMAccountName, and generates a full -fledged CSV file containing a comprehensive attribute list. This would save considerable time and efforts of admins and other staff associated with Active Directory management. One main advantage of using this tool is that you can create a complex CSV file in a fraction of time by just supplying a simple and basic CSV as input.

The following steps will guide you through to generate a CSV file.
1. Click the "**CSV Generator Tool**" from the **Launcher** to start the tool.
2. Select the AD object type from the list.
3. Browse and select the import CSV file in the File Name field.
4. Click on GENERATE to get CSV file containing Canonical Name, Display Name and Description attributes.
5. Click on EXPORT to save the CSV file in a different location.

A. If you require the output CSV file with additional attributes, follow the steps given below:

1. Follow steps 1 – 3 as mentioned above.
2. Click on the ADVANCED button. This opens the Advanced Attributes dialog.
3. Select the attributes from the given list. The corresponding fields will get displayed on the left pane.
4. Select from the list on the left pane and Click on ADD to include the attributes in the generation list, shown in the right.
5. You can use the DELETE option to remove field names from the generation list.
6. Click on the FINISH button.
7. Click on the GENERATE button. This will display the object details with all specified attributes.
8. Click on EXPORT to save the CSV file in a different location.

Extraction and storage of data from the generated file
Extraction through different languages
C and C++
Asp.Net
Java
Phython

Storing the extracted data through PL/SQL

The PL/SQL programming language was developed by Oracle Corporation in the late 1980s as procedural extension language for SQL and the Oracle relational database. Following are notable facts about PL/SQL.

PL/SQL is a completely portable, high-performance transaction-processing language.

PL/SQL provides a built-in interpreted and OS independent programming environment.

PL/SQL can also directly be called from the command-line SQL*Plus interface.

Direct call can also be made from external programming language calls to database.

PL/SQL's general syntax is based on that of ADA and Pascal programming language.

Benefits

Deploying ISM frame-work provides the following benefits to your organization:

Simplified administration and resource management.
You can delegate administration to all levels of an organization, and you can use Group Policy to centralize administration.

Increased network security and single sign on for users.
Active Directory supports multiple authentication protocols and X.509 certificates, and provides support for smart cards.

Interoperability with other directory services.
Active Directory provides standards-based, open interfaces that interoperate with other directory services and applications, such as e-mail applications.

Features that reduce administration costs, increase security, and provide additional functionality.
Application directory partitions allow you to configure application-specific data replication settings on domain controllers. When you raise domain or forest functional levels to Windows Server 2003, you can do the following:
- Rename domains and domain controllers
- Establish two-way forest trusts
- Restructure forests
- Improve replication
- Remove some limitations in environments with a large number of sites

Conclusion

The Active Directory is the focal point for administration of Windows servers. The security system with ownership, auditing, permissions, inheritance and DACLs, applies consistently to the file system, the registry, the Active Directory, and to printers. The security system uses the same rules with all of these objects, but the permissions are different with different object types.

The file system has many features including, junction points, distributed link tracking, compression, encryption, client-side caching, dfs, and quotas. User profiles and policies provide a mechanism to control user environments. There are a number of troubleshooting tools to manage the Active Directory.

At the end we are provided a link form pl/sql database to the html web view. We can easily monitor all the retrieved information from the html.

References

[1] Siyan K, Hare C (1995), "Internet Firewalls and Network Security", New Riders Publishing, Indianapolis, Indiana, USA

[2] Tudor K.A (2000), "Information Security Architecture: An Integrated Approach to Security in the Organization", Auerbach Publications. Available Online at: ENGnetBase. com [12 January 2005]

[3] Wikipedia (2005), "Intrusion detection system" [Online]. [Accessed 4 April 2005], available via WWW: http:// en.wikipedia.org/wiki/Intrusion_detection_system

[4] "Directory System Agent". MSDN Library. Microsoft. Retrieved 23 April 2014

[5] "The Lightweight Directory Access Protocol (LDAP) Content Synchronization Operation".   Retrieved 2013-11-26

[6] "Active Directory Backup and Restore". TechNet. Microsoft. Retrieved 5 February 2014

[7] "Domain and Forest Trusts Technical Reference". Microsoft Corporation. 28 March 2003. Trusts enable [...] authentication and [...] sharing resources across domains or forest

[8] "Running Domain Controllers in Hyper-V". TechNet. Microsoft. Planning to Virtualize Domain Controllers. Retrieved 5 February 2014. You should attempt to avoid creating potential single points of failure when you plan your virtual domain controller deployment. Frank

Author Profile

Mr. Prateeks.S is a student of national institute of engineering, Mysore. He had his graduation in siddaganga institute of technology, Tumkur. He was the former secretary of IEEE student branch during his graduation. He has published "Robust and auto-configurable network service framework For Airborne Network" in international journal of computer science and information technology research.

Dr. T.H.Sreenivas is an professor in dept of information science and engineering in NIE college,mysore. He has joined NIE ON 4/6/1983. He has pursued his BE IN Electronics and communication with FCD from UOM university. He has completed his M.Tech in CSE with cgpa of 8 in IIT Kanpur in the year 1986. He was the HID of MCA/ IS/CS for 3 years in NIE. He was the DEAN(Development) in NIE for 3 years. He was the principal coordinator TEQUIO-I for 4 years in NIE. He has published international paper named Parallel simulated annealing algorithms in the year 1996. He has also published a book "Computer Fundamentals in the year 2004.