SYSFORE®

Overview of Azure Active Directory

PART 3

Sysfore Technologies is a leading Azure Accelerate Partner with Microsoft for South India and a prime enabler for Microsoft Azure adoption.

OVERVIEW OF AZURE ACTIVE DIRECTORY

Like most directory services, Azure Active Directory stores information about users and the organizations they belong to. It lets users log in, then supplies them with tokens they can present to applications to prove their identity. It also allows synchronizing user information with Windows Server Active Directory running on premises in your local network. While the mechanisms and data formats used by Azure Active Directory aren't identical with those used in Windows Server Active Directory, the functions it performs are quite similar.

It's important to understand that Azure Active Directory is designed primarily for and used by cloud applications. It can be used by applications running on Azure, for example, or on other cloud platforms. It's also used by Microsoft's own cloud applications, such as those in Office 365. If you want to extend your data center into the cloud using Azure Virtual Machines and Azure Virtual Network, however, Azure Active Directory isn't the right choice. Instead, you'll want to run Windows Server Active Directory in Virtual Machines.

To let applications access the information it contains, Azure Active Directory provides a REST API called Azure Active Directory Graph. This API lets applications running on any platform access directory objects and the relationships among them. For example, an authorized application might use this API to learn about a user, the groups he belongs to, and other information. Applications can also see relationships between users-their social graph-letting them work more intelligently with the connections among people.

Another capability of this service, Azure Active Directory Access Control, makes it easier for an application to accept identity information from Facebook, Google, Windows Live ID, and other popular identity providers. Rather than requiring the application to understand the diverse data formats and protocols used by each of these providers, Access Control translates all of them into a single common format. It also lets an application accept logins from one or more Active Directory domains. For example, a vendor providing a SaaS application might use Azure Active Directory Access Control to give users in each of its customer's single sign-on to the application.

Directory services are a core underpinning of on-premises computing. It shouldn't be surprising that they're also important in the cloud.

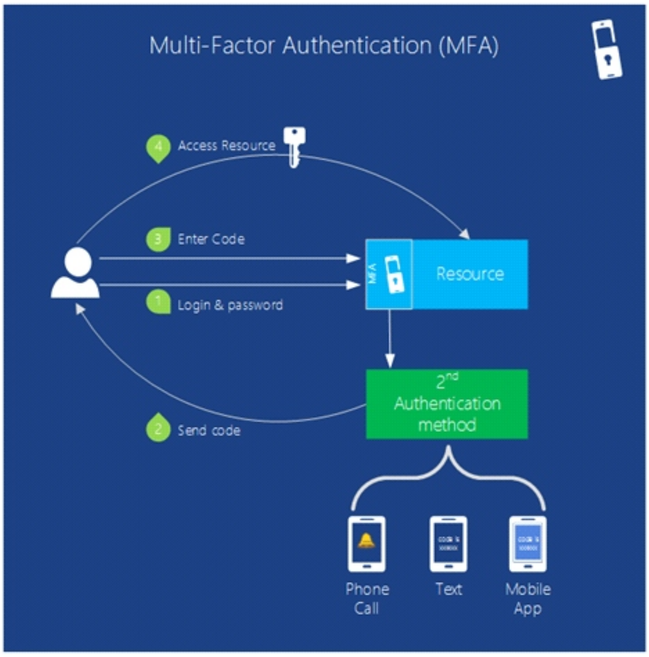

Figure: Multi-Factor Authentication provides the functionality for your application to verify more than one form of identification

Security is always important. Multi-factor authentication (MFA) helps insure that only users themselves access their accounts. MFA (also known as two-factor authentication or "2FA") requires users provide two of these three methods of identity verification for user sign-ins and transactions.

- □ Something you know (typically a password)
- □ Something you have (a trusted device that is not easily duplicated, like a phone)
- □ Something you are (biometrics)

So when a user signs in, you can require them to also verify their identity with a mobile app, a phone call or a text message in combination with their password. By default, Azure Active Directory supports the use of passwords as its only authentication method for user sign-ins. You can use MFA together with Azure AD or with custom applications and directories by using the MFA SDK. You can also use it together with on-premises applications by using Multi-Factor Authentication Server

Multi Factor Authentication Scenarios

Login protection on sensitive accounts such as bank logins and source code access where unauthorized entry could have a high financial or intellectual property cost.

Active Directory Benefits

The introduction of Active Directory in the Windows 2000 operating system provides the following benefits:

□ **Integration with DNS.** Active Directory uses the Domain Name System (DNS). DNS is an Internet standard service that translates human-readable computer names (such as mycomputer.microsoft.com) to computer-readable numeric Internet Protocol (IP) addresses (four numbers separated by periods). This lets processes running on computers in TCP/IP networks identify and connect to one another.

□ **Flexible querying.** Users and administrators can use the **Search** command on the Start menu, the **My Network Places** icon on the desktop, or the Active Directory Users and Computers snap-in to quickly find an object on the network using object properties. For example, you can find a user by first name, last name, e-mail name, office location, or other properties of that person's user account. Finding information is optimized by use of the global catalog.

□ **Extensibility.** Active Directory is extensible, which means that administrators can add new classes of objects to the schema and can add new attributes to existing classes of objects. The schema contains a definition of each object class, and each object class's attributes, that can be stored in the directory. For example, you could add a Purchase Authority attribute to the User object and then store each user's purchase authority limit as part of the user's account.

□ **Policy-based administration.** Group Policies are configuration settings applied to computers or users as they are initialized. All Group Policy settings are contained in Group Policy Objects (GPOs) applied to Active Directory sites, domains, or organizational units. GPO settings determine access to directory objects and domain resources, what domain resources (such as applications) are available to users, and how these domain resources are configured for use.

□ **Scalability.** Active Directory includes one or more domains, each with one or more domain controllers, enabling you to scale the directory to meet any network requirements. Multiple domains can be combined into a domain tree and multiple domain trees can be combined into a forest. In the simplest structure, a single-domain network is simultaneously a single tree and a single forest.

□ **Information Replication.** Active Directory uses multimaster replication, which lets you update the directory at any domain controller. Deploying multiple domain controllers in one domain provides fault tolerance and load balancing. If one domain controller within a domain slows, stops, or fails, other domain controllers within the same domain can provide necessary directory access, since they contain the same directory data.

□ **Information security.** Management of user authentication and access control, both fully integrated with Active Directory, are key security features in the Windows 2000 operating system. Active Directory centralizes authentication. Access control can be defined not only on each object in the directory, but also on each property of each object. In addition, Active Directory provides both the store and the scope of application for security policies. (For more about Active Directory logon authentication and access control, see the "For More Information" section at the end of this paper.)

□ **Interoperability.** Because Active Directory is based on standard directory access protocols, such as Lightweight Directory Access Protocol (LDAP), it can interoperate with other directory services employing these protocols. Several application programming interfaces (APIs) such as Active Directory Service Interfaces (ADSI)give developers access to these protocols.

For a need based free consultation, please write to us on Info@sysfore.com