Penn State Windows Active Directory services

Overview

Information Technology Services (ITS) provides a Windows Active Directory® Forest [ACCESS.PSU.EDU] for use by the entire University community that leverages the open standards-based Digital Credential Management. Any Penn State organization can use our core authentication (Kerberos V) and authorization (LDAP) services for account management.

Our goal is to provide the University community with maximum flexibility and control over their own Microsoft Active Directory® infrastructures. Through the use of child domains or organizational units (OUs), ACCESS.PSU.EDU allows for operational autonomy for participating Penn State units. It is a stable environment based upon Microsoft® supported technologies. Current participants include many of Penn State's campuses, colleges, and departments.

The Windows Active Directory® Team has developed a set of policies and guidelines related to this service in compliance with University policy. Information about this and other Windows® services related to Active Directory® can be found at the Penn State Windows® Active Directory website.

Technical Details

There are three key areas that where our Penn State deployment of Microsoft Active Directory® services is different from a typical Microsoft-centric environment:

1. Authentication:

Penn State AccessIDs authenticate to an external MIT Kerberos v5 realm (dce.psu.edu). Our AccessID passwords are only stored in that external (dce.psu.edu) realm on those KDCs. There is no syncing of passwords to our Active Directory forest from ACCESS.PSU.EDU. Logins with AccessIDs and passwords are made possible by the use of "shadow accounts" in Active Directory. Shadow accounts are simply user accounts created in ACCESS.PSU.EDU that are mapped to our MIT realm (dce.psu.edu) for authentication by means of a one-way trust between our forest ACCESS.PSU.EDU and the external realm (dce.psu.edu).

Therefore, NTLM authentication which relies upon a lookup comparison of a hash of the user account password kept in Active Directory services will not work in our environment. Any services we deploy must be able to operate using Kerberos authentication without referring to an NTLM lookup at any point.

2. Authorization:

Penn State's authoritative source for directory services information is located within an Open Standards compliant LDAP directory service. Some key fields of information Penn State

keeps in LDAP services (LDAP.PSU.EDU) are synched with user shadow accounts in our Active Directory. This includes group information and membership which is also synced to Global Security groups in our forest, ACCESS.PSU.EDU.

3. DNS:

Penn State deploys centralized DNS services running BIND on UNIX for all production systems. The forest was named ACCESS.PSU.EDU in order for this implementation of Active Directory to be compliant with Penn State's DNS naming policy. As a result, the forest name does not match the DNS suffix assigned to machines in this forest. This is known as a Disjoint DNS implementation which is a known and supported configuration of Microsoft Active Directory® services. (Note: this deployment is not described by a Split-Brain DNS implementation.)

Therefore, every client, member server and child domain in our forest are joined to an Active Directory domain name that does not match their own Fully Qualified Domain Names (FQDNs) in DNS. For example, the parent domain controllers for the forest ACCESS.PSU.EDU are hosted on the aset.psu.edu subdomain in DNS.

To support this configuration the NS records for the six Forward Lookup Zones for Active Directory Services are registered on Penn State's external BIND DNS servers. These NS records point to the respective domain controllers for the parent and child domains in this forest as follows (_msdcs; _sites; _tcp; _udp; DomainDnsZones; and ForestDnsZones).

Microsoft Services Dependencies

Microsoft services predominantly rely upon Kerberos authentication, however we have noted instances where there is not automatic support for Kerberos and authentication reverts to NTLM. Therefore, when configuring services on member servers it is critical to properly configure the following dependencies:

1. *Time*: set up time services,
2. *Networking*: register host names (A and PTR records) and configure networking services properly on each machine,
3. *Service Principal Name*: set up the appropriate SPNs since Microsoft services cannot use Kerberos authentication properly without them"

More Details Available

For more detail about our implementation of Active Directory refer to our documentation at: Penn State Active Directory and our forest design information at: Forest Design.