IOWA STATE UNIVERSITY
IT Services Technical Notes

Windows Enterprise
OU Administrator Tips
Authentication Issues Relating to LANMAN and NTLMv1

August 28, 2008
Revision 5

On August 13, 2008, IT Services enabled a domain policy on the Windows Enterprise Domain that requires NTLMv2 or Kerberos authentication. LANMAN and NTLMv1 (older insecure protocols) are no longer allowed for authentication to the domain controllers. This change can cause issues for existing systems. The following is a list of issues and resolutions (where available) IT Services has been made aware of so far. If you have additions/corrections to add to this document please send them to skunz@iastate.edu ASAP.

Windows-Enterprise-Domain Windows Systems Accessing Enterprise Domain Resources

When a Windows system that is a member of the Windows Enterprise Domain has trouble authenticating to domain resources it is generally due to Windows policy issues. The Enterprise domain policy is set to cause member systems to have the “LAN Manager Authentication level” policy set to “Send NTLMv2 response only\Refuse LM & NTLM”. However, OU policy (set by an OU admin) MAY override this. See the section “Policy Precedence**”** and “Other Useful Links” at the end of this document for more information.

Non-Enterprise-Domain Windows Systems Accessing Enterprise Domain Resources

When a Windows system that is NOT a member of the Windows Enterprise Domain has trouble authenticating to domain resources it is generally due to Windows policy issues. However, in this case it depends if the system is a member of ANY domain (or simply a “standalone” Windows system accessing resources on a domain).

In the case of a “standalone” system, the fix is relatively easy. The “Local Computer Policy” should be set as follows (assuming the system is running Windows XP Professional Service Pack 2):

1) Use “Start->Run” and type in “gpedit.msc” in the “Run” dialog box. A “Group Policy” window will open.
2) Click down to “Local Computer Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.
3) Find the policy “Network Security: LAN Manager authentication level”. Right click on this policy and choose “Properties”. Choose “Send NTLMv2 response only/refuse LM & NTLM”. Click OK and confirm the setting change.
4) Close the “Group Policy” window.

In the case of a “non-Enterprise domain” domain member, policy applied in the external domain the computer resides in MAY apply to the Windows system. In this case the policy applied in the external domain needs to be examined to determine the final policy applied when the system connects to the Enterprise domain. See the section “Policy Precedence**” ”** and “Other Useful Links” at the end of this document for more information.

Microsoft Exchange 2003 (Dept. Exchange Server, Member of Enterprise Domain)

For POP3 and IMAP4 to work properly it is necessary to disable "Simple Authentication and security layer" as that will only do NTLMv1 and all systems tested seem to default to that if it is available. Tested with Eudora, Thunderbird, Mozilla (old suite that included email), and Outlook (in non-Exchange mode).

Microsoft Failover Cluster and Mac OS X Clients (Windows Server 2003)

Connections from Mac OS X client systems to a Windows Server 2003 multi-node failover cluster server cannot authenticate. This is because port 137 on the cluster server does not expose the domain like port 137 on the individual nodes do. The Macintosh OS X operating system need the domain information on port 137 (see “Samba (RedHat Linux and Others) and Mac OS X Clients**”** elsewhere in this document). A workaround is to point the Mac OS X client to one of the cluster nodes (not the cluster server itself).

Microsoft IIS and Firefox

Connections to Windows Enterprise Domain member IIS servers from systems using "Firefox" may prompt for credentials, fail, require an "escape key" abort, which results in a second clear text authentication prompt that works successfully.

To fix this, you may be able to configure Microsoft IIS to "Negotiate" (not "Negotiate,NTLM"). See "How to configure IIS to support both the Kerberos protocol and the NTLM protocol for network authentication" (http://support.microsoft.com/kb/215383).

Turning off NTLM in IIS (with adsutil.vbs) and enabling "Integrated Windows Authentication" (see below) in IIS seems to continue to allow IE to logon properly, whether logged into the domain or not. Firefox may be able to perform an integrated logon if you turn on "Network.Negotiate ..." and you are logged onto the domain. Firefox may also be able to do a "clear text" login smoothly with "Network.Negotiate-..." off without having to press the Escape key. Caution: Having an SSL certificate is critical when “clear text” authentication is used!

Some Firefox settings on client systems may be desirable. Setting the “network.negotiate-auth.trusted-uris” preference in Firefox (via "about:config") allows automatic login without a prompt in Firefox on Windows. The setting does not have to be a specific URL -- it can be a portion, so you can enable automatic login to *any* iastate.edu web server by entering "iastate.edu" for the value. For accessing an intranet from on campus (which is presumably the only way this will work), you not need to add anything to “network.negotiate-auth.delegation-uris”.

Changing the Integrated Windows Authentication in Microsoft IIS (Windows 2003): Use “Control Panel,->Administrative Tools->IIS Manager” and navigate to the Site or Folder you want to change. Right-click your selection and select “Properties” and then the Directory Security tab->Authentication and Access Control->Edit. Check/uncheck Integrated Windows Authentication.

Microsoft SharePoint Services

[In Progress]

Microsoft VPN Server

If you run a Microsoft VPN server and you can no longer authenticate, the following article may help:

http://support.microsoft.com/kb/893318/en-us

Samba (RedHat Linux and Others) and Mac OS X Clients

If you run a Linux Samba server that is a member of the Enterprise Windows domain you may have problems connecting with Mac OS X clients based on firewall issues. Check to make sure port 137 is getting through from your server to your clients. Check the “iptables” Linux firewall settings (or any other firewall). Mac OS X requires port 137 on your server to get the domain membership of the server for authentication.

Samba – General Issues

- If you are using Samba on a Linux/*BSD/UNIX client to use tools such as “smbclient” and “smbacls”, you will need to tell your client to use NTLMv2 auth (unless you're using Kerberos authentication, of course). In the file /etc/samba/smb.conf on the client, you should add the following to the “[globals]” section:

  ```
  client ntlmv2 auth = yes
  ```

- To mount Windows 2003 server from RedHat 5 Linux:

  mount point: ~/server224-share58
  server name: server224
  share name: share58
  username: user873

  Previously this was all that was required:

  ```
  mkdir ~/server224-share58
  sudo /sbin/mount.cifs //server224/share58 ~/server224-share58 -o
  username=user873,domain=IASTATE
  ```

Now with NTLMv2 authentication:

```
mkdir ~/server224-share58
sudo /sbin/mount.cifs //server224/share58 ~/server224-share58 -o
username=user873,domain=IASTATE,sec=ntlmv2
```

Mount commands in RHEL require administrator permission, hence the “sudo" requirement

Scanners that Scan to Windows Files

Modern scanning devices can often be configured to deposit scans on a Windows system. Unfortunately, some devices capable of doing this use LANMAN or NTLMv1 and the manufacturer sees no reason to upgrade to modern secure authentication protocols. Two examples are the Ricoh Aficio MP C4500 and the Lanier LD425c. There is a workaround to this problem which involves forcing lower security for scanner-to-system file transmission.

The solution is to put the target workstation/server (which is a member of the Windows Enterprise Domain) in a special departmental OU and applying a special security policy to the OU. This policy should have the “Network Security: LAN Manager Authentication level” set to "Send LM & NTLM - use NTLMv2 session security if negotiated". See the section “Policy Precedence**”** section at the end of this document for more information on applying group policy.

Next, create a local system account on the target domain-member system and configure the scanner to use that account to deposit files into the system folder. If the format of the login account (on the scanner) is prefaced with a domain or hostname it may need to be changed to "<hostname>\<username>" (as opposed to "IASTATE\<username>). Refer to your scanner setup instructions for proper format.

The scanner will now use LANMAN or NTLMv1 for scanner-to-system authentication. Domain-account users can access the files on that server from the folder they are dropped into with normal (secure) domain authentication.

Policy Precedence

The order in which group policy applies is “group policy precedence”. Group policy is applied in the following order:

1. Local computer policy (set by the “Local Security Policy” administrative tool by a local system admin)
2. Site policy (Iowa State has no site policy for the Enterprise domain applied)
3. Domain policy (set by the Enterprise Domain Admins)
4. OU policy (set by your Enterprise Domain OU manager)

The Windows Enterprise domain policy that relates to authentication protocols is set as follows:

Default Domain Policy
  Windows Settings
    Security Settings
      Local Policies
        Security Options
          Network Security: LAN Manager Authentication level =
            Send NTLMv2 response only\Refuse LM & NTLM

The above setting ("LAN Manager Authentication level=Send NTLMv2 response only\Refuse LM & NTLM") is the required policy setting. Note that:

- An OU manager can override this with OU policy.
- Non-domain-member systems (standalone home systems, for example) will not have OU or domain policy applied, therefore they must change the default "local computer policy" to the "Send NTLMv2 response only" setting. The default is "Send LM & NTLM responses" which will not work in our environment.
- Windows systems that are members of domains other than the Enterprise domain must take into account that domains Site/Domain/OU policies to determine what setting is applied and correct the final policy applied.

Other Useful Links

Indiana University: "How can I use the local security settings to force NTLMv2?"
http://kb.iu.edu/data/atcb.html

California Institute of Technology (CALTECH): "Enabling NTLMv2 on Windows XP Home Computers"
http://imss.caltech.edu/cms.php?op=wiki&wiki_op=view&id=397

Microsoft MSDN: Security Briefs: Credentials and Delegation
http://msdn.microsoft.com/en-us/magazine/cc163740.aspx

Contributors

Thanks to all the following for their contributions:

Stephanie Bridges [ECONA]
Nicholas Burdine [CTRE]
Greg Buttery [BUS]
John Dickerson [ECSS]
Stephen Heideman [CHEM]
Mike Long [CARD]
Brent Moore [ECONA]
David Orman [CNDE]