Windows Administrators Meeting
August 12, 2011
Notes (taken by Steve Kunz [ITSYS] and Mike Lohrbach [ITSYS])

Meeting Started (9:00)

Announcements

- **Digital Certificates for LDAPS:** Steve Kunz [ITSYS] mentioned that the conversion of providers for the digital certificates on the enterprise domain controllers was completed August 8, 2011. These certificates support LDAPS connections to the domain controllers. More details are available here: http://www.tech.its.iastate.edu/windows/admin/Announce.2011.05.27.pdf
- **CyFiles:** Steve Kunz [ITSYS] reminded everyone that CyFiles is in full production mode. CyFiles provides every domain user with a 5 GB (default) home directory mapped to the "U:" drive letter and roaming profile storage. The official CyFiles information page is: http://it.iastate.edu/services/storage/cyfiles

Advanced Group Policy Management - AGPM [Mike Lohrbach - ITSYS]

Mike Lohrbach [ITSYS] talked about Microsoft's "Advanced Group Policy Management" product. AGPM is one component of the "Microsoft Desktop Optimization Pack" (MDOP). MDOP is a collection of tools targeted on improving desktop management. The components are:

Microsoft Bitlocker Administration and Monitoring (MBAM).

- Provides compliance and reporting insight into how compliant your organization is with your defined BitLocker encryption policies.
- Secure web page to easily get recovery keys.
- Standard users can start the encryption process or change their PIN without calling support.
- Windows 7 only with a TPM module installed.

Microsoft Diagnostic and Recovery Toolkit 7 (DaRT)

- A set of tools to help easily recover unusable PCs, rapidly diagnose probable causes of issues, and quickly repair unbootable or locked-out systems.
- Flexible deployment options like booting into DaRT from the network and the ability to remote control a DaRT session.

Asset Inventory Service (AIS)

- A cloud based asset management service that helps you translate your inventory data into actionable information.
- This update to AIS provided detailed hardware information on the computers in your inventory, software reports that aggregate products by major and minor versions, support for inventorying of Microsoft Application Virtualization (App-V) applications, and is localized in eleven languages with support up to 100,000 clients per account

Application Virtualization (App-V)

- Turns applications into centrally managed services that are never installed, never conflict, and are streamed on demand.

Microsoft Enterprise Desktop Virtualization (MED-V)

- Provides deployment and management of virtual PC images.

Microsoft Advanced Group Policy Management (AGPM)

- Provides governance and control over group policy through change management and role based administration

Advanced Group Policy Management has several features as follows:

1) Offline editing (changes can be made outside of the production environment allowing you to test without impacting production systems)

2) GPMC integration (requires a server to be setup and then admins wishing to use AGPM need to install a client)

3) Change Control
   - Check out the GPO from the archive.
   - Edit the GPO as necessary.
   - Check in the GPO to the archive.
   - Deploy the GPO to production.
   - Deploy any version of a GPO.
   - Compare multiple versions of a GPO.
   - Role-Based Delegation (role-based delegation model that adds a review and approval step to the workflow). Roles are:
     - **Administrator** has full control of the AGPM archive.
     - **Reviewer** can view and compare GPOs. They cannot edit or deploy GPOs.
     - **Editor** can view and compare GPOs. They can also check out GPOs from the archive, edit GPOs, and check in GPOs to the archive. Editors can request deployment of a GPO.
     - **Approver** can approve the creation and deployment of GPOs. (When Approvers create or deploy a GPO, approval is automatic.)

4) Search and Filter
   - Supports complex search strings using the format *column*: *string*, where *column* is the name of the column by which to search and *string* is the string to match.
   - For example, to display GPOs that were checked in by Jerry, type **state: "checked in" changed by: Jerry** in the search box.
   - Filter the list by GPO attributes by using the format *attribute*:*string*, where *attribute* is the name of the GPO attribute to match.

- To display all GPOs that use the Windows Management Instrumentation (WMI) filter called MyWMIFilter, type **wmi filter: mywmifilter** in the search box.

MDOP Costs
- MDOP can be licensed through MCA at a department or university level.
- Cost via the MCA is $3 per FTE
- MDOP can also be purchased through TechCyte
- AGPM only needs to be licensed per admin

Resources
- MDOP: http://technet.microsoft.com/en-us/library/bb852167.aspx
- MDOP: http://technet.microsoft.com/en-us/windows/bb899442
- AGPM overview: http://technet.microsoft.com/en-us/library/ee532079.aspx

Questions/comments can be directed to Mike Lohrbach [ITSYS] (mlbach@iastate.edu) or Steve Kunz [ITSYS] (skunz@iastate.edu).

Password Settings Objects (PSOs) – Granular Password Policies

Steve Kunz [ITSYS] reviewed the work done on PSOs to allow OU managers to apply more restrictive password policies to specific users within their OU structure. He reviewed the core design and highlighted certain key features and points to remember. All of the information is included in the following ITS TechNote: http://www.tech.its.iastate.edu/windows/admin/PSO_HowTo.pdf
This page is also linked to from the main OU Administrator Support TechNote page at http://www.tech.its.iastate.edu/windows/admin/ouadmin.shtml in the "Actions Requiring Enterprise Admin Action" section.

Questions/comments can be directed to Steve Kunz [ITSYS] (skunz@iastate.edu).

Open Discussion

Questions were asked about the status of multi-casting issues. Mike Lohrbach said the networking folks are aware of the issues No ITS networking staff were present to directly address the issue.

A question was asked about PXE boot in our network environment. A partial answer was that PXE boot can be supported but the comment was made that not all request types were passed. No ITS networking/NetReg staff were present to directly address the issue.

Meeting Adjourned (9:50)

Next meeting is scheduled for September 9 (provided a sufficient agenda exists).