A policy service perspective on Delegated Directory Administration

Delegated Directory Administration

Scenario setup

The Enterprise AD Functions as the PIP

The following administrative groups are defined

- Dept-Chem-OU-Adm
- Dept-Bio-OU-Adm
- Mail-Service-Adm
- Core-AD-Adm

At the start, the membership in the groups are as follows

- Bill is a member of Dept-Chem-OU-Adm
- Patrick is a member of Core-AD-Adm

A member of the college-wide AD Adm staff uses the AD Management Console as a PAP to configure attribute acls in the PIP for user objects under each of the departmental OU's. The following ACL's are assigned

- Members of "Dept-Chem-OU-Adm" may only modify workstation, file service and print service attributes (i.e. "homeDirectory" and "homeDrive") in the Chemistry-OU
- Members of "Dept-Bio-OU-Adm" may modify workstation, file service and print service attributes (i.e. "homeDirectory" and "homeDrive") in the Biology-OU
- Members of "Mail-Service-Adm" may modify Exchange and PII attributes (i.e. "msExchgHomeServerName") in the entire AD
- "Core-Ad-Adm" retain full rights in the entire AD

Action 1 - File Move

The file servers "new-fs.chem.someuni.edu" and "full-fs.chem.someuni.edu" are both registered in the college AD. Any access management policy decisions for both servers use the college AD as a PDP. The "Dept-Chem-OU-Adm" AD Group has been given administrative rights on both file servers. Bill RDP's into "new-fs" and remotely mounts the file system on "full-fs" to perform the file copy of all the faculty with odd office numbers. The Microsoft shell acts as a PEP and verifies that Bill is a member of the "Dept-Chem-OU-Adm" AD Group and can thus RDP in, perform the file system mount, and file copies. Bill closes his RDP session after the file copies complete.

Action 2 - Updating Attributes

Bill now needs to update the "homeDirectory", "homeDrive", and "msExchgHomeServerName" attributes in the college AD for the affected faculty. He recorded a list of the UID's for the affected faculty and has written a Powershell script to update the attributes. When he invokes powershell.exe, it functions as a PEP and consults the college AD as appropriate the PDP to determine that Bill does not have policy rights to update "msExchgHomeServerName". The script returns an error. Bill modifies the script to send an individual email for each of the 537 changes to the Mail Service Admin list requesting an attribute update and re-runs the script. Powershell.exe performs the same PEP evaluation and this time completes with a success.

Action 3 - Incident Response

Prior to leaving for a cheese making trip in the Swiss Alps, Bill is having coffee with Patrick who works in the College AD admin group. Bill is complaining about the turf issue he has with the mail folks and the script that bombed. Patrick asks if he could get a copy of the script, Bill said sure and forwarded it on from his cell phone.

Shortly after Bill leaves, Patrick gets a call from the Chem department that many of the faculty cannot get to files. Investigation indicates "new-fs" is corrupt and must be restored to "shiny-fs".
After last nights backup of "new-fs" is restored to "shiny-fs", Patrick edits Bill's script to comment out the routine to email the Mail Service Admin list and restores the update of the "msExchgHomeServerName" attribute. When Patrick runs powershell.exe, the PEP evaluation is successful because Patrick has sufficient policy rights to update the needed attributes as defined by the PDP. The script completes successfully.

Action 4 - Bill Returns

Shortly after returning from his trip, Bill learns that the AD admin for the Bio department is retiring. Bill jumps at the chance to transfer to the home of the International Lactobacillus Institute. Patrick learns of Bill's transfer and uses the AD Administration console as a PAP to move Bill from the "Dept-Chem-OU-Adm" group to the "Dept-Bio-OU-Adm" group.

See Also

XACML Terminology and Data Flow Diagram