ST2612 Tutorial 4 (Week 12)

Self-evaluation Check list

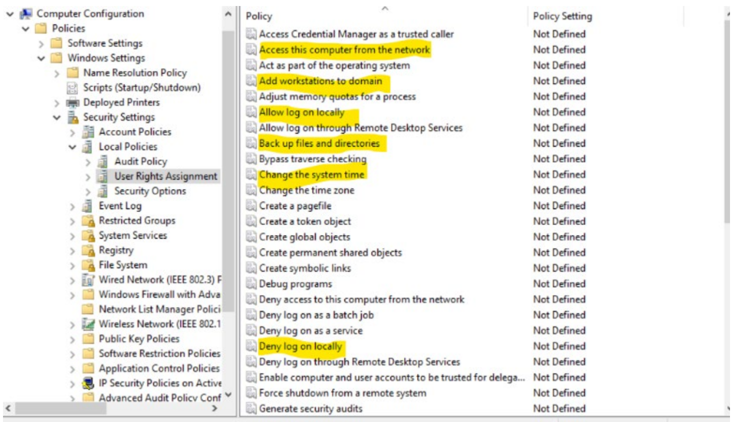
- Briefly explain how the GPO Enforced option affects the Group Policy Precedence.

  GPO Enforced option ensure the GPO will not be overridden by other GPO with a conflicting settings nor blocked by any containers. The only exception is GPO Enforced option may not override GPO that has applied earlier and it also has its Enforced option set to on.

- Briefly explain how the Group policy block inheritance works.

  Block inheritance is a container option. The container with this option will not apply GPOs that inherit from the parent containers. The only exception is, it cannot block GPOs with their Enforced option set to on.

- List 3 settings under the User Right Assignment Policies.



Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Not Defined
Act as part of the operating system	Not Defined
Add workstations to domain	Not Defined
Adjust memory quotas for a process	Not Defined
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Not Defined
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Not Defined
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delega...	Not Defined
Force shutdown from a remote system	Not Defined
Generate security audits	Not Defined

  (PS. The highlighted ones are expected to be known by our student.)

- How often the domain clients will get the updated Group Policies? Can we configure this settings? How?

  By default: Domain members GPO refresh interval is set at 90 minutes. With a random 0-30 minutes add on.

  By default: Domain controller GPO refresh interval is set at 5 minutes.

  We can configure the above two settings via Group Policy settings at:

  Computer Configuration > Policies > Administrative Templates > System > Group Policy.

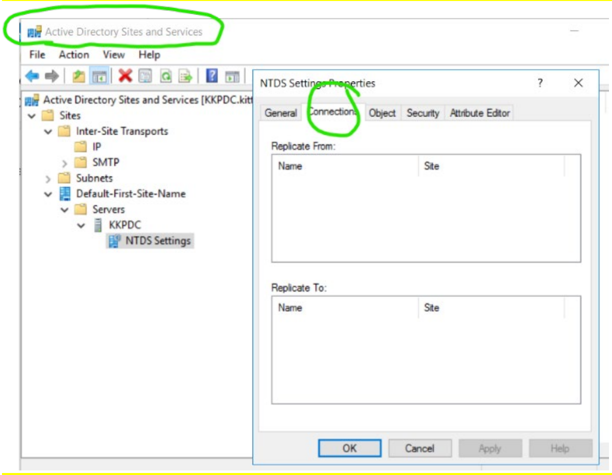
  Set Group Policy refresh interval for computers.

  Or

  Set Group Policy refresh interval for domain controller.

- How often the Domain Controllers will exchange/replicate updated Group Policies with each other? Can we configure this setting? How?

For replication between DCs which are residing in different sites:
By default: one hour.
In most of the case, the Administrators should set the interval.
The minimal interval is 15 minutes.
The setting can be carried out at the Active Directory Sites and Services Snap-in.



For domain controllers are residing in the same site. The replication time is much shorter. Usually is within 5 minutes, and it does not require any particular settings.

- Describe how you can check / view the current active/effective GPOs applied to a client machine.

  We can use the GPRESULT /R /V command at the client machine.

  Or we can use the RSoP feature at the Group Policy Management Console (GPMC) if the remote access setting is configured properly.

- The following is a question of ST2612 EXAM in AY2019/2020 S2. Try to answer it.

  List three possible events that can trigger the process of applying the Computer Configuration Settings of a GPO to a specific domain workstation. (6 marks)

  1. System Reboot.
  2. When the time is due for the refresh (default every 90 minutes + (random time)
  3. User running GPUPDATE command at the local workstation.
  4. When a user logon to the local workstation and the GPO has loopback option turned on.

- In terms of security patch management, list the possible outcomes of a risk evaluation process of a new security patch.

1. Not apply the security patch and do nothing
   as the party is willing to take the risk.
   Or the security patch is not relevant to the target system.
2. Apply a mitigation measure as a short term solution for now.
   Will apply the patch in the next schedule patching time.
3. Plan to apply the security patch ASAP.
   May or may not apply a mitigation measure.

- Which type of the following vulnerabilities may cause more damage to an organization: The one with the Critical severity rating or the one with the important severity rating?

  Vulnerabilities with Critical severity rating may cause more damage as the exploits may propagate to external parties. Since it may involve any number and any types of external parties, the actual damage to the organization may go out of the expectation. Compare to Important severity rating vulnerabilities, the damage only occurs internally.

- In your opinion, what is the most important testing criterion for a new patch?

  Able to rollback.

  Able to restart the system.

  Not affecting mission critical applications.

  (Anyone of the above or other acceptable answers)

- List 3 possible costs that should be factored in to the patch management operations.

  The manpower to deploy the patch.

  The resource to facilitate the pathc.

  The system down time during the patch operation.

  Possible recovery cost if the patch operation is failed.

  The manpower to test the patch.

  The resource to facilitate the testing.

  (Any three of the above or other acceptable answers)

- Identify the security advantages for using WSUS-like centralized windows update services for an Enterprise Network.

  Centralized system can help monitoring the overall update services status.

  Enable offline (to Internet) systems to receive security updates.

  Possible to bring more systems go offline (to Internet) to reduce their attack surfaces.

  Minimize the security risk of offering a single source of update services.

  Let professionals to handle/troubleshoot update issues to avoid foul play.

- Briefly describe two scenarios that the patch management manager would decide not to deploy a security patch (with the critical severity rating) to a mission critical production server.

  1. Not apply the security patch as the security patch is not relevant to the target system.
  2. Apply a mitigation measure as a short term solution for now as the cost to bring down the mission critical production server is too high.

~ That's all ~