Security Mechanisms in OS Windows

Contents

Group Policy

Group Policy is an infrastructure that allows you to specify managed configurations for users and computers through Group Policy settings and Group Policy Preferences. To secure Group Policy settings that affect only a local computer or user, you can use the Local Group Policy Editor `gpedit.msc`. You can secure Group Policy settings and Group Policy Preferences in an Active Directory Domain Services (AD DS) environment centrally through the Group Policy Management Console (GPMC) `gpmgmnt.msc`. Both options can be combined, i.e. some policies can be applied from the domain and other form local policy. However, domain policies have priority.

Administrators need to be able to quickly modify Group Policy settings for multiple users and computers throughout a network environment. The Local Group Policy Editor provides administrators with a hierarchical tree structure for configuring Group Policy settings in GPOs. These GPOs can then be linked to sites, domains, and organizational units (OU) that contain computer or user objects.

The principle of the majority of group policies that are used to modify operating system settings is based on editing values in Windows Registry. For illustration, let us consider Windows 10 that is not added to a domain. Policy definition files of type ADMX are stored in the location `%SystemRoot%\PolicyDefinitions\`. Structure of this file is illustrated in the Figure 1. A property text that can be translated into different language mutations (`dispalyname`) has an information about Windows Registry path that should be changed saved in field `key`.

```
<policy name="HostToRealm" class="Machine"
displayName="$(string.hosttorealm)"
explainText="$(string.hosttorealm_explain)"
presentation="$(presentation.hosttorealm)"
key="Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos"
valueName="domain_realm_Enabled">
      <parentCategory ref="kerberos" />
      <supportedOn ref="windows:SUPPORTED_WindowsVista" />
      <elements>
        <list id="hosttorealm"
key="Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\dom
ain_realm" additive="true" explicitValue="true" />
      </elements>
    </policy>
```

Figure 1 – Selection from group policy definition file

Computer Management

Computer Management is a collection of Windows administrative tools that you can use to manage a local or remote computer. The administrative tools in Computer Management are grouped into the following three categories in the console tree:

- System Tools
- Storage
- Services and Applications

System Tools

- Event Viewer – management and viewing of events that are recorded in the logs.
- Shared Folders – creating, viewing, and management of shares.
- Local Users and Groups – creating and managing local user accounts and groups.
- Performance – monitoring performance and state of the computer.
- Device Manager – management of hardware devices installed in the computer.

Storage

- Removable storage – management of removable storage media.
- Disk Defragmenter – analysis and defragmentation of volumes on the hard disks.
- Disk Management – operations related to disks management.

Services and Applications

- Services – management of services on local and remote computers.
- WMI Control – Windows Management Instrumentation (WMI) configuration.

Server Manager

Server Manager is a management console in Windows Server that helps IT professionals provision and manage both local and remote Windows-based servers.

NTFS Permissions

Every container and object on the network has a set of access control information attached to it. Known as a security descriptor, this information controls the type of access allowed to users and groups. Permissions are defined within an object's security descriptor. Permissions are associated with, or assigned to, specific users and groups.

When you are a member of a security group that is associated with an object, you have some ability to manage the permissions on that object. For those objects you own, you have full control. You can use different methods, such as Active Directory Domain Services (AD DS), Group Policy, or access control lists, to manage different types of objects.

Access can be controlled on the file and folder level. Basic permissions that are predefined in Windows operating systems are the following: full access, modify, read & execute, list folder contents, read, write. Special permissions are summarized in the Table 1.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Table 1 – Combinations of data access permissions

Windows Firewall

In an enterprise network, server and workstation firewall can be considered the last line of defence (if we are considering Defense-In-Depth model).

Windows Firewall with Advanced Security combines a host firewall and IPsec. Unlike a perimeter firewall, Windows Firewall with Advanced Security runs on each computer running this version of Windows and provides local protection from network attacks that might pass through your perimeter network or originate inside your organization. It also provides computer-to-computer connection security that allows you to require authentication and data protection for communications.

In practice, there are multiple services running on a Windows Serveri in an enterprise environment: DNS, LDAP – to support Active Directory service, possibly DHCP service.

From a user's point of view, it is necessary to create exceptions for certain applications that will be allowed by Windows Firewall to communicate on the network.

References

Administrative Tools

https://docs.microsoft.com/en-us/windows/client-management/administrative-tools-in-windows-10

Server Manager

https://docs.microsoft.com/en-us/windows-server/administration/server-manager/server-manager

Windows Security

https://docs.microsoft.com/en-us/windows/security/

Windows Server Security

https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance

Windows Server 2008 Documentation

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc772323(v=ws.10)

Windows Server 2012 Documentation

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh801901(v=ws.11)

Firewall Best Practice

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

M. Pavelka: KOMPLEXNÝ NÁSTROJ NA AUTOMATIZOVANÉ ZABEZPEČOVANIE OPERAČNÉHO SYSTÉMU VO FIREMNOM PROSTREDÍ. Bachelor thesis. FIIT STU, 2021.