**1. Contexts within Windows Administration**

User Context

Executes with the permissions of the logged-in user.

Used for operations requiring access to user-specific files or registry (HKCU).

System Context

Runs with Local System account rights.

Often utilized by SCCM and task scheduler.

Can access system resources (HKLM).

Admin Context

Needs privileges with elevation.

Used when administrative rights are required for changes, such as system file modification or software installation.

**2. Logon Scripts**

Automatic scripts that execute during user logon.

Usual application to map drives, install printers, or define environment variables.

Set through Group Policy: User Configuration > Windows Settings > Scripts (Logon/Logoff).

**3. Active Setup within MS**

Mechanism to run per-user configuration on first logon.

Utilizes registry keys:

HKLM\\SOFTWARE\\Microsoft\\Active Setup\\Installed Components\\{GUID}

Includes command and version.

When new user logs on, Windows compares HKCU key. In case missing or version does not match, executes the command.

**4. Windows 10 & 11 Advantages**

Windows 10

Familiar UI with extensive compatibility.

Strong business support.

Windows 11

New UI and productivity features.

Improved performance and security.

Native hardware support for newer hardware (e.g., TPM 2.0).

**5. Application Packaging Considerations**

Determine whether the app is per-user or per-machine.

Support multiple versions of Windows.

Process prerequisites (e.g., .NET, Visual C++ runtimes).

Use Active Setup or logon scripts for per-user setup.

Test in all applicable contexts (User/System/Admin).

**6. Processing Scheduled Tasks**

Used for automation and execution at specified times or events.

Created through Task Scheduler or programmatically (e.g., schtasks.exe).

Can execute under user or system accounts.

Set up appropriate permissions and triggers.

**7. Sysinternals Debugging Tools**

Autologon

Sets up auto-login for a user account.

Process Explorer

Advanced task manager; displays parent-child relationships, open handles, etc.

PsExec

Runs commands remotely or under alternate contexts.

PsTools

Suite containing PsExec, PsKill, PsList, etc., for remote administration.

RegMon (replaced by Process Monitor)

Used to monitor registry changes.

SysMon

System activity monitor that writes to Event Viewer.

Whois

Retrieves domain registration information.

**8. Active Setup Versioning During Fresh Install**

Version string in Active Setup registry key controls whether the stub runs.

If version changes or HKCU key is absent, the setup command runs.

Assists in applying updated settings for new or new users.

**9. HKLM vs HKCU in Registry**

**HKLM** (HKEY\_LOCAL\_MACHINE)

Machine-wide settings.

Impacts all users.

Requires admin rights to change.

**HKCU** (HKEY\_CURRENT\_USER)

User-specific settings.

Only impacts the current user.

Updated through logon scripts or Active Setup.