**Sessions in Windows**

Session 0 Isolation:

During start-up, a windows session is created for the system processes to run which are not related to a specific user, this is called session 0.this session allows windows to run system processes needed for machine itself.

When a user log on to that machine a new session is created called User Session in which user-specific services run.

Background process from an Attended robots run in user’s session 1 and un attended in 0.

thumbnail image 1 of blog post titled 
 
 
  
 
 
 
    
  
   
    
      
       Sessions, Desktops and Windows Stations
       
      
     
   
  
 
   
 
 
 
 
 


Session 0 in Windows XP / Windows Server 2003

thumbnail image 2 of blog post titled 
 
 
  
 
 
 
    
  
   
    
      
       Sessions, Desktops and Windows Stations
       
      
     
   
  
 
   
 
 
 
 
 


Session 0 / Session 1 in Windows Vista

A session consists of all of the processes and other system objects that represent a single user’s logon session.  These objects include all windows, desktops and windows stations.  A desktop is a session-specific paged pool area and loads in the kernel memory space.  This area is where session-private GUI objects are allocated from.  A windows station is basically a security boundary to contain desktops and processes.  So, a session may contain more than one Windows Station and each windows station can have multiple desktops.

A window station is a securable object that is associated with a process, and contains a clipboard, an atom table, and one or more desktop objects.

A desktop is a securable object contained within a window station. A desktop has a logical display surface and contains user interface objects such as windows, menus, and hooks.

The Default desktop is created when Winlogon starts the initial process as the logged-on user. At that point, the Default desktop becomes active, and it is used to interact with the user.

Only one windows station is permitted to interact with the user at the console; this is called Winsta0. Under Winsta0 there are three desktops loaded:

* Winlogon (the logon screen),
* Default (the user desktop)
* Disconnect.

All three of these have separate logical displays, which is why your main desktop disappears if you lock the workstation.  When you lock the workstation, the display switches from Default to Winlogon and there is no user interaction between the two.

Session space is divided into four different areas:

* Session Structure – Memory management control structures including session Working Set List.
* Session Image Space – holds a private copy of Win32k.sys modified data, a single copy of Win32k.sys code and unmodified data and various session drivers.
* Session View Space – session mapped views including desktop heap
* Session Paged Pool – paged pool memory used for this session

Win32k.sys, also known as a **Full/Desktop Multi-User Win32 Driver file**

A single desktop object will have a single desktop heap set aside for it.  This heap stores various user interface objects, such as the windows, menus and hooks.  When an application needs to draw a user interface object, it calls User32.dll to allocate this object. As I am sure you can guess, each of these interface elements requires resources out of desktop heap.  If the desktop heap becomes depleted, you will get symptoms such as a corrupt display or other anomalies.

Every service process created under a user account will be given a new desktop in a "non-interactive" window station created by the Service Control Manager (SCM).

**User Accounts:**

Local user accounts:

Local user accounts are stored locally on the server. These accounts can be assigned rights and permissions on a particular server, but on that server only. Local user accounts are security principals that are used to secure and manage access to the resources on a standalone or member server for services or users.

The default local user accounts, and the local user accounts that you create, are located in the Users folder. The Users folder is located in Local Users and Groups.

You can use Local Users and Groups to assign rights and permissions on the local server, and that server only, to limit the ability of local users and groups to perform certain actions.

An access permission is a rule that is associated with an object, usually a file, folder, or printer. It regulates which users can have access to an object on the server and in what manner.

**Administrator account**

The default local Administrator account is a user account for the system administrator. Every computer has an Administrator account. The Administrator account is the first account that is created during the Windows installation.

The Administrator account has full control of the files, directories, services, and other resources on the local computer. The Administrator account can create other local users, assign user rights, and assign permissions. The Administrator account can take control of local resources at any time simply by changing the user rights and permissions.

The default Administrator account cannot be deleted or locked out, but it can be renamed or disabled.

### Guest account

The Guest account is disabled by default on installation. The Guest account lets occasional or one-time users, who do not have an account on the computer, temporarily sign in to the local server or client computer with limited user rights. By default, the Guest account has a blank password. Because the Guest account can provide anonymous access, it is a security risk.

## **HelpAssistant account (installed with a Remote Assistance session)**

The HelpAssistant account is a default local account that is enabled when a Remote Assistance session is run. This account is automatically disabled when no Remote Assistance requests are pending.

HelpAssistant is the primary account that is used to establish a Remote Assistance session. The Remote Assistance session is used to connect to another computer running the Windows operating system, and it is initiated by invitation.

The HelpAssistant account is managed by the Remote Desktop Help Session Manager service.

### DefaultAccount

The DefaultAccount, also known as the Default System Managed Account (DSMA), is a built-in account introduced in Windows 10 version 1607 and Windows Server 2016. The DSMA is a well-known user account type. It is a user neutral account that can be used to run processes that are either multi-user aware or user-agnostic.

the DefaultAccount is a standard user account. The DefaultAccount is needed to run multi-user-manifested-apps (MUMA apps). MUMA apps run all the time and react to users signing in and signing out of the devices. Unlike Windows Desktop where apps run in context of the user and get terminated when the user signs off, MUMA apps run by using the DSMA.

## **Default local system accounts**

**SYSTEM**

The SYSTEM account is used by the operating system and by services that run under Windows. There are many services and processes in the Windows operating system that need the capability to sign in internally, such as during a Windows installation. The SYSTEM account was designed for that purpose, and Windows manages the SYSTEM account’s user rights. It is an internal account that does not show up in User Manager, and it cannot be added to any groups.

**NETWORK SERVICE**

The NETWORK SERVICE account is a predefined local account used by the service control manager (SCM). A service that runs in the context of the NETWORK SERVICE account presents the computer's credentials to remote servers.

By default, the remote token contains SIDs for the Everyone and Authenticated Users groups. The user SID is created from the SECURITY\_NETWORK\_SERVICE\_RID value.

**LOCAL SERVICE**

The LOCAL SERVICE account is a predefined local account used by the service control manager. It has minimum privileges on the local computer and presents anonymous credentials on the network.

**Active Directory:**

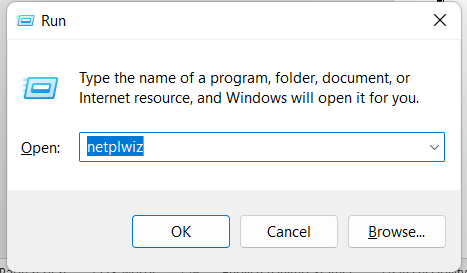
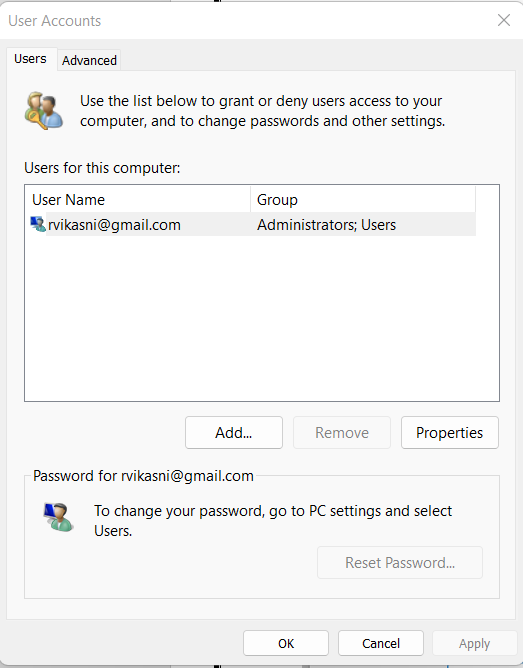
It runs on Windows Server and enables administrators to manage permissions and access to network resources.

Active Directory stores data as objects. An object is a single element, such as a user, group, application or device such as a printer. Objects are normally defined as either resources, such as printers or computers, or security principals, such as users or groups.

The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource, as well as group policies.

**process creation on different user account(token extraction) using c++.**

**Creating new user:**

**** **** 