Windows Access Control List (ACL) 5

What do we have in this session?

1. More on SID Strings
2. More on SID Components
3. Well-known SIDs

The expected abilities that supposed to be acquired in this session are:

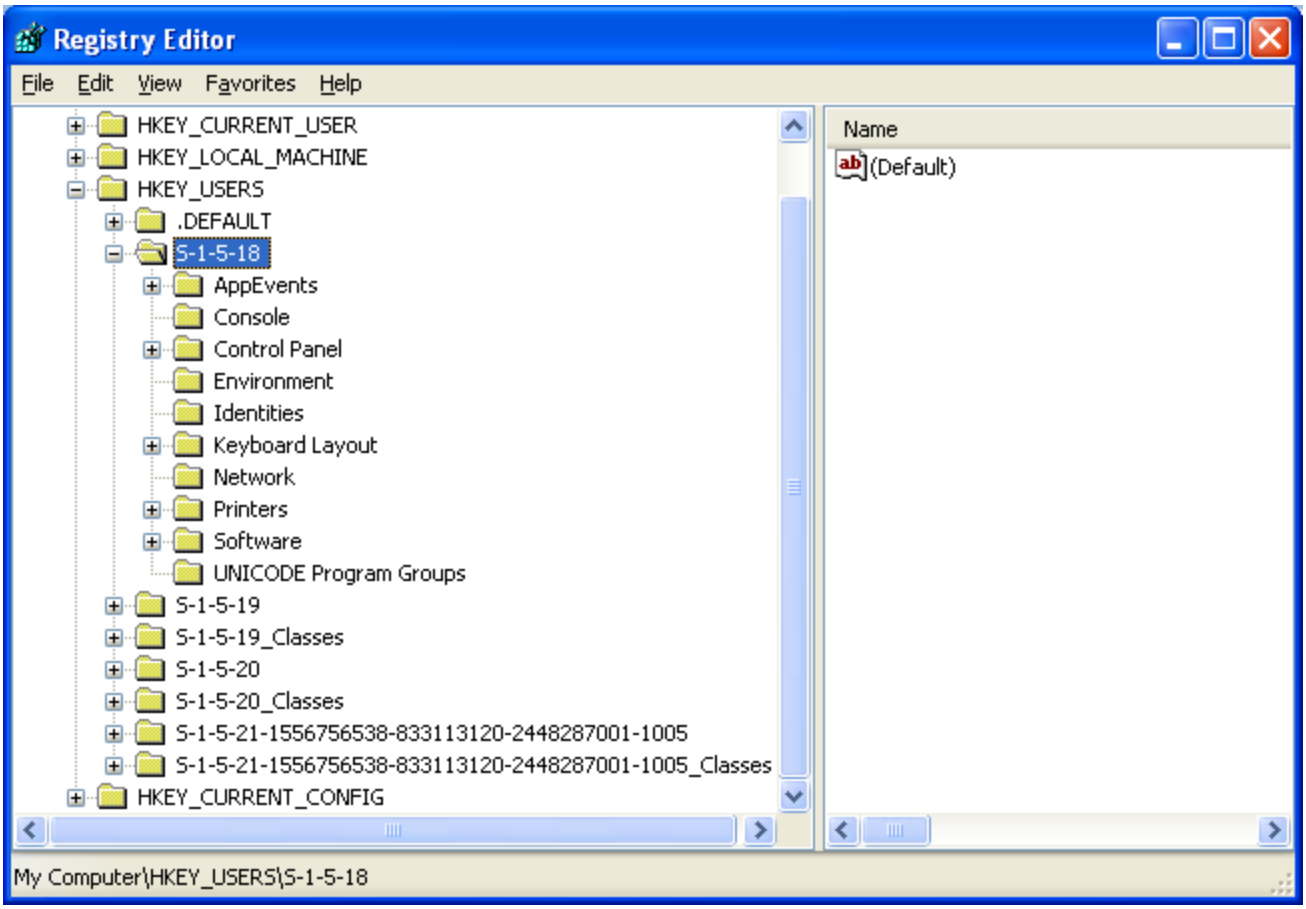
1. Able to understand descriptor definition language (SDDL).
2. Able to understand SID Strings and SID conversion.
3. Able to know the Well-known SID constants.
4. Able to understand and differentiate the well-known identifier authority and relative identifier (RID) values.

More on SID Strings

In the security descriptor definition language (SDDL), security descriptor string use SID strings for the following components of a security descriptor:

1. Owner.
2. Primary group.
3. The trustee in an ACE.

A SID string in a security descriptor string can use either the standard string representation of a SID (S-R-I-S-S...) or one of the string constants defined in sddl.h.



More on SID Components

A SID value includes components that provide information about the SID structure and components that uniquely identify a trustee. A SID consists of the following components:

1. The revision level of the SID structure.
2. A 48-bit identifier authority value that identifies the authority that issued the SID.
3. A variable number of sub authority or relative identifier (RID) values that uniquely identify the trustee relative to the authority that issued the SID.

RID is a portion of a security identifier (SID) that identifies a user or group in relation to the authority that issued the SID. The combination of the identifier authority value and the sub authority values ensures that no two SIDs will be the same, even if two different SID-issuing authorities issue the same combination of RID values. Each SID-issuing authority issues a given RID only once. SIDs are stored in binary format in a SID structure. To display a SID, you can call the ConvertSidToStringSid() function to convert a binary SID to string format. To convert a SID string back to a valid, functional SID, call the ConvertStringSidToSid() function. These

functions use the following standardized string notation for SIDs, which makes it simpler to visualize their components:

```
S-R-I-S-S...
```

In this notation, the literal character S identifies the series of digits as a SID, R is the revision level, I is the identifier-authority value, and S... is one or more sub authority values. The following example uses this notation to display the well-known domain-relative SID of the local Administrators group:

```
S-1-5-32-544
```

In this example, the SID has the following components. The constants in parentheses are well-known identifier authority and RID values defined in winnt.h:

a. A revision level of 1.
b. An identifier-authority value of 5 (SECURITY_NT_AUTHORITY).
c. A first sub authority value of 32 (SECURITY_BUILTIN_DOMAIN_RID).
d. A second sub authority value of 544 (DOMAIN_ALIAS_RID_ADMINS).

The following SID string constants for well-known SIDs are defined in sddl.h.

SID string	Constant in Sddl.h	Account alias and corresponding RID
"AO"	SDDL_ACCOUNT_OPERATORS	Account operators. The corresponding RID is DOMAIN_ALIAS_RID_ACCOUNT_OPS.
"RU"	SDDL_ALIAS_PREW2KCOMPACC	Alias to grant permissions to accounts that use applications compatible with Windows NT 4.0 operating systems. The corresponding RID is DOMAIN_ALIAS_RID_PREW2KCOMPACCESS.
"AN"	SDDL_ANONYMOUS	Anonymous logon. The corresponding RID is SECURITY_ANONYMOUS_LOGON_RID.
"AU"	SDDL_AUTHENTICATED_USERS	Authenticated users. The corresponding RID is SECURITY_AUTHENTICATED_USER_RID.
"BA"	SDDL_BUILTIN_ADMINISTRATORS	Built-in administrators. The corresponding RID is DOMAIN_ALIAS_RID_ADMINS.
"BG"	SDDL_BUILTIN_GUESTS	Built-in guests. The corresponding RID is DOMAIN_ALIAS_RID_GUESTS.
"BO"	SDDL_BACKUP_OPERATORS	Backup operators. The corresponding RID is

		DOMAIN_ALIAS_RID_BACKUP_OPS.
"BU"	SDDL_BUILTIN_USERS	Built-in users. The corresponding RID is DOMAIN_ALIAS_RID_USERS.
"CA"	SDDL_CERT_SERV_ADMINISTRATORS	Certificate publishers. The corresponding RID is DOMAIN_GROUP_RID_CERT_ADMINS.
"CG"	SDDL_CREATOR_GROUP	Creator group. The corresponding RID is SECURITY_CREATOR_GROUP_RID.
"CO"	SDDL_CREATOR_OWNER	Creator owner. The corresponding RID is SECURITY_CREATOR_OWNER_RID.
"DA"	SDDL_DOMAIN_ADMINISTRATORS	Domain administrators. The corresponding RID is DOMAIN_GROUP_RID_ADMINS.
"DC"	SDDL_DOMAIN_COMPUTERS	Domain computers. The corresponding RID is DOMAIN_GROUP_RID_COMPUTERS.
"DD"	SDDL_DOMAIN_DOMAIN_CONTROLLERS	Domain controllers. The corresponding RID is DOMAIN_GROUP_RID_CONTROLLERS.
"DG"	SDDL_DOMAIN_GUESTS	Domain guests. The corresponding RID is DOMAIN_GROUP_RID_GUESTS.
"DU"	SDDL_DOMAIN_USERS	Domain users. The corresponding RID is DOMAIN_GROUP_RID_USERS.
"EA"	SDDL_ENTERPRISE_ADMINS	Enterprise administrators. The corresponding RID is DOMAIN_GROUP_RID_ENTERPRISE_ADMINS.
"ED"	SDDL_ENTERPRISE_DOMAIN_CONTROLLERS	Enterprise domain controllers. The corresponding RID is SECURITY_SERVER_LOGON_RID.
"WD"	SDDL_EVERYONE	Everyone. The corresponding RID is SECURITY_WORLD_RID.
"PA"	SDDL_GROUP_POLICY_ADMINS	Group Policy administrators. The corresponding RID is DOMAIN_GROUP_RID_POLICY_ADMINS.
"IU"	SDDL_INTERACTIVE	Interactively logged-on user. This is a group identifier added to the token of a process when it was logged on interactively. The corresponding logon type is LOGON32_LOGON_INTERACTIVE. The corresponding RID is SECURITY_INTERACTIVE_RID.
"LA"	SDDL_LOCAL_ADMIN	Local administrator. The corresponding RID is

		DOMAIN_USER_RID_ADMIN.
"LG"	SDDL_LOCAL_GUEST	Local guest. The corresponding RID is DOMAIN_USER_RID_GUEST.
"LS"	SDDL_LOCAL_SERVICE	Local service account. The corresponding RID is SECURITY_LOCAL_SERVICE_RID.
"SY"	SDDL_LOCAL_SYSTEM	Local system. The corresponding RID is SECURITY_LOCAL_SYSTEM_RID.
"NU"	SDDL_NETWORK	Network logon user. This is a group identifier added to the token of a process when it was logged on across a network. The corresponding logon type is LOGON32_LOGON_NETWORK. The corresponding RID is SECURITY_NETWORK_RID.
"NO"	SDDL_NETWORK_CONFIGURATION_OPS	Network configuration operators. The corresponding RID is DOMAIN_ALIAS_RID_NETWORK_CONFIGURATION_OPS.
"NS"	SDDL_NETWORK_SERVICE	Network service account. The corresponding RID is SECURITY_NETWORK_SERVICE_RID.
"PO"	SDDL_PRINTER_OPERATORS	Printer operators. The corresponding RID is DOMAIN_ALIAS_RID_PRINT_OPS.
"PS"	SDDL_PERSONAL_SELF	Principal self. The corresponding RID is SECURITY_PRINCIPAL_SELF_RID.
"PU"	SDDL_POWER_USERS	Power users. The corresponding RID is DOMAIN_ALIAS_RID_POWER_USERS.
"RS"	SDDL_RAS_SERVERS	RAS servers group. The corresponding RID is DOMAIN_ALIAS_RID_RAS_SERVERS.
"RD"	SDDL_REMOTE_DESKTOP	Terminal server users. The corresponding RID is DOMAIN_ALIAS_RID_REMOTE_DESKTOP_USERS.
"RE"	SDDL_REPLICATOR	Replicator. The corresponding RID is DOMAIN_ALIAS_RID_REPLICATOR.
"RC"	SDDL_RESTRICTED_CODE	Restricted code. This is a restricted token created using the CreateRestrictedToken() function. The corresponding RID is SECURITY_RESTRICTED_CODE_RID.

"SA"	SDDL_SCHEMA_ADMINISTRATORS	Schema administrators. The corresponding RID is DOMAIN_GROUP_RID_SCHEMA_ADMINS.
"SO"	SDDL_SERVER_OPERATORS	Server operators. The corresponding RID is DOMAIN_ALIAS_RID_SYSTEM_OPS.
"SU"	SDDL_SERVICE	Service logon user. This is a group identifier added to the token of a process when it was logged as a service. The corresponding logon type is LOGON32_LOGON_SERVICE. The corresponding RID is SECURITY_SERVICE_RID.

Table 6

The ConvertSidToStringSid() and ConvertStringSidToSid() functions always use the standard SID string notation and do not support SDDL SID string constants.

Well-known SIDs

Well-known SIDs identify generic groups and generic users. For example, there are well-known SIDs to identify the following groups and users:

1. Everyone or World, which is a group that includes all users.
2. CREATOR_OWNER, which is used as a placeholder in an inheritable ACE. When the ACE is inherited, the system replaces the CREATOR_OWNER SID with the SID of the object's creator.
3. The Administrators group for the built-in domain on the local computer.

There is universal well-known SIDs, which are meaningful on all secure systems using this security model, including operating systems other than Windows. In addition, there are well-known SIDs that are meaningful only on Windows systems. The Windows API defines a set of constants for well-known identifier authority and relative identifier (RID) values. You can use these constants to create well-known SIDs. The following example combines the SECURITY_WORLD_SID_AUTHORITY and SECURITY_WORLD_RID constants to show the universal well-known SID for the special group representing all users (Everyone or World): S-1-1-0. This example uses the string notation for SIDs in which S identifies the string as a SID, the first 1 is the revision level of the SID, and the remaining two digits are the SECURITY_WORLD_SID_AUTHORITY and SECURITY_WORLD_RID constants. You can use the AllocateAndInitializeSid() function to build a SID by combining an identifier authority value with up to eight sub authority values. For example, to determine whether the logged-on

user is a member of a particular well-known group, call AllocateAndInitializeSid() to build a SID for the well-known group and use the EqualSid() function to compare that SID to the group SIDs in the user's access token. You must call the FreeSid() function to free a SID allocated by AllocateAndInitializeSid(). The following contains tables of well-known SIDs and tables of identifier authority and sub authority constants that you can use to build well-known SIDs. The following are some universal well-known SIDs.

Universal well-known SID	Identifies
Null SID Value: (S-1-0-0)	A group with no members. This is often used when a SID value is not known.
World Value: (S-1-1-0)	A group that includes all users.
Local Value: (S-1-2-0)	Users who log on to terminals locally (physically) connected to the system.
Creator Owner ID Value: (S-1-3-0)	A security identifier to be replaced by the security identifier of the user who created a new object. This SID is used in inheritable ACEs.
Creator Group ID Value: (S-1-3-1)	Identifies a security identifier to be replaced by the primary-group SID of the user who created a new object. Use this SID in inheritable ACEs.

Table 7

The following table lists the predefined identifier authority constants. The first four values are used with universal well-known SIDs; the last value is used with Windows well-known SIDs.

Identifier authority	Value	SID string prefix
SECURITY_NULL_SID_AUTHORITY	0	S-1-0
SECURITY_WORLD_SID_AUTHORITY	1	S-1-1
SECURITY_LOCAL_SID_AUTHORITY	2	S-1-2
SECURITY_CREATOR_SID_AUTHORITY	3	S-1-3
SECURITY_NT_AUTHORITY	5	S-1-5

Table 8

The following RID values are used with universal well-known SIDs. The Identifier authority column shows the prefix of the identifier authority with which you can combine the RID to create a universal well-known SID.

Relative identifier (RID) authority	Value	Identifier authority
SECURITY_NULL_RID	0	S-1-0
SECURITY_WORLD_RID	0	S-1-1
SECURITY_LOCAL_RID	0	S-1-2
SECURITY_CREATOR_OWNER_RID	0	S-1-3
SECURITY_CREATOR_GROUP_RID	1	S-1-3

Table 9

The SECURITY_NT_AUTHORITY (S-1-5) predefined identifier authority produces SIDs that are not universal but are meaningful only on Windows installations. You can use the following RID values with SECURITY_NT_AUTHORITY to create well-known SIDs.

Constant	Identifies
SECURITY_DIALUP_RID - (S-1-5-1)	Users who log on to terminals using a dial-up modem. This is a group identifier.
SECURITY_NETWORK_RID - (S-1-5-2)	Users who log on across a network. This is a group identifier added to the token of a process when it was logged on across a network. The corresponding logon type is LOGON32_LOGON_NETWORK.
SECURITY_BATCH_RID - (S-1-5-3)	Users who log on using a batch queue facility. This is a group identifier added to the token of a process when it was logged as a batch job. The corresponding logon type is LOGON32_LOGON_BATCH.
SECURITY_INTERACTIVE_RID - (S-1-5-4)	Users who log on for interactive operation. This is a group identifier added to the token of a process when it was logged on interactively. The corresponding logon type is LOGON32_LOGON_INTERACTIVE.
SECURITY_LOGON_IDS_RID - (S-1-5-5-X-Y)	A logon session. This is used to ensure that only processes in a given logon session can gain access to the window-station objects for that session. The X and Y values for these SIDs are different for each logon session. The value

	SECURITY_LOGON_IDS_RID_COUNT is the number of RIDs in this identifier (5-X-Y).
SECURITY_SERVICE_RID - (S-1-5-6)	Accounts authorized to log on as a service. This is a group identifier added to the token of a process when it was logged as a service. The corresponding logon type is LOGON32_LOGON_SERVICE.
SECURITY_ANONYMOUS_LOGON_RID -(S-1-5-7)	Anonymous logon or null session logon.
SECURITY_PROXY_RID - (S-1-5-8)	Proxy.
SECURITY_ENTERPRISE_CONTROLLERS_RID - (S-1-5-9)	Enterprise controllers.
SECURITY_PRINCIPAL_SELF_RID - (S-1-5-10)	The PRINCIPAL_SELF security identifier can be used in the ACL of a user or group object. During an access check, the system replaces the SID with the SID of the object. The PRINCIPAL_SELF SID is useful for specifying an inheritable ACE that applies to the user or group object that inherits the ACE. It the only way of representing the SID of a created object in the default security descriptor of the schema.
SECURITY_AUTHENTICATED_USER_RID - (S-1-5-11)	The authenticated users.
SECURITY_RESTRICTED_CODE_RID - (S-1-5-12)	Restricted code.
SECURITY_TERMINAL_SERVER_RID - (S-1-5-13)	Terminal Services. Automatically added to the security token of a user who logs on to a Terminal Server.
SECURITY_LOCAL_SYSTEM_RID - (S-1-5-18)	A special account used by the operating system.
SECURITY_NT_NON_UNIQUE - (S-1-5-21)	SIDS are not unique.
SECURITY_BUILTIN_DOMAIN_RID - (S-1-5-32)	The built-in system domain.

Table 10

The following RIDs are relative to each domain.

RID	Identifies
DOMAIN_USER_RID_ADMIN	The administrative user account in a domain.
DOMAIN_USER_RID_GUEST	The guest-user account in a domain. Users who do not have an account can automatically log on to this account.
DOMAIN_GROUP_RID_ADMINS	The domain administrators' group. This account exists only on systems running server operating systems.
DOMAIN_GROUP_RID_USERS	A group that contains all user accounts in a domain. All users are automatically added to this group.
DOMAIN_GROUP_RID_GUESTS	The guest-group account in a domain.
DOMAIN_GROUP_RID_COMPUTERS	The domain computers' group. All computers in the domain are members of this group.
DOMAIN_GROUP_RID_CONTROLLERS	The domain controllers' group. All DCs in the domain are members of this group.
DOMAIN_GROUP_RID_CERT_ADMINS	The certificate publishers' group. Computers running Certificate Services are members of this group.
DOMAIN_GROUP_RID_SCHEMA_ADMINS	The schema administrators' group. Members of this group can modify the Active Directory schema.
DOMAIN_GROUP_RID_ENTERPRISE_ADMINS	The enterprise administrators' group. Members of this group have full access to all domains in the Active Directory forest. Enterprise administrators are responsible for forest-level operations such as adding or removing new domains.
DOMAIN_GROUP_RID_POLICY_ADMINS	The policy administrators' group.

Table 11

The following table has examples of domain-relative RIDs that you can use to form well-known SIDs for local groups (aliases).

RID	Identifies
DOMAIN_ALIAS_RID_ADMINS	A local group used for administration of the domain.
DOMAIN_ALIAS_RID_USERS	A local group that represents all users in the domain.
DOMAIN_ALIAS_RID_GUESTS	A local group that represents guests of the domain.
DOMAIN_ALIAS_RID_POWER_USERS	A local group used to represent a user or set of users who expect to treat a system as if it were their personal computer rather than as a workstation for multiple users.
DOMAIN_ALIAS_RID_ACCOUNT_OPS	A local group that exists only on systems running server operating systems. This local group permits control over non administrator accounts.
DOMAIN_ALIAS_RID_SYSTEM_OPS	A local group that exists only on systems running server operating systems. This local group performs system administrative functions, not including security functions. It establishes network shares, controls printers, unlocks workstations, and performs other operations.
DOMAIN_ALIAS_RID_PRINT_OPS	A local group that exists only on systems running server operating systems. This local group controls printers and print queues.
DOMAIN_ALIAS_RID_BACKUP_OPS	A local group used for controlling assignment of file backup-and-restore privileges.
DOMAIN_ALIAS_RID_REPLICATOR	A local group responsible for copying security databases from the primary domain controller to the backup domain controllers. These accounts are used only by the system.
DOMAIN_ALIAS_RID_RAS_SERVERS	A local group that represents RAS and IAS servers. This group permits access to various attributes of user

	objects.
DOMAIN_ALIAS_RID_PREW2KCOMPACCESS	A local group that exists only on systems running Windows 2000 Server. It provides access rights and privileges equal to anonymous access under Windows NT, which is Everyone access.

Table 12

The WELL_KNOWN_SID_TYPE enumeration defines the list of commonly used SIDs. Additionally, the SDDL uses SID strings to reference well-known SIDs in a string format.