Windows Access Control List (ACL) 4

What do we have in this session?

1. The ACE String Components
2. The ACE String Description
3. The ACE Inheritance Rules

The ability that supposed to be acquired for this session is: Able to understand ACE string components.

The ACE Strings

The security descriptor definition language (SDDL) uses ACE strings in the DACL and SACL components of a security descriptor string as shown in the following Security Descriptor String Format examples:

```
"O:AOG:DAD:(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-0-0)"
```

Each ACE in a security descriptor string is enclosed in parentheses. The fields of the ACE are in the following order and are separated by semicolons (;).

```
(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-0-0)
```

The format is:

```
ace_type;ace_flags;rights;object_guid;inherit_object_guid;account_sid
```

The ACE String Description

ace_type - A string that indicates the value of the AceType member of the ACE_HEADER structure. The ACE type string can be one of the following strings defined in sddl.h.

ACE type string	Constant in Sddl.h	AceType value
"A"	SDDL_ACCESS_ALLOWED	ACCESS_ALLOWED_ACE_TYPE
"D"	SDDL_ACCESS_DENIED	ACCESS_DENIED_ACE_TYPE
"OA"	SDDL_OBJECT_ACCESS_ALLOWED	ACCESS_ALLOWED_OBJECT_ACE_TYPE

"OD"	SDDL_OBJECT_ACCESS_DENIED	ACCESS_DENIED_OBJECT_ACE_TYPE
"AU"	SDDL_AUDIT	SYSTEM_AUDIT_ACE_TYPE
"AL"	SDDL_ALARM	SYSTEM_ALARM_ACE_TYPE
"OU"	SDDL_OBJECT_AUDIT	SYSTEM_AUDIT_OBJECT_ACE_TYPE
"OL"	SDDL_OBJECT_ALARM	SYSTEM_ALARM_OBJECT_ACE_TYPE

Table 1

If ace_type is ACCESS_ALLOWED_OBJECT_ACE_TYPE and neither object_guid nor inherit_object_guid has a GUID specified, then ConvertStringSecurityDescriptorToSecurityDescriptor() converts ace_type to ACCESS_ALLOWED_ACE_TYPE.
ace_flags - A string that indicates the value of the AceFlags member of the ACE_HEADER structure. The ACE flags string can be a concatenation of the following strings that defined in sddl.h.

ACE flags string	Constant in Sddl.h	AceFlag value
"CI"	SDDL_CONTAINER_INHERIT	CONTAINER_INHERIT_ACE
"OI"	SDDL_OBJECT_INHERIT	OBJECT_INHERIT_ACE
"NP"	SDDL_NO_PROPAGATE	NO_PROPAGATE_INHERIT_ACE
"IO"	SDDL_INHERIT_ONLY	INHERIT_ONLY_ACE
"ID"	SDDL_INHERITED	INHERITED_ACE
"SA"	SDDL_AUDIT_SUCCESS	SUCCESSFUL_ACCESS_ACE_FLAG
"FA"	SDDL_AUDIT_FAILURE	FAILED_ACCESS_ACE_FLAG

Table 2

rights - A string that indicates the access rights controlled by the ACE. This string can be a hexadecimal string representation of the access rights, such as "0x7800003F", or it can be a concatenation of the following strings.

Access rights string	Constant in Sddl.h	Access right value
Generic access rights		
"GA"	SDDL_GENERIC_ALL	GENERIC_ALL
"GR"	SDDL_GENERIC_READ	GENERIC_READ
"GW"	SDDL_GENERIC_WRITE	GENERIC_WRITE
"GX"	SDDL_GENERIC_EXECUTE	GENERIC_EXECUTE

Standard access rights		
"RC"	SDDL_READ_CONTROL	READ_CONTROL
"SD"	SDDL_STANDARD_DELETE	DELETE
"WD"	SDDL_WRITE_DAC	WRITE_DAC
"WO"	SDDL_WRITE_OWNER	WRITE_OWNER
Directory service object access rights		
"RP"	SDDL_READ_PROPERTY	ADS_RIGHT_DS_READ_PROP
"WP"	SDDL_WRITE_PROPERTY	ADS_RIGHT_DS_WRITE_PROP
"CC"	SDDL_CREATE_CHILD	ADS_RIGHT_DS_CREATE_CHILD
"DC"	SDDL_DELETE_CHILD	ADS_RIGHT_DS_DELETE_CHILD
"LC"	SDDL_LIST_CHILDREN	ADS_RIGHT_DS_LIST
"SW"	SDDL_SELF_WRITE	ADS_RIGHT_DS_SELF
"LO"	SDDL_LIST_OBJECT	ADS_RIGHT_DS_LIST_OBJECT
"DT"	SDDL_DELETE_TREE	ADS_RIGHT_DS_DELETE_TREE
"CR"	SDDL_CONTROL_ACCESS	ADS_RIGHT_DS_CONTROL_ACCESS
File access rights		
"FA"	SDDL_FILE_ALL	FILE_ALL_ACCESS
"FR"	SDDL_FILE_READ	FILE_GENERIC_READ
"FW"	SDDL_FILE_WRITE	FILE_GENERIC_WRITE
"FX"	SDDL_FILE_EXECUTE	FILE_GENERIC_EXECUTE
Registry key access rights		
"KA"	SDDL_KEY_ALL	KEY_ALL_ACCESS
"KR"	SDDL_KEY_READ	KEY_READ
"KW"	SDDL_KEY_WRITE	KEY_WRITE
"KX"	SDDL_KEY_EXECUTE	KEY_EXECUTE

Table 3

object_guid - A string representation of a GUID that indicates the value of the ObjectType member of an object-specific ACE structure, such as ACCESS_ALLOWED_OBJECT_ACE. The GUID string uses the format returned by the UuidToString() function. The following table lists some commonly used object GUIDs.

Rights and GUID	Permission
`CR;ab721a53-1e2f-11d0-9819-00aa0040529b`	Change password.
`CR;00299570-246d-11d0-a768-00aa006e0529`	Reset password.

Table 4

inherit_object_guid - A string representation of a GUID that indicates the value of the InheritedObjectType member of an object-specific ACE structure. The GUID string uses the UuidToString() format.
account_sid - SID string that identifies the trustee of the ACE.

The following example shows an ACE string for an access-allowed ACE. It is not an object-specific ACE, so it has no information in the object_guid and inherit_object_guid fields. The ace_flags field is also empty, which indicates that none of the ACE flags are set.

```
(A;;RPWPCCDCLCSWRCWDWOGA;;;S-1-0-0)
```

The ACE string shown above describes the following ACE information:

AceType:	**0x00 (ACCESS_ALLOWED_ACE_TYPE)**
AceFlags:	**0x00**
Access Mask:	**0x100e003f** **READ_CONTROL** **WRITE_DAC** **WRITE_OWNER** **GENERIC_ALL** **Other access rights(0x0000003f)**
Ace Sid:	**(S-1-0-0)**

ACE Inheritance Rules

The system propagates inheritable ACEs to child objects according to a set of inheritance rules. The system places inherited ACEs in the DACL of the child according to the preferred order of ACEs in a DACL. The system sets the INHERITED_ACE flag in all inherited ACEs. For Windows NT, Windows Me/98/95, the system does not set the INHERITED_ACE flag in all inherited ACEs. The ACEs inherited by container and non-container child objects differ, depending on the combinations of inheritance flags. These inheritance rules work the same for both DACLs and SACLs.

Parent ACE flag	Effect on child ACL
OBJECT_INHERIT_ACE only	Non-container child objects: Inherited as an effective ACE. Container child objects: Containers inherit an inherit-only ACE unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.

CONTAINER_INHERIT_ACE only	Non-container child objects: No effect on the child object. Container child objects: The child object inherits an effective ACE. The inherited ACE is inheritable unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set.
CONTAINER_INHERIT_ACE and OBJECT_INHERIT_ACE	Non-container child objects: Inherited as an effective ACE. Container child objects: The child object inherits an effective ACE. The inherited ACE is inheritable unless the NO_PROPAGATE_INHERIT_ACE bit flag is also set
No inheritance flags set	No effect on child container or non-container objects.

Table 5

If an inherited ACE is an effective ACE for the child object, the system maps any generic rights to the specific rights for the child object. Similarly, the system maps generic security identifiers (SIDs), such as CREATOR_OWNER, to the appropriate SID. If an inherited ACE is an inherit-only ACE, any generic rights or generic SIDs are left unchanged so that they can be mapped appropriately when the ACE is inherited by the next generation of child objects. For a case in which a container object inherits an ACE that is both effective on the container and inheritable by its descendants, the container may inherit two ACEs. This occurs if the inheritable ACE contains generic information. The container inherits an inherit-only ACE that contains the generic information and an effective-only ACE in which the generic information has been mapped.

An object-specific ACE has an InheritedObjectType member that can contain a GUID to identify the type of object that can inherit the ACE. If the InheritedObjectType GUID is not specified, the inheritance rules for an object-specific ACE are the same as for a standard ACE. If the InheritedObjectType GUID is specified, the ACE is inheritable by objects that match the GUID if OBJECT_INHERIT_ACE is set, and by containers that match the GUID if CONTAINER_INHERIT_ACE is set. Note that currently only DS objects support object-specific ACEs, and the DS treats all object types as containers.