[MS-ADTS]: Active Directory Technical Specification
Control Access Rights Concordance

Table of Contents

1 Introduction

This document provides a concordance for all Microsoft Active Directory 'Control Access Rights' documented in [MS-Open-Specifications], as of 10 August 2009. For the purposes of this document, the base reference for these rights is [MS-ADTS] 5.1.3.2.1 Control Access Rights.

1.1 References

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L", March 2007.

[MS-ADA2] Microsoft Corporation, "Active Directory Schema Attributes M", March 2007.

[MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z", March 2007.

[MS-ADLS] Microsoft Corporation, "Active Directory Lightweight Directory Services Schema", March 2007.

[MS-ADSC] Microsoft Corporation, "Active Directory Schema Classes", March 2007.

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification", March 2007.

[MS-DRSR] Microsoft Corporation, "Directory Replication Service (DRS) Remote Protocol Specification", March 2007.

[MS-DTYP] Microsoft Corporation, "Windows Data Types", February 2008.

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions", March 2007.

[MS-Open-Specifications] Microsoft Corporation, "Open Specifications", © 2009 Microsoft Corporation.

[MS-SAMR] Microsoft Corporation, "Security Account Manager (SAM) Remote Protocol Specification (Client-to-Server)", March 2007.

[MS-SFU] Microsoft Corporation, "Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol Specification", March 2007.

[MSDN-AD-Classes] Microsoft Corporation, "Active Directory Schema Classes"

[MSDN-AD-Extended-Rights] Microsoft Corporation, "Control Access Rights: Extended Rights"

[MSDN-AD-Group-Policy] Microsoft Corporation, "Group Policy"

[MSDN-AD-LDS] Microsoft Corporation, "Active Directory Lightweight Directory Services (Active Directory Application Mode)"

[MSDN- Authorization] Microsoft Corporation, "Authorization"

[MSDN- Control-Access-Rights] Microsoft Corporation, "Control Access Rights"

[MSDN-DC-Replication] Microsoft Corporation, "Domain Controller and Replication Management Functions"

[MSDN-MS-CHAP-Password] Microsoft Corporation, "MS-CHAP Password Management Functions"

[MSDN-Net-Mgmt] Microsoft Corporation, "Network Management Functions"

[MSDN-Windows-Protocols] Microsoft Corporation, "Windows Protocols"

[MSDN- Windows-SDK] Microsoft Corporation, "Windows SDK Download"

[MSDN-Windows-Server-Protocols] Microsoft Corporation, "Windows Server Protocols"

1.2 Overview (Synopsis)

This document provides a concordance for all Microsoft Active Directory 'Control Access Rights' documented in [MS-Open-Specifications], as of 10 August 2009. For the purposes of this document, the base reference for these rights is [MS-ADTS] 5.1.3.2.1 Control Access Rights.

1.2.1 Control Access Rights

The text in this section is based on [MS-ADTS] 5.1.3.2.1 Control Access Rights.

In Active Directory, the implementer can control which users have the right to perform a particular operation on an object or its attributes by using standard access rights. However, there are certain operations that have semantics that are not tied to specific properties, or where it is desirable to control access in a way that is not supported by the standard access rights. For example, the implementer can grant users a "Reanimate tombstones" right so that they are able to perform tombstone reanimation on any object in a naming context. Active Directory allows the standard access control mechanism to be extended for controlling access to custom actions or operations, using a mechanism called control access rights.

A control access right is not identified by a specific bit in an access mask as the standard access rights are. Instead, each control access right is identified by a GUID. An ACE that grants or denies a control access right specifies the RIGHT_DS_CONTROL_ACCESS (CR) bit in the ACCESS_MASK field and the GUID identifying the particular control access right in the ObjectType field of the ACE. If the ObjectType field does not contain a GUID, the ACE is deemed to control the right to perform all operations associated with the objects that are controlled by control access rights. For convenience and easy identification by Active Directory administrative tools facilitating access control, each control access right is represented by an object of [MS-ADSC] 2.26 Class controlAccessRight in the Extended-Rights container. Note that these objects are not integral to evaluating access to an operation and, therefore, their presence is not required for the proper functioning of the access control mechanism. There are a number of predefined control access rights in Active Directory, and that list can be extended by application developers by adding [MS-ADSC] 2.26 Class controlAccessRight objects to the Extended-Rights container.

The pertinent attributes on the ([MS-ADSC] 2.26 Class) controlAccessRight object that defines the use of the control access right for the administrative tools are as follows:

- [MS-ADA3] 2.359 Attribute validAccesses: The type of access right bits in the ACCESS_MASK field of an ACE with which the control access right can be associated. The only permitted access right for control access rights is RIGHT_DS_CONTROL_ACCESS (CR) (See ADS_RIGHTS_ENUM Enumeration).
- [MS-ADA3] 2.207 Attribute rightsGuid: The GUID that is used to identify the control access right in an ACE. The GUID value is placed in the ObjectType field of the ACE.

- [MS-ADA1] 2.64 Attribute appliesTo: This multivalue attribute has a list of object classes that the control access right applies to. Each object class in the list is represented by the ([MS-ADA3] 2.226 Attribute) schemaIDGUID attribute of the ([MS-ADLS] 3.4 Class) classSchema object that defines the object class in the Active Directory schema.
    - [MS-ADLS] 3.4 Class classSchema
    - [MS-ADSC] 2.18 Class classSchema
    - [MS-ADTS] 3.1.1.2.4.8 Class classSchema

1.2.2 ACCESS_ALLOWED_OBJECT_ACE

Control Access Rights are generally configured in an ACCESS_ALLOWED_OBJECT_ACE, which is documented in the following referenced content:

- [MS-DTYP] 2.4.4.3 ACCESS_ALLOWED_OBJECT_ACE
- MSDN Win32 and COM Development \ Security \ Authorization \ Authorization Structures ACCESS_ALLOWED_OBJECT_ACE Structure
- [MSDN- Windows-SDK] (winnt.h)

```
typedef struct _ACCESS_ALLOWED_OBJECT_ACE {
    ACE_HEADER  Header;
    ACCESS_MASK Mask;
    DWORD       Flags;
    GUID        ObjectType;
    GUID        InheritedObjectType;
    DWORD       SidStart;
} ACCESS_ALLOWED_OBJECT_ACE, *PACCESS_ALLOWED_OBJECT_ACE;
```

MSDN Win32 and COM Development \ Security \ Authorization \ Authorization Structures ACE_HEADER Structure:

```
typedef struct _ACE_HEADER {
    BYTE        AceType;
    BYTE        AceFlags;
    WORD        AceSize;
}ACE_HEADER, *PACE_HEADER;
```

See [MSDN- Windows-SDK] (winnt.h) for the definition of ACCESS_ALLOWED_OBJECT_ACE_TYPE, which is used for the `ACE_HEADER.AceType` value.

```
#define ACCESS_ALLOWED_ACE_TYPE                 (0x0)
#define ACCESS_DENIED_ACE_TYPE                  (0x1)
#define SYSTEM_AUDIT_ACE_TYPE                   (0x2)
#define SYSTEM_ALARM_ACE_TYPE                   (0x3)
#define ACCESS_ALLOWED_COMPOUND_ACE_TYPE        (0x4)
#define ACCESS_ALLOWED_OBJECT_ACE_TYPE          (0x5)
#define ACCESS_DENIED_OBJECT_ACE_TYPE           (0x6)
#define SYSTEM_AUDIT_OBJECT_ACE_TYPE            (0x7)
#define SYSTEM_ALARM_OBJECT_ACE_TYPE            (0x8)
#define ACCESS_ALLOWED_CALLBACK_ACE_TYPE        (0x9)
```

```
#define ACCESS_DENIED_CALLBACK_ACE_TYPE          (0xA)
#define ACCESS_ALLOWED_CALLBACK_OBJECT_ACE_TYPE (0xB)
#define ACCESS_DENIED_CALLBACK_OBJECT_ACE_TYPE  (0xC)
#define SYSTEM_AUDIT_CALLBACK_ACE_TYPE           (0xD)
#define SYSTEM_ALARM_CALLBACK_ACE_TYPE           (0xE)
#define SYSTEM_AUDIT_CALLBACK_OBJECT_ACE_TYPE    (0xF)
#define SYSTEM_ALARM_CALLBACK_OBJECT_ACE_TYPE    (0x10)
```

The only permitted access right for control access rights is RIGHT_DS_CONTROL_ACCESS (CR) (See ADS_RIGHTS_ENUM Enumeration). This is applied to the ACCESS_ALLOWED_OBJECT_ACE.Mask (ACCESS_MASK) field:

```
typedef enum  {
    ADS_RIGHT_DELETE                    = 0x10000,
    ADS_RIGHT_READ_CONTROL              = 0x20000,
    ADS_RIGHT_WRITE_DAC                 = 0x40000,
    ADS_RIGHT_WRITE_OWNER               = 0x80000,
    ADS_RIGHT_SYNCHRONIZE               = 0x100000,
    ADS_RIGHT_ACCESS_SYSTEM_SECURITY    = 0x1000000,
    ADS_RIGHT_GENERIC_READ              = 0x80000000,
    ADS_RIGHT_GENERIC_WRITE             = 0x40000000,
    ADS_RIGHT_GENERIC_EXECUTE           = 0x20000000,
    ADS_RIGHT_GENERIC_ALL               = 0x10000000,
    ADS_RIGHT_DS_CREATE_CHILD           = 0x1,
    ADS_RIGHT_DS_DELETE_CHILD           = 0x2,
    ADS_RIGHT_ACTRL_DS_LIST             = 0x4,
    ADS_RIGHT_DS_SELF                   = 0x8,
    ADS_RIGHT_DS_READ_PROP              = 0x10,
    ADS_RIGHT_DS_WRITE_PROP             = 0x20,
    ADS_RIGHT_DS_DELETE_TREE            = 0x40,
    ADS_RIGHT_DS_LIST_OBJECT            = 0x80,
    ADS_RIGHT_DS_CONTROL_ACCESS         = 0x100
} ADS_RIGHTS_ENUM;
```

2 Control Access Rights

The following text is adapted from [MSDN- Control-Access-Rights].

All objects in Active Directory Domain Services support a standard set of access rights defined in the ADS_RIGHTS_ENUM enumeration. These access rights can be used in the Access Control Entries (ACEs) of an object's security descriptor to control access to the object; that is, to control who can perform standard operations, such as creating and deleting child objects, or reading and writing the object attributes. However, for some object classes, it may be desirable to control access in a way not supported by the standard access rights. To facilitate this, Active Directory Domain Services allow the standard access control mechanism to be extended through the controlAccessRight object.

Control access rights are used in three ways:

- For extended rights, which are special operations not covered by the standard set of access rights. For example, the user class can be granted a "Send As" right that can be used by Exchange, Outlook, or any other mail application, to determine whether a particular user can have another user send mail on their behalf. Extended rights are created on controlAccessRight objects by setting the validAccesses attribute to equal the ADS_RIGHT_DS_CONTROL_ACCESS (256) access right.
- For defining property sets, to enable controlling access to a subset of an object's attributes, rather than just to the individual attributes. Using the standard access rights, a single ACE can grant or deny access to all of an object's attributes or to a single attribute. Control access rights provide a way for a single ACE to control access to a set of attributes. For example, the user class supports the Personal-Information property set that includes attributes such as street address and telephone number. Property set rights are created on controlAccessRight objects by setting the validAccesses attribute to contain both the ACTR_DS_READ_PROP (16) and the ACTRL_DS_WRITE_PROP (32) access rights.
- For validated writes, to require that the system perform value checking, or validation, beyond that which is required by the schema, before writing a value to an attribute on a DS object. This ensures that the value entered for the attribute conforms to required semantics, is within a legal range of values, or undergoes some other special checking that would not be performed for a simple low-level write to the attribute. A validated write is associated to a special permission that is distinct from the "Write <attribute>" permission that would allow any value to be written to the attribute with no value checking performed. The validated write is the only one of the three control access rights that cannot be created as a new control access right for an application. This is because the existing system cannot be programmatically modified to enforce validation. If a control access right was set up in the system as a validated write, the validAccesses attribute on the controlAccessRight objects will contain the ADS_RIGHT_DS_SELF (8) access right. There are only three validated writes defined in the Windows 2000 Active Directory schema:

- Self-Membership permission on a Group object, which allows the caller's account, but no other account, to be added or removed from a group's membership.
- Validated-DNS-Host-Name permission on a Computer object, which allows a DNS host name attribute that is compliant with the computer name and domain name to be set.
- Validated-SPN permission on a Computer object, which allows an SPN attribute which is compliant with the DNS host name of the computer to be set.

2.1 Abandon-Replication Control Access Right

The 'Abandon-Replication' right is an extended right needed to cancel a replication sync.

Control access right symbol	Identifying GUID used in ACE
Abandon-Replication	ee914b82-0a98-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	Win 2000

MSDN References:

Title	URL
Abandon-Replication Extended Right	http://msdn.microsoft.com/en-us/library/ms684293.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx

2.2 Add-GUID Control Access Right

The 'Add-GUID' right is an extended right needed at the NC root to add an object with a specific GUID.

Control access right symbol	Identifying GUID used in ACE
Add-GUID	440820ad-65b4-11d1-a3da-0000f875ae0d

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Add-GUID Extended Right	http://msdn.microsoft.com/en-us/library/ms684296.aspx
[MS-ADTS] 3.1.1.5.2.2 Constraints	http://msdn.microsoft.com/en-us/library/cc223443.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.7 Add-GUID	http://msdn.microsoft.com/en-us/library/cc223656.aspx

2.3 Allocate-Rids Control Access Right

The 'Allocate-Rids' right is an extended right needed to request rid pool.

Control access right symbol	Identifying GUID used in ACE
Allocate-Rids	1abd7cf8-0a99-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Allocate-Rids Extended Right	http://msdn.microsoft.com/en-us/library/ms684297.aspx
NTDS-DSA Class	http://msdn.microsoft.com/en-us/library/ms683855.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx

2.4 Allowed-To-Authenticate Control Access Right

The 'Allowed-To-Authenticate' right is an extended right that controls who can authenticate to a particular machine or service. It basically lives on computer, user and InetOrgPerson objects. It is also applicable on the domain object if access is allowed for the entire domain. It can be applied to OU's to permit users to be able to set inheritable ACE's on OU's containing a set of user/computer objects.

Control access right symbol	Identifying GUID used in ACE
Allowed-To-Authenticate	68b1d179-0d15-4d4f-ab71-46152e79a7bc

Class Objects with this Extended Right:

AD Schema Class	Description
Computer	Represents a computer account in the domain.
inetOrgPerson	Represents people associated with an organization.
User	Stores information about an employee, contractor or visitor that works for an organization.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL

Title	URL
Allowed-To-Authenticate Extended Right	http://msdn.microsoft.com/en-us/library/ms684300.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.41 Allowed-To-Authenticate	http://msdn.microsoft.com/en-us/library/cc223625.aspx
[MS-KILE] 3.3.5.4 TGS Exchange	http://msdn.microsoft.com/en-us/library/cc233962.aspx
[MS-SFU] 4.3 S4U2proxy Example <Windows Behavior>	http://msdn.microsoft.com/en-us/library/cc246110.aspx

2.5 Apply-Group-Policy Control Access Right

The 'Apply-Group-Policy' right is an extended right used by Group Policy engine to determine if a GPO applies to a user/computer or not.

Control access right symbol	Identifying GUID used in ACE
Apply-Group-Policy	edacfd8f-ffb3-11d1-b41d-00a0c968f939

Class Objects with this Extended Right:

AD Schema Class	Description
Group-Policy-Container	Represents the Group Policy Object; used to define group polices.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Apply-Group-Policy Extended Right	http://msdn.microsoft.com/en-us/library/ms684306.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.19 Apply-Group-Policy	http://msdn.microsoft.com/en-us/library/cc223601.aspx

2.6 Certificate-Enrollment Control Access Right

The 'Certificate-Enrollment' right is an extended right .

Control access right symbol	Identifying GUID used in ACE
Certificate-Enrollment	0e10c968-78fb-11d2-90d4-00c04f79dc55

Class Objects with this Extended Right:

AD Schema Class	Description
PKI-Certificate-Template	Contains information for certificate issued by Certificate Server.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Certificate-Enrollment Extended Right	http://msdn.microsoft.com/en-us/library/ms684310.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.26 Certificate-Enrollment	http://msdn.microsoft.com/en-us/library/cc223609.aspx
Certificate Enrollment API	http://msdn.microsoft.com/en-us/library/aa374863.aspx

2.7 Change-Domain-Master Control Access Right

The 'Change-Domain-Master' right is an extended right needed to change the domain naming FSMO role owner.

Control access right symbol	Identifying GUID used in ACE
Change-Domain-Master	014bf69c-7b3b-11d1-85f6-08002be74fab

Class Objects with this Extended Right:

AD Schema Class	Description
Cross-Ref-Container	Holds cross-refs objects for all Naming Contexts.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Change-Domain-Master Extended Right	http://msdn.microsoft.com/en-us/library/ms684314.aspx
[MS-ADTS] 3.1.1.3.3.1 becomeDomainMaster	http://msdn.microsoft.com/en-us/library/cc223298.aspx
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.8 Change-Domain-Master	http://msdn.microsoft.com/en-us/library/cc223658.aspx

2.8 Change-Infrastructure-Master Control Access Right

The 'Change-Infrastructure-Master' right is an extended right needed to change the infrastructure FSMO role owner.

Control access right symbol	Identifying GUID used in ACE
Change-Infrastructure-Master	cc17b1fb-33d9-11d2-97d4-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
Infrastructure-Update	Represents the infrastructure master for a domain.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Change-Infrastructure-Master Extended Right	http://msdn.microsoft.com/en-us/library/ms684316.aspx
[MS-ADTS] 3.1.1.3.3.2 becomeInfrastructureMaster	http://msdn.microsoft.com/en-us/library/cc223309.aspx
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 3.1.1.5.3.1.2 FSMO Changes	http://msdn.microsoft.com/en-us/library/cc223461.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.22 Change-Infrastructure-Master	http://msdn.microsoft.com/en-us/library/cc223605.aspx

2.9 Change-PDC Control Access Right

The 'Change-PDC' right is an extended right needed to change the primary domain controller (PDC) emulator FSMO role owner.

Control access right symbol	Identifying GUID used in ACE
Change-PDC	bae50096-4752-11d1-9052-00c04fc2d4cf

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Change-PDC Extended Right	http://msdn.microsoft.com/en-us/library/ms684321.aspx
[MS-ADTS] 3.1.1.3.3.3 becomePdc	http://msdn.microsoft.com/en-us/library/cc223312.aspx

Title	URL
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 3.1.1.5.3.1.2 FSMO Changes	http://msdn.microsoft.com/en-us/library/cc223461.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.6 Change-PDC	http://msdn.microsoft.com/en-us/library/cc223646.aspx

2.10 Change-Rid-Master Control Access Right

The 'Change-Rid-Master' right is an extended right needed to change the relative identifier (RID) master FSMO role owner.

Control access right symbol	Identifying GUID used in ACE
Change-Rid-Master	d58d5f36-0a98-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
RID-Manager	Contains the RID FSMO and the RID-Available-Pool location.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Change-Rid-Master Extended Right	http://msdn.microsoft.com/en-us/library/ms684324.aspx
[MS-ADTS] 3.1.1.3.3.5 becomeRidMaster	http://msdn.microsoft.com/en-us/library/cc223314.aspx
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 3.1.1.5.3.1.2 FSMO Changes	http://msdn.microsoft.com/en-us/library/cc223461.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.2 Change-Rid-Master	http://msdn.microsoft.com/en-us/library/cc223602.aspx

2.11 Change-Schema-Master Control Access Right

The 'Change-Schema-Master' right is an extended right needed to change the schema master FSMO role owner.

Control access right symbol	Identifying GUID used in ACE
Change-Schema-Master	e12b56b6-0a95-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
DMD	Holds the Active Directory schema.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Change-Schema-Master Extended Right	http://msdn.microsoft.com/en-us/library/ms684327.aspx
[MS-ADTS] 3.1.1.3.3.6 becomeSchemaMaster	http://msdn.microsoft.com/en-us/library/cc223315.aspx
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 3.1.1.5.3.1.2 FSMO Changes	http://msdn.microsoft.com/en-us/library/cc223461.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.69 Change-Schema-Master	http://msdn.microsoft.com/en-us/library/cc223655.aspx

2.12 Create-Inbound-Forest-Trust Control Access Right

The 'Create-Inbound-Forest-Trust' right is an extended right that enables users to create an inbound-only trust between forests by adding them to the appropriate group.

Control access right symbol	Identifying GUID used in ACE
Create-Inbound-Forest-Trust	e2a36dc9-ae17-47c3-b58b-be34c55ba633

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Create-Inbound-Forest-Trust Extended Right	http://msdn.microsoft.com/en-us/library/ms684328.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.37 Create-Inbound-Forest-Trust	http://msdn.microsoft.com/en-us/library/cc223620.aspx

Title	URL
MS-DS-All-Users-Trust-Quota Attribute	http://msdn.microsoft.com/en-us/library/ms677184.aspx
MS-DS-Per-User-Trust-Quota Attribute	http://msdn.microsoft.com/en-us/library/ms677460.aspx

2.13 Do-Garbage-Collection Control Access Right

The 'Do-Garbage-Collection' right is an extended right to force the Directory Service to do garbage collection.

Control access right symbol	Identifying GUID used in ACE
Do-Garbage-Collection	fec364e0-0a98-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Do-Garbage-Collection Extended Right	http://msdn.microsoft.com/en-us/library/ms684345.aspx
[MS-ADTS] 3.1.1.3.3.8 doGarbageCollection	http://msdn.microsoft.com/en-us/library/cc223317.aspx
[MS-ADTS] 3.1.1.3.3.19 doGarbageCollectionPhantomsNow	http://msdn.microsoft.com/en-us/library/cc223308.aspx
[MS-ADTS] 3.1.1.3.3.15 doLinkCleanup	http://msdn.microsoft.com/en-us/library/cc223304.aspx
[MS-ADTS] 3.1.1.3.3.16 doOnlineDefrag	http://msdn.microsoft.com/en-us/library/cc223305.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.3 Do-Garbage-Collection	http://msdn.microsoft.com/en-us/library/cc223613.aspx

2.14 Domain-Administer-Server Control Access Right

The 'Domain-Administer-Server' right is an extended right: Legacy SAM right.

Control access right symbol	Identifying GUID used in ACE
Domain-Administer-Server	ab721a52-1e2f-11d0-9819-00aa0040529b

Class Objects with this Extended Right:

AD Schema Class	Description
Sam-Server	Holds a revision level and a security descriptor that specifies who can make RPC calls through the SAM interface.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Domain-Administer-Server Extended Right	http://msdn.microsoft.com/en-us/library/ms684334.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.51 Domain-Administer-Server	http://msdn.microsoft.com/en-us/library/cc223636.aspx
[MS-SAMR] 2.2.1.4 Domain ACCESS_MASK Values	http://msdn.microsoft.com/en-us/library/cc245522.aspx
[MS-SAMR] 3.1.5.1.5 SamrOpenDomain (Opnum 7)	http://msdn.microsoft.com/en-us/library/cc245748.aspx

2.15 DS-Check-Stale-Phantoms Control Access Right

The 'DS-Check-Stale-Phantoms' right is an extended right needed to force DS to check stale phantom objects.

Control access right symbol	Identifying GUID used in ACE
DS-Check-Stale-Phantoms	69ae6200-7f46-11d2-b9ad-00c04f79f805

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Check-Stale-Phantoms Extended Right	http://msdn.microsoft.com/en-us/library/ms684347.aspx
[MS-ADTS] 3.1.1.3.3.7 checkPhantoms	http://msdn.microsoft.com/en-us/library/cc223316.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.25 DS-Check-Stale-Phantoms	http://msdn.microsoft.com/en-us/library/cc223608.aspx

2.16 DS-Execute-Intentions-Script Control Access Right

The 'DS-Execute-Intentions-Script' right is an extended right, which should be granted to the partitions container that allows the Rendom.exe or prepare operation to be used in a domain rename. This control access right also appears as an audit-only right when the Redom.exe or execute step operations are performed.

Control access right symbol	Identifying GUID used in ACE
DS-Execute-Intentions-Script	2f16c4a5-b98e-432c-952a-cb388ba33f2e

Class Objects with this Extended Right:

AD Schema Class	Description
Cross-Ref-Container	Holds cross-refs objects for all Naming Contexts.

Implemented on:	AD-LDS (ADAM)	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Execute-Intentions-Script Extended Right	http://msdn.microsoft.com/en-us/library/ms684349.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.42 DS-Execute-Intentions-Script	http://msdn.microsoft.com/en-us/library/cc223626.aspx
[MS-DRSR] 4.2.1.3 Server Behavior of the IDL_DSAPrepareScript Method	http://msdn.microsoft.com/en-us/library/dd207922.aspx

2.17 DS-Install-Replica Control Access Right

The 'DS-Install-Replica' right is an extended right needed to do a replica install.

Control access right symbol	Identifying GUID used in ACE
DS-Install-Replica	9923a32a-3607-11d2-b9be-0000f87a36b2

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Install-Replica Extended Right	http://msdn.microsoft.com/en-us/library/ms684351.aspx
[MS-ADTS] 3.1.1.3.4.1.23 LDAP_SERVER_RODC_DCPROMO_OID	http://msdn.microsoft.com/en-us/library/cc223346.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.21 DS-Install-Replica	http://msdn.microsoft.com/en-us/library/cc223604.aspx
[MS-SAMR] 3.1.1.8.10 userAccountControl	http://msdn.microsoft.com/en-us/library/cc245673.aspx

2.18 DS-Query-Self-Quota Control Access Right

The 'DS-Query-Self-Quota' right is an extended right .

Control access right symbol	Identifying GUID used in ACE
DS-Query-Self-Quota	4ecc03fe-ffc0-4947-b630-eb672a8a9dbc

Class Objects with this Extended Right:

AD Schema Class	Description
ms-DS-Quota-Container	Holds all quota specifications for the directory database.

Implemented on:	AD-LDS (ADAM)	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Query-Self-Quota Extended Right	http://msdn.microsoft.com/en-us/library/ms684352.aspx
[MS-ADTS] 3.1.1.3.4.1.19 LDAP_SERVER_QUOTA_CONTROL_OID	http://msdn.microsoft.com/en-us/library/cc223341.aspx
[MS-ADTS] 3.1.1.4.4 Extended Access Checks	http://msdn.microsoft.com/en-us/library/cc223383.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.47 DS-Query-Self-Quota	http://msdn.microsoft.com/en-us/library/cc223631.aspx

2.19 DS-Replication-Get-Changes Control Access Right

The 'DS-Replication-Get-Changes' right is an extended right needed to replicate changes from a given NC.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Get-Changes	

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Replication-Get-Changes Extended Right	http://msdn.microsoft.com/en-us/library/ms684354.aspx
[MS-ADTS] 3.1.1.3.4.1.3 LDAP_SERVER_DIRSYNC_OID	http://msdn.microsoft.com/en-us/library/cc223347.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.1 Naming Contexts	http://msdn.microsoft.com/en-us/library/cc223526.aspx
[MS-ADTS] 7.1.1.1.2 Config NC Root	http://msdn.microsoft.com/en-us/library/cc223528.aspx
[MS-ADTS] 7.1.1.1.3 Schema NC Root	http://msdn.microsoft.com/en-us/library/cc223529.aspx
[MS-ADTS] 7.1.1.1.4 Domain NC Root	http://msdn.microsoft.com/en-us/library/cc223530.aspx
[MS-ADTS] 7.1.1.2.7.66 DS-Replication-Get-Changes	http://msdn.microsoft.com/en-us/library/cc223652.aspx
[MS-DRSR] 4.1.8.3 Server Behavior of the IDL_DRSGetMemberships Method	http://msdn.microsoft.com/en-us/library/dd240102.aspx
[MS-DRSR] 4.1.12.4 Server Behavior of the IDL_DRSGetObjectExistence Method	http://msdn.microsoft.com/en-us/library/dd207824.aspx
[MS-DRSR] 5.106.12 SecurityCheckForChanges	http://msdn.microsoft.com/en-us/library/dd303556.aspx
[MS-DRSR] 5.94 IsGetNCChangesPermissionGranted	http://msdn.microsoft.com/en-us/library/dd240185.aspx

2.20 DS-Replication-Get-Changes-All Control Access Right

The 'DS-Replication-Get-Changes-All' right is an extended right needed to replicate changes from a given NC.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Get-Changes-All	1131f6ad-9c07-11d1-f79f-00c04fc2dcd2

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Replication-Get-Changes-All Extended Right	http://msdn.microsoft.com/en-us/library/ms684355.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.1 Naming Contexts	http://msdn.microsoft.com/en-us/library/cc223526.aspx
[MS-ADTS] 7.1.1.1.2 Config NC Root	http://msdn.microsoft.com/en-us/library/cc223528.aspx
[MS-ADTS] 7.1.1.1.3 Schema NC Root	http://msdn.microsoft.com/en-us/library/cc223529.aspx
[MS-ADTS] 7.1.1.1.4 Domain NC Root	http://msdn.microsoft.com/en-us/library/cc223530.aspx
[MS-ADTS] 7.1.1.1.5 Application NC Root	http://msdn.microsoft.com/en-us/library/cc223531.aspx
[MS-ADTS] 7.1.1.2.7.38 DS-Replication-Get-Changes-All	http://msdn.microsoft.com/en-us/library/cc223621.aspx
[MS-DRSR] 5.106.12 SecurityCheckForChanges	http://msdn.microsoft.com/en-us/library/dd303556.aspx
[MS-DRSR] 5.94 IsGetNCChangesPermissionGranted	http://msdn.microsoft.com/en-us/library/dd240185.aspx

2.21 DS-Replication-Get-Changes-In-Filtered-Set Control Access Right

The 'DS-Replication-Get-Changes-In-Filtered-Set' right is an extended right that allows the replication of data to a partial or read-only domain replica NC.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Get-Changes-In-Filtered-Set	89e95b76-444d-4c62-991a-0facbeda640c

Class Objects with this Extended Right:

AD Schema Class	Description

Implemented on:	

MSDN References:

Title	URL

Title	URL
[MS-ADTS] 3.1.1.3.4.1.3 LDAP_SERVER_DIRSYNC_OID	http://msdn.microsoft.com/en-us/library/cc223347.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.1 Naming Contexts	http://msdn.microsoft.com/en-us/library/cc223526.aspx
[MS-ADTS] 7.1.1.1.2 Config NC Root	http://msdn.microsoft.com/en-us/library/cc223528.aspx
[MS-ADTS] 7.1.1.1.3 Schema NC Root	http://msdn.microsoft.com/en-us/library/cc223529.aspx
[MS-ADTS] 7.1.1.1.4 Domain NC Root	http://msdn.microsoft.com/en-us/library/cc223530.aspx
[MS-ADTS] 7.1.1.1.5 Application NC Root	http://msdn.microsoft.com/en-us/library/cc223531.aspx
[MS-ADTS] 7.1.1.2.7.70 DS-Replication-Get-Changes-In-Filtered-Se	http://msdn.microsoft.com/en-us/library/cc223657.aspx
[MS-DRSR] 5.106.12 SecurityCheckForChanges	http://msdn.microsoft.com/en-us/library/dd303556.aspx
[MS-DRSR] 5.94 IsGetNCChangesPermissionGranted	http://msdn.microsoft.com/en-us/library/dd240185.aspx

2.22 DS-Replication-Manage-Topology Control Access Right

The 'DS-Replication-Manage-Topology' right is an extended right needed to update the replication topology for a given NC.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Manage-Topology	1131f6ac-9c07-11d1-f79f-00c04fc2dcd2

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Replication-Manage-Topology Extended Right	http://msdn.microsoft.com/en-us/library/ms684357.aspx
MS-ADTS] 3.1.1.4.4 Extended Access Checks	http://msdn.microsoft.com/en-us/library/cc223383.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx

Title	URL
[MS-ADTS] 7.1.1.2.7.68 DS-Replication-Manage-Topology	http://msdn.microsoft.com/en-us/library/cc223654.aspx
[MS-DRSR] 4.1.1.2.3 CreateNtdsDsa	http://msdn.microsoft.com/en-us/library/dd207878.aspx
[MS-DRSR] 4.1.1.3 Server Behavior of the IDL_DRSAddEntry Method	http://msdn.microsoft.com/en-us/library/dd207885.aspx
[MS-DRSR] 4.1.6.3 Server Behavior of the IDL_DRSExecuteKCC Method	http://msdn.microsoft.com/en-us/library/cc228366.aspx
[MS-DRSR] 4.1.13.3 Server Behavior of the IDL_DRSGetReplInfo Method	http://msdn.microsoft.com/en-us/library/cc228170.aspx
[MS-DRSR] 4.1.19.2 Server Behavior of the IDL_DRSReplicaAdd Method	http://msdn.microsoft.com/en-us/library/cc228211.aspx
[MS-DRSR] 4.1.20.2 Server Behavior of the IDL_DRSReplicaDel Method	http://msdn.microsoft.com/en-us/library/cc228217.aspx
[MS-DRSR] 4.1.22.2 Server Behavior of the IDL_DRSReplicaModify Method	http://msdn.microsoft.com/en-us/library/cc228236.aspx
[MS-DRSR] 4.1.24.3 Server Behavior of the IDL_DRSReplicaVerifyObjects Method	http://msdn.microsoft.com/en-us/library/cc228248.aspx
[MS-DRSR] 4.1.26.2 Server Behavior of the IDL_DRSUpdateRefs Method	http://msdn.microsoft.com/en-us/library/cc228255.aspx
[MS-DRSR] 5.3 AccessCheckCAR	http://msdn.microsoft.com/en-us/library/cc228469.aspx

2.23 DS-Replication-Monitor-Topology Control Access Right

The 'DS-Replication-Monitor-Topology' right is an extended right that allows the reading of replication monitoring data, such as replication status and object metadata.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Monitor-Topology	f98340fb-7c5b-4cdb-a00b-2ebdfa115a96

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Replication-Monitor-Topology Extended Right	http://msdn.microsoft.com/en-us/library/ms684358.aspx

Title	URL
MS-ADTS] 3.1.1.4.4 Extended Access Checks	http://msdn.microsoft.com/en-us/library/cc223383.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.43 DS-Replication-Monitor-Topology	http://msdn.microsoft.com/en-us/library/cc223627.aspx
[MS-DRSR] 4.1.13.3 Server Behavior of the IDL_DRSGetReplInfo Method	http://msdn.microsoft.com/en-us/library/cc228170.aspx

2.24 DS-Replication-Secrets-Synchronize Control Access Right

The 'DS-Replication-Secrets-Synchronize' right is an extended right needed to replicate object secret attributes.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Secrets-Synchronize	1131f6ae-9c07-11d1-f79f-00c04fc2dcd2

Class Objects with this Extended Right:

AD Schema Class	Description

Implemented on:	

MSDN References:

Title	URL
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx

2.25 DS-Replication-Synchronize Control Access Right

The 'DS-Replication-Synchronize' right is an extended right needed to synchronize replication from a given NC.

Control access right symbol	Identifying GUID used in ACE
DS-Replication-Synchronize	1131f6ab-9c07-11d1-f79f-00c04fc2dcd2

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
DS-Replication-Synchronize Extended Right	http://msdn.microsoft.com/en-us/library/ms684361.aspx
[MS-ADTS] 3.1.1.3.3.14 removeLingeringObject	http://msdn.microsoft.com/en-us/library/cc223303.aspx
[MS-ADTS] 3.1.1.3.3.17 replicateSingleObject	http://msdn.microsoft.com/en-us/library/cc223306.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.67 DS-Replication-Synchronize	http://msdn.microsoft.com/en-us/library/cc223653.aspx
[MS-DRSR] 4.1.23.2 Server Behavior of the IDL_DRSReplicaSync Method	http://msdn.microsoft.com/en-us/library/cc228241.aspx

2.26 Enable-Per-User-Reversibly-Encrypted-Password Control Access Right

The 'Enable-Per-User-Reversibly-Encrypted-Password' right is an extended right .

Control access right symbol	Identifying GUID used in ACE
Enable-Per-User-Reversibly-Encrypted-Password	05c74c5e-4deb-43b4-bd9f-86664c2a7fd5

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Enable-Per-User-Reversibly-Encrypted-Password Extended Right	http://msdn.microsoft.com/en-us/library/ms684364.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.46 Enable-Per-User-Reversibly-Encrypted-Password	http://msdn.microsoft.com/en-us/library/cc223630.aspx
[MS-SAMR] 3.1.1.8.10 userAccountControl	http://msdn.microsoft.com/en-us/library/cc245673.aspx
NetUserSetInfo	http://msdn.microsoft.com/en-us/library/bb706734.aspx

2.27 Generate-RSoP-Logging Control Access Right

The 'Generate-RSoP-Logging' right is an extended right allowing the user who has the rights on an OU/Domain will be able to generate logging mode RSoP data for the users/computers within the OU.

Control access right symbol	Identifying GUID used in ACE
Generate-RSoP-Logging	b7b1b3de-ab09-4242-9e30-9980e5d322f7

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.
Organizational-Unit	A container for storing users, computers, and other account objects.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Generate-RSoP-Logging Extended Right	http://msdn.microsoft.com/en-us/library/ms684368.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.34 Generate-RSoP-Logging	http://msdn.microsoft.com/en-us/library/cc223617.aspx
GPMPermissionType Enumeration	http://msdn.microsoft.com/en-us/library/bb540649.aspx
GPPermissionType Enumeration	http://msdn.microsoft.com/en-us/library/microsoft.grouppolicy.gppermissiontype.aspx

2.28 Generate-RSoP-Planning Control Access Right

The 'Generate-RSoP-Planning' right is an extended right allowing the user who has the rights on an OU/Domain will be able to generate planning mode RSoP data for the users/computers within the OU.

Control access right symbol	Identifying GUID used in ACE
Generate-RSoP-Planning	b7b1b3dd-ab09-4242-9e30-9980e5d322f7

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.
Organizational-Unit	A container for storing users, computers, and other account objects.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Generate-RSoP-Planning Extended Right	http://msdn.microsoft.com/en-us/library/ms684370.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.30 Generate-RSoP-Planning	http://msdn.microsoft.com/en-us/library/cc223614.aspx
GPMPermissionType Enumeration	http://msdn.microsoft.com/en-us/library/bb540649.aspx
GPPermissionType Enumeration	http://msdn.microsoft.com/en-us/library/microsoft.grouppolicy.gppermissiontype.aspx

2.29 Migrate-SID-History Control Access Right

The 'Migrate-SID-History' right is an extended right that enables a user to migrate the SID-History without administrator privileges.

Control access right symbol	Identifying GUID used in ACE
Migrate-SID-History	ba33815a-4f93-4c76-87f3-57574bff8109

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Migrate-SID-History Extended Right	http://msdn.microsoft.com/en-us/library/ms684374.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.39 Migrate-SID-History	http://msdn.microsoft.com/en-us/library/cc223622.aspx
[MS-DRSR] 4.1.2.3 Server Behavior of the IDL_DRSAddSidHistory Method	http://msdn.microsoft.com/en-us/library/cc228291.aspx
DsAddSidHistory Function	http://msdn.microsoft.com/en-us/library/ms675918.aspx

2.30 msmq-Open-Connector Control Access Right

The 'msmq-Open-Connector' right is an extended right which allows opening a connector queue.

Control access right symbol	Identifying GUID used in ACE

Control access right symbol	Identifying GUID used in ACE
msmq-Open-Connector	b4e60130-df3f-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
Site	Stores server objects; represents a physical location; used to manage replication.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Open-Connector Extended Right	http://msdn.microsoft.com/en-us/library/ms684376.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.18 msmq-Open-Connector	http://msdn.microsoft.com/en-us/library/cc223600.aspx

2.31 msmq-Peek Control Access Right

The 'msmq-Peek' right is an extended right that allows peeking at messages in the queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Peek	06bd3201-df3e-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.
MSMQ-Queue	Associated with a specific computer, under the MSMQ-Configuration.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Peek Extended Right	http://msdn.microsoft.com/en-us/library/ms684378.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.15 msmq-Peek	http://msdn.microsoft.com/en-us/library/cc223597.aspx

2.32 msmq-Peek-computer-Journal Control Access Right

The 'msmq-Peek-computer-Journal' right is an extended right that allows peeking at messages in the Computer Journal queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Peek-computer-Journal	4b6e08c3-df3c-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Peek-computer-Journal Extended Right	http://msdn.microsoft.com/en-us/library/ms684380.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.13 msmq-Peek-computer-Journal	http://msdn.microsoft.com/en-us/library/cc223595.aspx

2.33 msmq-Peek-Dead-Letter Control Access Right

The 'msmq-Peek-Dead-Letter' right is an extended right that allows peeking at messages in the Dead Letter queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Peek-Dead-Letter	4b6e08c1-df3c-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Peek-Dead-Letter Extended Right	http://msdn.microsoft.com/en-us/library/ms684381.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx

Title	URL
[MS-ADTS] 7.1.1.2.7.11 msmq-Peek-Dead-Letter	http://msdn.microsoft.com/en-us/library/cc223593.aspx

2.34 msmq-Receive Control Access Right

The 'msmq-Receive' right is an extended right that allows receiving messages from the queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Receive	06bd3200-df3e-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.
MSMQ-Queue	Associated with a specific computer, under the MSMQ-Configuration.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Receive Extended Right	http://msdn.microsoft.com/en-us/library/ms684383.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.14 msmq-Receive	http://msdn.microsoft.com/en-us/library/cc223596.aspx

2.35 msmq-Receive-computer-Journal Control Access Right

The 'msmq-Receive-computer-Journal' right is an extended right that allows receiving messages from the Computer Journal queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Receive-computer-Journal	4b6e08c2-df3c-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL

Title	URL
msmq-Receive-computer-Journal Extended Right	http://msdn.microsoft.com/en-us/library/ms684385.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.12 msmq-Receive-computer-Journal	http://msdn.microsoft.com/en-us/library/cc223594.aspx

2.36 msmq-Receive-Dead-Letter Control Access Right

The 'msmq-Receive-Dead-Letter' right is an extended right that allows receiving messages from the Dead Letter queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Receive-Dead-Letter	4b6e08c0-df3c-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Configuration	Configuration parameters for a specific computer for routing decisions.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Receive-Dead-Letter Extended Right	http://msdn.microsoft.com/en-us/library/ms684387.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.10 msmq-Receive-Dead-Letter	http://msdn.microsoft.com/en-us/library/cc223592.aspx

2.37 msmq-Receive-journal Control Access Right

The 'msmq-Receive-journal' right is an extended right that allows receiving messages from the queue's Journal.

Control access right symbol	Identifying GUID used in ACE
msmq-Receive-journal	06bd3203-df3e-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Queue	Associated with a specific computer, under the MSMQ-Configuration.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Receive-journal Extended Right	http://msdn.microsoft.com/en-us/library/ms684389.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.17 msmq-Receive-journal	http://msdn.microsoft.com/en-us/library/cc223599.aspx

2.38 msmq-Send Control Access Right

The 'msmq-Send' right is an extended right that allows sending messages to the queue.

Control access right symbol	Identifying GUID used in ACE
msmq-Send	06bd3202-df3e-11d1-9c86-006008764d0e

Class Objects with this Extended Right:

AD Schema Class	Description
MSMQ-Group	Used to define a group of MSMQ queues (aka Distribution List).
MSMQ-Queue	Associated with a specific computer, under the MSMQ-Configuration.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
msmq-Send Extended Right	http://msdn.microsoft.com/en-us/library/ms684390.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.16 msmq-Send	http://msdn.microsoft.com/en-us/library/ms684390.aspx

2.39 Open-Address-Book Control Access Right

The 'Open-Address-Book' right is an extended right that is checked when opening an address book object for address book views.

Control access right symbol	Identifying GUID used in ACE
Open-Address-Book	a1990816-4298-11d1-ade2-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
Address-Book-Container	Holds members of an address book view.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Open-Address-Book Extended Right	http://msdn.microsoft.com/en-us/library/ms684393.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.62 Open-Address-Book	http://msdn.microsoft.com/en-us/library/cc223648.aspx

2.40 Read-Only-Replication-Secret-Synchronization Control Access Right

The 'Read-Only-Replication-Secret-Synchronization' right is an extended right needed to replicate object secret attributes to an RODC.

Control access right symbol	Identifying GUID used in ACE
Read-Only-Replication-Secret-Synchronization	1131f6ae-9c07-11d1-f79f-00c04fc2dcd2

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2008

MSDN References:

Title	URL
Read-Only-Replication-Secret-Synchronization Extended Right	http://msdn.microsoft.com/en-us/library/ms684398.aspx
[MS-ADTS] 3.1.1.3.3.17 replicateSingleObject	http://msdn.microsoft.com/en-us/library/cc223306.aspx
[MS-ADTS] 3.1.1.3.3.22 rODCPurgeAccount	http://msdn.microsoft.com/en-us/library/cc223850.aspx
[MS-ADTS] 3.1.1.3.4.1.24 LDAP_SERVER_INPUT_DN_OID	http://msdn.microsoft.com/en-us/library/cc223864.aspx
[MS-ADTS] 3.1.1.4.4 Extended Access Checks	http://msdn.microsoft.com/en-us/library/cc223383.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.74 Read-Only-Replication-Secret-Synchronization	http://msdn.microsoft.com/en-us/library/dd541413.aspx

2.41 Reanimate-Tombstones Control Access Right

The 'Reanimate-Tombstones' right is an extended right that allows deleted schema elements to be restored.

Control access right symbol	Identifying GUID used in ACE
Reanimate-Tombstones	45ec5156-db7e-47bb-b53f-dbeb2d03c40f

Class Objects with this Extended Right:

AD Schema Class	Description
Configuration	Holds the configuration information for a domain.
DMD	Holds the Active Directory schema.
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	AD-LDS (ADAM)	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Reanimate-Tombstones Extended Right	http://msdn.microsoft.com/en-us/library/ms684399.aspx
[MS-ADTS] 3.1.1.5.3 Modify Operation	http://msdn.microsoft.com/en-us/library/cc223454.aspx
[MS-ADTS] 3.1.1.5.3.2 Constraints	http://msdn.microsoft.com/en-us/library/cc223462.aspx
[MS-ADTS] 3.1.1.5.3.7.1 Undelete Security Considerations	http://msdn.microsoft.com/en-us/library/cc223468.aspx
[MS-ADTS] 3.1.1.5.5.4 Security Considerations	http://msdn.microsoft.com/en-us/library/cc223484.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.40 Reanimate-Tombstones	http://msdn.microsoft.com/en-us/library/cc223623.aspx

2.42 Recalculate-Hierarchy Control Access Right

The 'Recalculate-Hierarchy' right is an extended right to force the DS to recalculate the hierarchy.

Control access right symbol	Identifying GUID used in ACE
Recalculate-Hierarchy	0bc1554e-0a99-11d1-adbb-00c04fd8d5cd

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Recalculate-Hierarchy Extended Right	http://msdn.microsoft.com/en-us/library/ms684400.aspx
[MS-ADTS] 3.1.1.3.3.12 recalcHierarchy	http://msdn.microsoft.com/en-us/library/cc223301.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.4 Recalculate-Hierarchy	http://msdn.microsoft.com/en-us/library/cc223624.aspx

2.43 Recalculate-Security-Inheritance Control Access Right

The 'Recalculate-Security-Inheritance' right is an extended right needed to force DS to recompute ACL inheritance on a Naming Context.

Control access right symbol	Identifying GUID used in ACE
Recalculate-Security-Inheritance	62dd28a8-7f46-11d2-b9ad-00c04f79f805

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Recalculate-Security-Inheritance Extended Right	http://msdn.microsoft.com/en-us/library/ms684401.aspx
[MS-ADTS] 3.1.1.3.3.10 fixupInheritance	http://msdn.microsoft.com/en-us/library/cc223299.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.24 Recalculate-Security-Inheritance	http://msdn.microsoft.com/en-us/library/cc223299.aspx

2.44 Receive-As Control Access Right

The 'Receive-As' right is an extended right (Exchange) that allows receiving mail as a given mailbox.

Control access right symbol	Identifying GUID used in ACE
Receive-As	ab721a56-1e2f-11d0-9819-00aa0040529b

Class Objects with this Extended Right:

AD Schema Class	Description
Computer	Represents a computer account in the domain.
inetOrgPerson	Represents people associated with an organization.
User	Stores information about an employee, contractor or visitor that works for an organization.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Receive-As Extended Right	http://msdn.microsoft.com/en-us/library/ms684402.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.55 Receive-As	http://msdn.microsoft.com/en-us/library/cc223640.aspx

2.45 Refresh-Group-Cache Control Access Right

The 'Refresh-Group-Cache' right is an extended right for no GC logon. No GC logon relies on caching group memberships and this control access right is used to permission administrators/operators with rights to cause an immediate refresh of the cache, contacting an available G.C..

Control access right symbol	Identifying GUID used in ACE
Refresh-Group-Cache	9432c620-033c-4db7-8b58-14ef6d0bf477

Class Objects with this Extended Right:

AD Schema Class	Description
NTDS-DSA	Represents the Active Directory DSA process on the server.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Refresh-Group-Cache Extended Right	http://msdn.microsoft.com/en-us/library/ms684403.aspx
[MS-ADTS] 3.1.1.3.3.18 updateCachedMemberships	http://msdn.microsoft.com/en-us/library/cc223307.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.31 Refresh-Group-Cache	http://msdn.microsoft.com/en-us/library/cc223615.aspx

2.46 Reload-SSL-Certificate Control Access Right

The 'Reload-SSL-Certificate' right is an extended right used to renew Server Certificate (Reload SSL/TLS Certificate).

Control access right symbol	Identifying GUID used in ACE
Reload-SSL-Certificate	1a60ea8d-58a6-4b20-bcdc-fb71eb8a9ff8

Class Objects with this Extended Right:

AD Schema Class	Description

Implemented on:	

MSDN References:

Title	URL
[MS-ADTS] 3.1.1.3.3.21 renewServerCertificate	http://msdn.microsoft.com/en-us/library/cc223311.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.32 Reload-SSL-Certificate	http://msdn.microsoft.com/en-us/library/cc223851.aspx

2.47 SAM-Enumerate-Entire-Domain Control Access Right

The 'SAM-Enumerate-Entire-Domain' right is a special extended right that can be used to restrict who can be allowed to use downlevel API such as NetQueryDisplayInformation and NetUser/GroupEnum and enumerate the entire domain.

Control access right symbol	Identifying GUID used in ACE
SAM-Enumerate-Entire-Domain	91d67418-0135-4acc-8d79-c08e857cfbec

Class Objects with this Extended Right:

AD Schema Class	Description
Sam-Server	Holds a revision level and a security descriptor that specifies who can make RPC calls through the SAM interface.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL

Title	URL
SAM-Enumerate-Entire-Domain Extended Right	http://msdn.microsoft.com/en-us/library/ms684404.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.33 SAM-Enumerate-Entire-Domain	http://msdn.microsoft.com/en-us/library/cc223616.aspx
[MS-SAMR] 3.1.5.2.5 SamrEnumerateUsersInDomain (Opnum 13)	http://msdn.microsoft.com/en-us/library/cc245759.aspx
NetQueryDisplayInformation Function	http://msdn.microsoft.com/en-us/library/aa370610.aspx
NetGroupEnum Function	http://msdn.microsoft.com/en-us/library/aa370428.aspx

2.48 Send-As Control Access Right

The 'Send-As' right is an extended right (Exchange) that allows sending mail as the mailbox.

Control access right symbol	Identifying GUID used in ACE
Send-As	ab721a54-1e2f-11d0-9819-00aa0040529b

Class Objects with this Extended Right:

AD Schema Class	Description
Computer	Represents a computer account in the domain.
inetOrgPerson	Represents people associated with an organization.
User	Stores information about an employee, contractor or visitor that works for an organization.

Implemented on:	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Send-As Extended Right	http://msdn.microsoft.com/en-us/library/ms684406.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.54 Send-As	http://msdn.microsoft.com/en-us/library/cc223639.aspx

2.49 Send-To Control Access Right

The 'Send-To' right is an extended right (Exchange) that allows sending to a mailbox.

Control access right symbol	Identifying GUID used in ACE
Send-To	ab721a55-1e2f-11d0-9819-00aa0040529b

Class Objects with this Extended Right:

AD Schema Class	Description
Group	Stores a user name list for applying security principals on resources.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Send-To Extended Right	http://msdn.microsoft.com/en-us/library/ms684407.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.56 Send-To	http://msdn.microsoft.com/en-us/library/cc223641.aspx

2.50 Unexpire-Password Control Access Right

The 'Unexpire-Password' right is an extended right that allows a user to restore an expired password for a user object.

Control access right symbol	Identifying GUID used in ACE
Unexpire-Password	ccc2dc7d-a6ad-4a7a-8846-c04e3cc53501

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Unexpire-Password Extended Right	http://msdn.microsoft.com/en-us/library/ms684409.aspx
[MS-ADTS] 3.1.1.5.3.1 Security Considerations	http://msdn.microsoft.com/en-us/library/cc223455.aspx
[MS-ADTS] 3.1.1.5.3.3 Processing Specifics	http://msdn.microsoft.com/en-us/library/cc223463.aspx
[MS-ADTS] 3.1.1.8.10 userAccountControl	http://msdn.microsoft.com/en-us/library/cc245673.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.45 Unexpire-Password	http://msdn.microsoft.com/en-us/library/cc223629.aspx
[MS-SAMR] 3.1.1.8.6 dbcsPwd	http://msdn.microsoft.com/en-us/library/cc245687.aspx
[MS-SAMR] 3.1.1.8.7 unicodePwd	http://msdn.microsoft.com/en-us/library/cc245688.aspx
[MS-SAMR] 3.1.1.8.10 userAccountControl	http://msdn.microsoft.com/en-us/library/cc245673.aspx
NetUserSetInfo Function	http://msdn.microsoft.com/en-us/library/aa370659.aspx

2.51 Update-Password-Not-Required-Bit Control Access Right

The ‘Update-Password-Not-Required-Bit’ right is an extended right that allows a user to enable or disable the "password not required" setting for user objects.

Control access right symbol	Identifying GUID used in ACE
Update-Password-Not-Required-Bit	280f369c-67c7-438e-ae98-1d46f3c6f541

Class Objects with this Extended Right:

AD Schema Class	Description
Domain-DNS	Windows NT Domain with DNS-based (DC=) naming.

Implemented on:	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Update-Password-Not-Required-Bit Extended Right	http://msdn.microsoft.com/en-us/library/ms684410.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.44 Update-Password-Not-Required-Bit	http://msdn.microsoft.com/en-us/library/cc223628.aspx
[MS-SAMR] 3.1.1.8.10 userAccountControl	http://msdn.microsoft.com/en-us/library/cc245673.aspx

2.52 Update-Schema-Cache Control Access Right

The ‘Update-Schema-Cache’ right is an extended right used to force a schema cache update.

Control access right symbol	Identifying GUID used in ACE
Update-Schema-Cache	be2bb760-7f46-11d2-b9ad-00c04f79f805

Class Objects with this Extended Right:

AD Schema Class	Description
DMD	Holds the Active Directory schema.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
Update-Schema-Cache Extended Right	http://msdn.microsoft.com/en-us/library/ms684411.aspx

Title	URL
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.23 Update-Schema-Cache	http://msdn.microsoft.com/en-us/library/cc223606.aspx

2.53 User-Change-Password Control Access Right

The 'User-Change-Password' right is an extended right that allows changing the password on user account.

Control access right symbol	Identifying GUID used in ACE
User-Change-Password	ab721a53-1e2f-11d0-9819-00aa0040529b

Class Objects with this Extended Right:

AD Schema Class	Description
Computer	Represents a computer account in the domain.
inetOrgPerson	Represents people associated with an organization.
User	Stores information about an employee, contractor or visitor that works for an organization.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
User-Change-Password Extended Right	http://msdn.microsoft.com/en-us/library/ms684413.aspx
[MS-ADTS] 3.1.1.3.1.5.1 unicodePwd	http://msdn.microsoft.com/en-us/library/cc223248.aspx
[MS-ADTS] 3.1.1.5.3.1 Security Considerations	http://msdn.microsoft.com/en-us/library/cc223455.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.52 User-Change-Password	http://msdn.microsoft.com/en-us/library/cc223637.aspx
[MS-SAMR] 2.2.1.7 User ACCESS_MASK Values	http://msdn.microsoft.com/en-us/library/cc245525.aspx
[MS-SAMR] 3.1.5.12 Security Pattern	http://msdn.microsoft.com/en-us/library/cc245714.aspx
[MS-SAMR] 3.1.5.12.1.1 SamrSetSecurityObject (DC Configuration)	http://msdn.microsoft.com/en-us/library/cc245716.aspx
[MS-SAMR] 3.1.5.12.2.1 SamrQuerySecurityObject (DC Configuration)	http://msdn.microsoft.com/en-us/library/cc245719.aspx
MSChapSrvChangePassword Function	http://msdn.microsoft.com/en-us/library/ms697868.aspx

Title	URL
MSChapSrvChangePassword2 Function	http://msdn.microsoft.com/en-us/library/ms697869.aspx
NetUserChangePassword Function	http://msdn.microsoft.com/en-us/library/aa370650.aspx

2.54 User-Force-Change-Password Control Access Right

The 'User-Force-Change-Password' right is an extended right that permits resetting a password on user account.

Control access right symbol	Identifying GUID used in ACE
User-Force-Change-Password	00299570-246d-11d0-a768-00aa006e0529

Class Objects with this Extended Right:

AD Schema Class	Description
Computer	Represents a computer account in the domain.
inetOrgPerson	Represents people associated with an organization.
User	Stores information about an employee, contractor or visitor that works for an organization.

Implemented on:	AD-LDS (ADAM)	Win 2000	Win 2003	Win 2003 R2	Win 2008

MSDN References:

Title	URL
User-Force-Change-Password Extended Right	http://msdn.microsoft.com/en-us/library/ms684414.aspx
[MS-ADTS] 3.1.1.3.1.5.1 unicodePwd	http://msdn.microsoft.com/en-us/library/cc223248.aspx
[MS-ADTS] 3.1.1.5.3.1 Security Considerations	http://msdn.microsoft.com/en-us/library/cc223455.aspx
[MS-ADTS] 5.1.3.2.1 Control Access Rights	http://msdn.microsoft.com/en-us/library/cc223512.aspx
[MS-ADTS] 7.1.1.2.7.53 User-Force-Change-Password	http://msdn.microsoft.com/en-us/library/cc223638.aspx

3 Appendix A: Control Access Right to Object Class Cross-Reference

Control Access Right Symbol	Address-Book-Container Class	Computer Class	Configuration Class	Cross-Ref-Container Class	DMD Class	Domain-DNS Class	Group Class	Group-Policy-Container Class	inetOrgPerson Class	Infrastructure-Update Class	ms-DS-Quota-Container Class	MSMQ-Configuration Class	MSMQ-Group Class	MSMQ-Queue Class	NTDS-DSA Class	Organizational-Unit Class	PKI-Certificate-Template Class	RID-Manager Class	Sam-Server Class	Site Class	User Class
Abandon-Replication															x						
Add-GUID						x															
Allocate-Rids															x						
Allowed-To-Authenticate		x							x												x
Apply-Group-Policy								x													
Certificate-Enrollment																	x				
Change-Domain-Master				x																	
Change-Infrastructure-Master										x											
Change-PDC						x															
Change-Rid-Master																		x			
Change-Schema-Master					x																
Create-Inbound-Forest-Trust						x															
Do-Garbage-Collection															x						
Domain-Administer-Server																			x		
DS-Check-Stale-Phantoms															x						
DS-Execute-Intentions-Script				x																	
DS-Install-Replica						x															
DS-Query-Self-Quota											x										
DS-Replication-Get-Changes			x		x	x															
DS-Replication-Get-Changes-All			x		x	x															
DS-Replication-Get-Changes-In-Filtered-Set																					
DS-Replication-Manage-Topology			x		x	x															
DS-Replication-Monitor-Topology			x		x	x															
DS-Replication-Secrets-Synchronize																					
DS-Replication-Synchronize			x		x	x															
Enable-Per-User-Reversibly-Encrypted-Password						x															
Generate-RSoP-Logging						x										x					
Generate-RSoP-Planning						x										x					
Migrate-SID-History						x															
msmq-Open-Connector																				x	
msmq-Peek												x		x							
msmq-Peek-computer-Journal												x									
msmq-Peek-Dead-Letter												x									
msmq-Receive												x		x							
msmq-Receive-computer-Journal												x									
msmq-Receive-Dead-Letter												x									
msmq-Receive-journal														x							

Control Access Right Symbol	Address-Book-Container Class	Computer Class	Configuration Class	Cross-Ref-Container Class	DMD Class	Domain-DNS Class	Group Class	Group-Policy-Container Class	inetOrgPerson Class	Infrastructure-Update Class	ms-DS-Quota-Container Class	MSMQ-Configuration Class	MSMQ-Group Class	MSMQ-Queue Class	NTDS-DSA Class	Organizational-Unit Class	PKI-Certificate-Template Class	RID-Manager Class	Sam-Server Class	Site Class	User Class
msmq-Send													x	x							
Open-Address-Book	x																				
Read-Only-Replication-Secret-Synchronization																					
Reanimate-Tombstones			x		x	x															
Recalculate-Hierarchy															x						
Recalculate-Security-Inheritance															x						
Receive-As		x							x												x
Refresh-Group-Cache															x						
Reload-SSL-Certificate																					
SAM-Enumerate-Entire-Domain																			x		
Send-As		x							x												x
Send-To							x														
Unexpire-Password						x															
Update-Password-Not-Required-Bit						x															
Update-Schema-Cache					x																
User-Change-Password		x							x												x
User-Force-Change-Password		x							x												x