

Windows Management with Secure Scripting

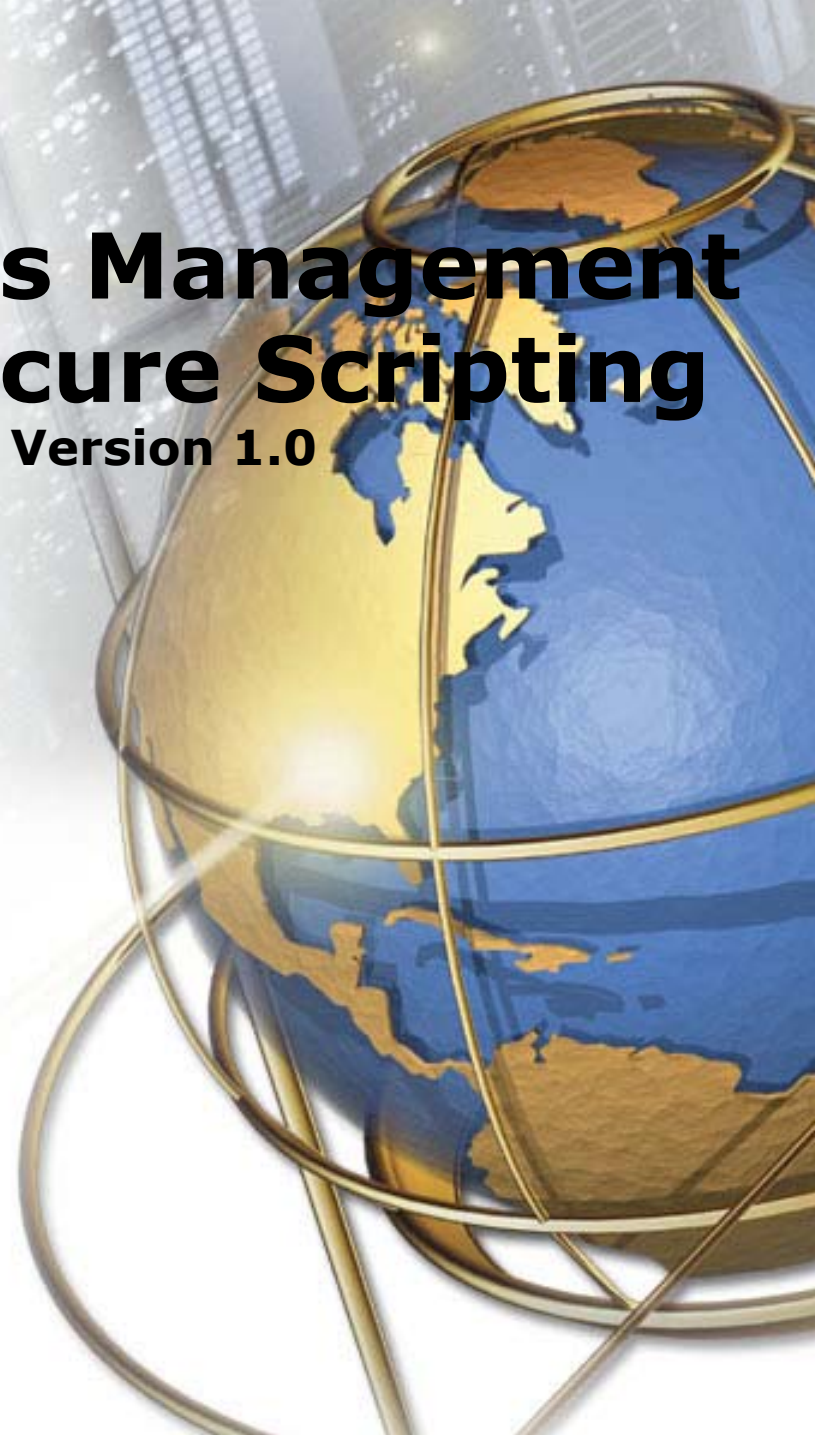
Version 1.0

Alain Lissair

(alain.lissair@hp.com)

HP Services

Technology Leadership Group



Objectives

Running trusted scripts safely!

**Features available in Windows
to manipulate security related items.**

Security Descriptors

Extended Rights

NT Event Log

System Monitoring

System modifications

Group memberships modifications

Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

A quick WSH review ...

WSH=Windows Scripting Host

Infrastructure to run scripts

First version (WSH 1.0) came with Option Pack 1.0

Support various languages

(by default: Jscript and VBScript)

Today WSH 5.6

(part of Windows XP/2003 and downloadable for Win9x, NT 4.0 and Win2K)

WSH features

Information on the running script

Digitally sign scripts (WinSAFER/SRP)
(Support of policies to determine the system behavior)

New

Create, retrieve and delete network drive connections

Access the environment

Access the registry

Run external programs

Drag and Drop support

Manipulate Desktop objects

Use scriptable COM objects
(ADSI, CDOEX, CDOEXM, WMI, ...)

Mix languages in a same script (XML)

Standard Output/Input/Error support

Windows Script Components (XML)

Code reusability (XML)

Run WSH scripts remotely

New

Network information

Command line argument reading (XML)

New

Signature samples ...

VBScript (.vbs)

```
" SIG " Begin signature block
" SIG " MIIRKQYJKoZIhvcNAQcCoIIRGjCCERYCAQExCzAJBgUr
" SIG " DgMCGgUAMGcGCisGAQQBgjcCAQSgWTBXMDIGCisGAQQB
...:
" SIG " s1t8ocWIRUefHOdMIZ7Bssx+SOnf+PUv81Evl9+aZCxK
" SIG " tgqZ4DWO88c=
" SIG " End signature block
```

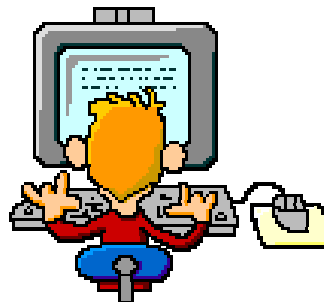
Jscript (.js)

```
// SIG // Begin signature block
// SIG // MIIRLQYJKoZIhvcNAQcCoIIRHjCCERoCAQExCzAJBgUr
// SIG // DgMCGgUAMGcGCisGAQQBgjcCAQSgWTBXMDIGCisGAQQB
...:
// SIG // a9TgqM7DGOOzKpaOUHodDDGxs71RqrGMU8rQO4f+6fF4
// SIG // g/quZ43MghAZ7/Sc
// SIG // End signature block
```

Windows Script File (.wsf)

```
<signature>
** SIG ** MIIKgyYJKoZIhvcNAQcCoIIIGzCCCCBcCAQExDjAMBggq
** SIG ** hkiG9w0CBQUAMGYGCisGAQQBgjcCAQSgWDBWMDIGCisG
...:
** SIG ** IokduL7pJDvNTZQ419aNZ777bP68fZC7oG59u6w0ZrA3
** SIG ** Raa8LhWRtH5HO0IRHEp
</signature>
```

Digitally Signing Scripts



Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

A quick ADSI review ...

ADSI=Active Directory Service Interface

Abstracts the interface to the Directory Service

Windows NT 4.0
IIS 4.x, 5.x, 6.x
Site Server 3.0
Exchange 5.5
Netware 3.x, 4.x, 5.x

Able to reach more than Active Directory

WSH + ADSI

➤ Provide the tools needed for unattended/remote administration

ADSI features

Bind to a Directory Object

Submit queries

Enumerate objects

Manage security

Move objects

Read/write properties

Rename objects

ADSI can be extended
(CDOEXM, WMI)

Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

The ADSI NT Security Descriptor

nTSecurityDescriptor

Security Descriptor

Owner



Group



Revision

Control

DiscretionaryACL

AccessControlEntry

Trustee
AccessMask
AceType
AceFlags
Flags

Trustee
AccessMask
AceType
AceFlags

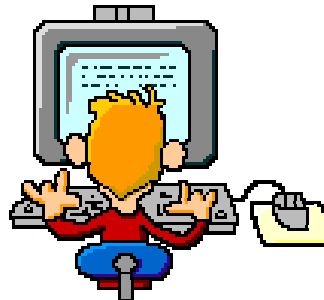
SystemACL

AccessControlEntry

Trustee
AccessMask
AceType
AceFlags
Flags

Trustee
AccessMask
AceType
AceFlags

ADSI Security Descriptor



Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

Extended Rights overview

The screenshot shows the ADSI Edit console window. The left pane displays a tree view of the directory structure, with 'CN=Extended-Rights' selected under the 'Configuration Container'. The right pane shows a list of 68 objects within this container, each with a name, class, and distinguished name.

Name	Class	Distinguished Name
CN=Abandon-Replication	controlAccessRight	CN=Abandon-Replicatio
CN=Add-GUID	controlAccessRight	CN=Add-GUID,CN=Ext
CN=Allocate-Rids	controlAccessRight	CN=Allocate-Rids,CN=E
CN=Apply-Group-Policy	controlAccessRight	CN=Apply-Group-Policy
CN=Certificate-Enrollment	controlAccessRight	CN=Certificate-Enrollme
CN=Change-Domain-Master	controlAccessRight	CN=Change-Domain-Ma
CN=Change-Infrastructure-Master	controlAccessRight	CN=Change-Infrastruc
CN=Change-PDC	controlAccessRight	CN=Change-PDC,CN=E
CN=Change-Rid-Master	controlAccessRight	CN=Change-Rid-Maste
CN=Change-Schema-Master	controlAccessRight	CN=Change-Schema-M
CN=Do-Garbage-Collection	controlAccessRight	CN=Do-Garbage-Collec
CN=Domain-Administer-Server	controlAccessRight	CN=Domain-Administer
CN=Domain-Password	controlAccessRight	CN=Domain-Password,
CN=DS-Check-Stale-Phantoms	controlAccessRight	CN=DS-Check-Stale-Ph
CN=DS-Install-Replica	controlAccessRight	CN=DS-Install-Replica,
CN=DS-Replication-Get-Changes	controlAccessRight	CN=DS-Replication-Get
CN=DS-Replication-Manage-Topology	controlAccessRight	CN=DS-Replication-Mar
CN=DS-Replication-Synchronize	controlAccessRight	CN=DS-Replication-Syn
CN=Email-Information	controlAccessRight	CN=Email-Information,
CN=General-Information	controlAccessRight	CN=General-Infoatio
CN=Membership	controlAccessRight	CN=Membership,CN=E
CN=ms-Exch-Add-PF-To-Admin-Group	controlAccessRight	CN=ms-Exch-Add-PF-T

Extended Right types

Enforced by Active Directory

Enforced by the system

Enforced by applications

LISSOIR Alain Properties

Environment | Sessions | Remote control | Terminal Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization | Published Certificates | Member Of | Dial-in | Object | Security

Group or user names:

- Enterprise Admins (LISSWARENET\Enterprise Admins)
- Everyone
- Exchange Enterprise Servers (LISSWARENET\Exchange Ente...)
- LISSOIR Alain (alain.lissoir@LissWare.NET)**
- Pre-Windows 2000 Compatible Access (LISSWARENET\Pre-...)

Permissions for LISSOIR Alain

	Allow	Deny
Write Logon Information	<input type="checkbox"/>	<input type="checkbox"/>
Read Personal Information	<input type="checkbox"/>	<input type="checkbox"/>
Write Personal Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read Phone and Mail Options	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write Phone and Mail Options	<input type="checkbox"/>	<input type="checkbox"/>
Read Public Information	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

OK Cancel Apply

LISSOIR Alain Properties

Environment | Sessions | Remote control | Terminal Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization | Published Certificates | Member Of | Dial-in | Object | Security

Group or user names:

- Enterprise Admins (LISSWARENET\Enterprise Admins)
- Everyone
- Exchange Enterprise Servers (LISSWARENET\Exchange Ente...)
- LISSOIR Alain (alain.lissoir@LissWare.NET)**
- Pre-Windows 2000 Compatible Access (LISSWARENET\Pre-...)

Permissions for LISSOIR Alain

	Allow	Deny
Change Password	<input type="checkbox"/>	<input type="checkbox"/>
Receive As	<input type="checkbox"/>	<input type="checkbox"/>
Reset Password	<input type="checkbox"/>	<input type="checkbox"/>
Send As	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read Account Restrictions	<input type="checkbox"/>	<input type="checkbox"/>
Write Account Restrictions	<input type="checkbox"/>	<input type="checkbox"/>
Read General Information	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

OK Cancel Apply

Enterprise Admins Properties

General | Members | Member Of | Managed By | Object | Security

Group or user names:

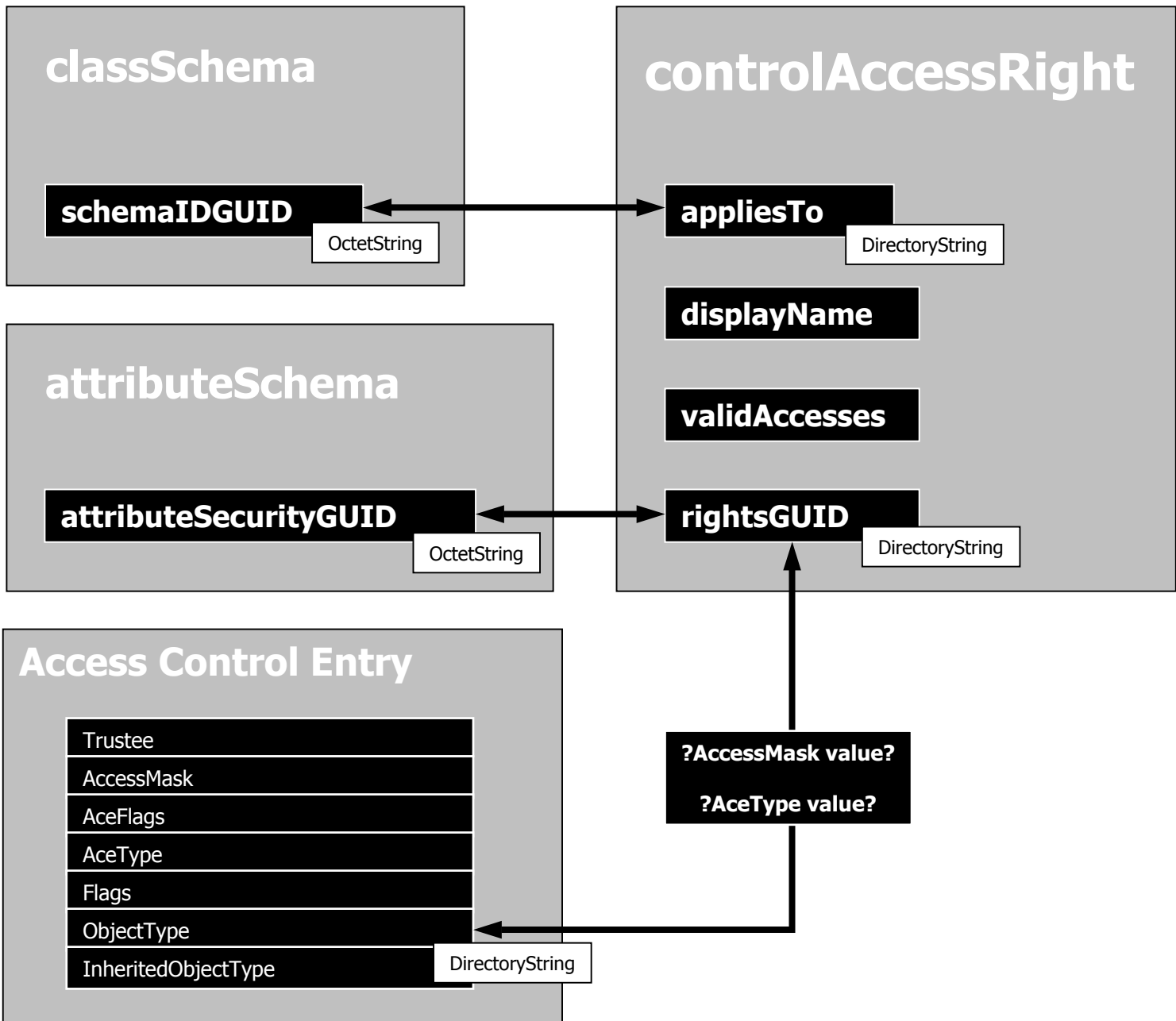
- Enterprise Admins (LISSWARENET\Enterprise Admins)
- Everyone
- Exchange Enterprise Servers (LISSWARENET\Exchange Ente...)
- LISSOIR Alain (alain.lissoir@LissWare.NET)**
- Pre-Windows 2000 Compatible Access (LISSWARENET\Pre-...)

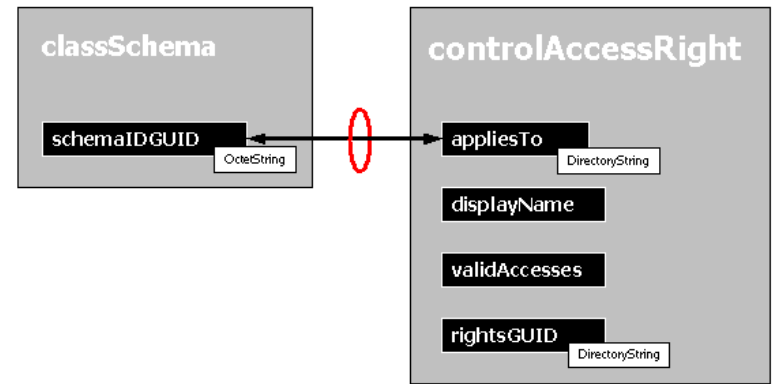
Permissions for LISSOIR Alain

	Allow	Deny
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete All Child Objects	<input type="checkbox"/>	<input type="checkbox"/>
Add/Remove self as member	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Send As	<input type="checkbox"/>	<input type="checkbox"/>
Send To	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or for advanced settings, click Advanced.

OK Cancel Apply





CN=User Properties [?] [X]

Attributes | Security

Path: LDAP://w2k-dpen6400.Myw2KDomain.Com/CN=User,CN=Sche

Class: classSchema

Select which properties to view: Both

Select a property to view: schemaIDGUID

Attribute Values

Syntax: OctetString

Edit Attribute:

Value(s): 0xba 0x7a 0x96 0xbf 0xe6 0x0d 0xd0 0x11 0xa2 0x85

[Set] [Clear]

[OK] [Cancel] [Apply]

CN=Personal-Information Properties [?] [X]

Attributes | Security

Path: LDAP://w2k-dpen6400.Myw2KDomain.Com/CN=Personal-Inform

Class: controlAccessRight

Select which properties to view: Both

Select a property to view: appliesTo

Attribute Values

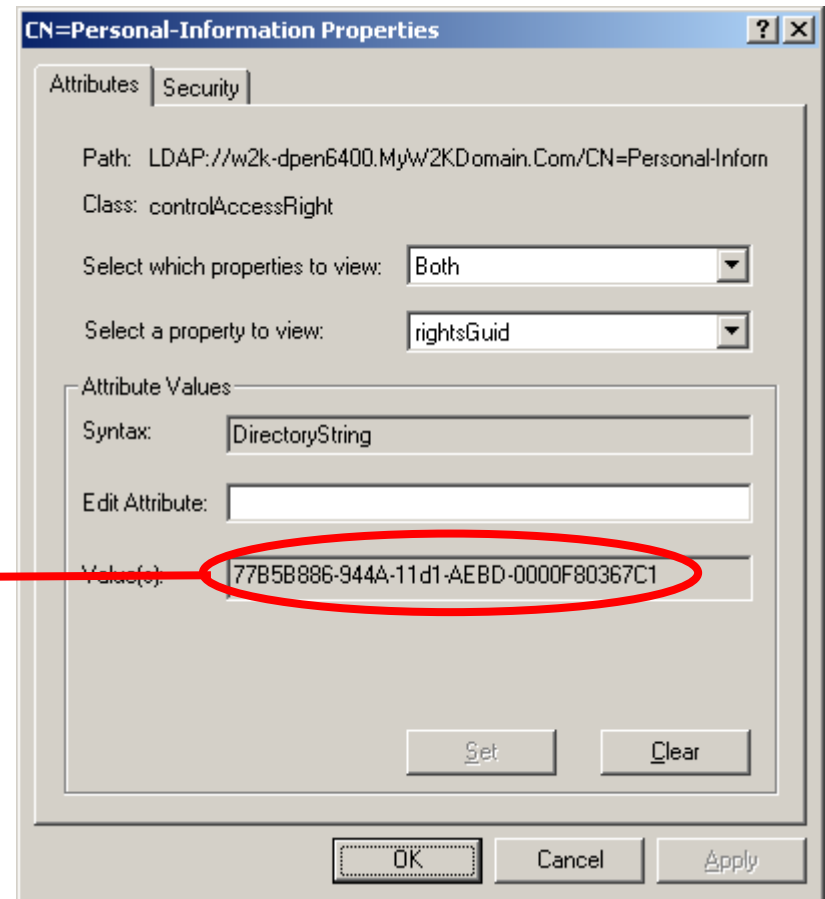
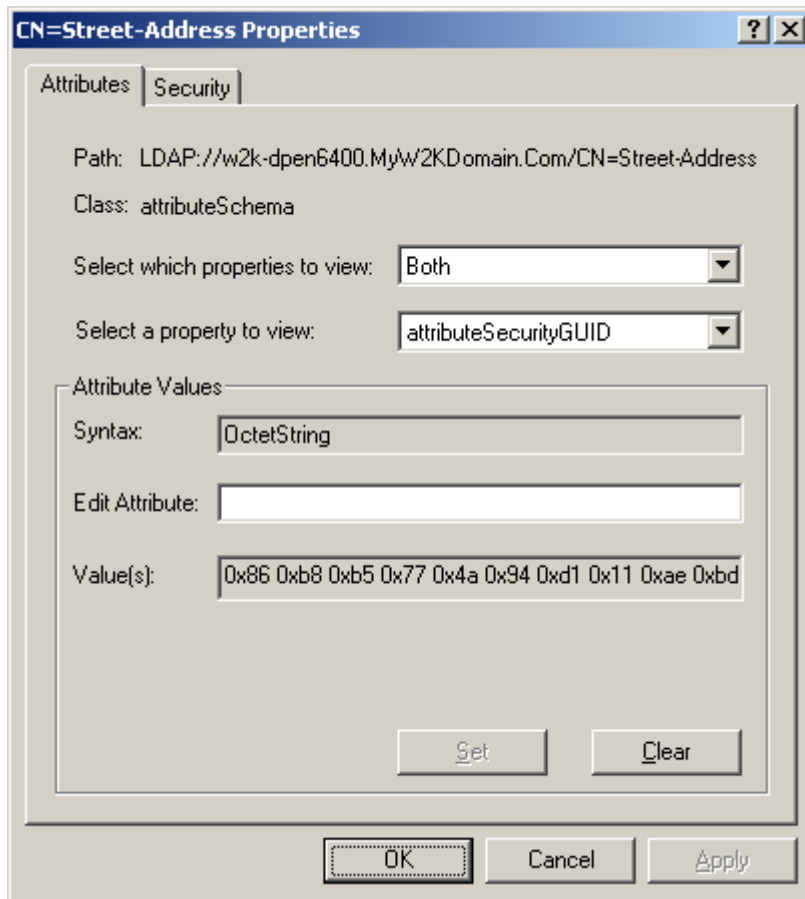
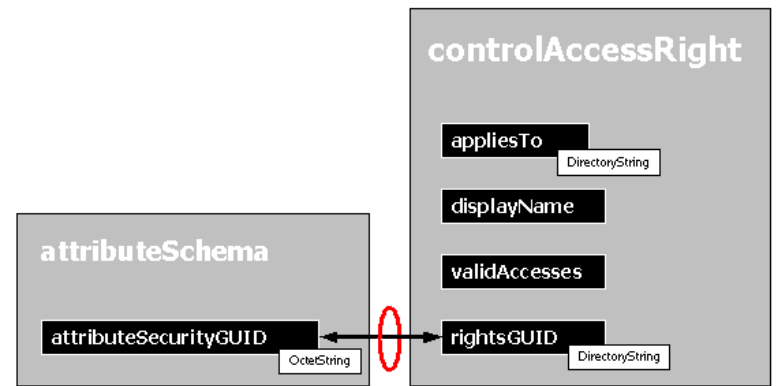
Syntax: DirectoryString

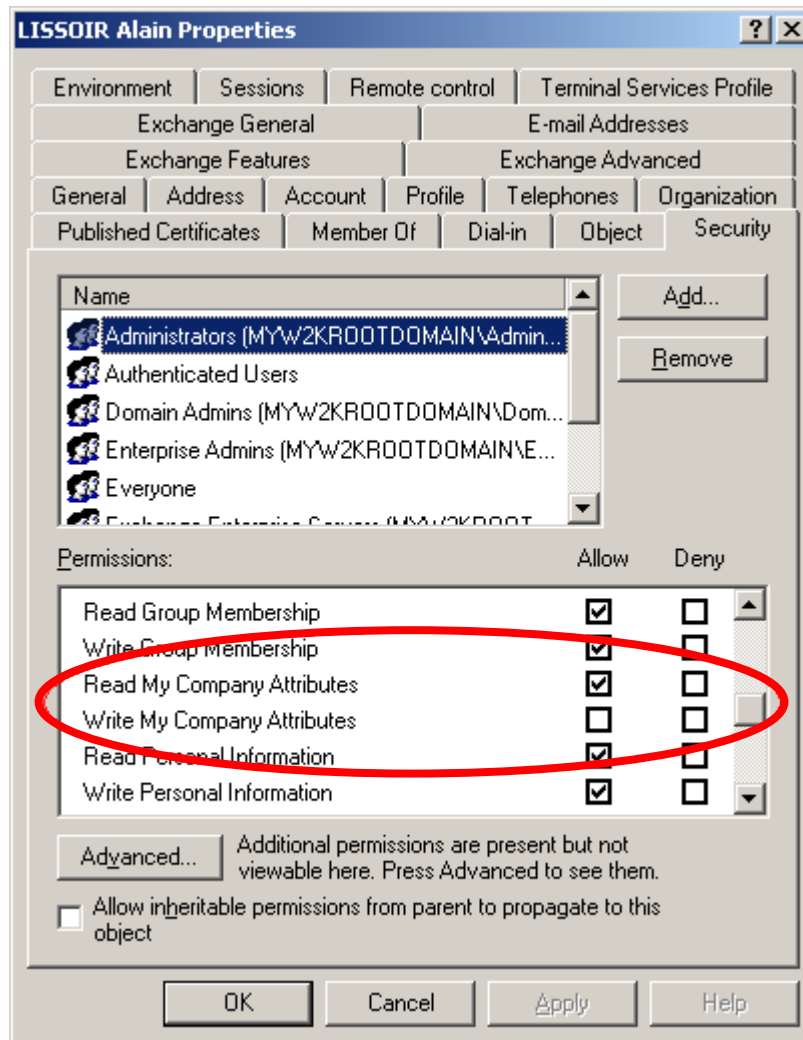
Edit Attribute:

Value(s): bf967a86-0de6-11d0-a285-00aa003049e2
5cb41e38-0e4c-11d0-az08-00aa003049e2
bf967aba-0de6-11d0-a285-00aa003049e2

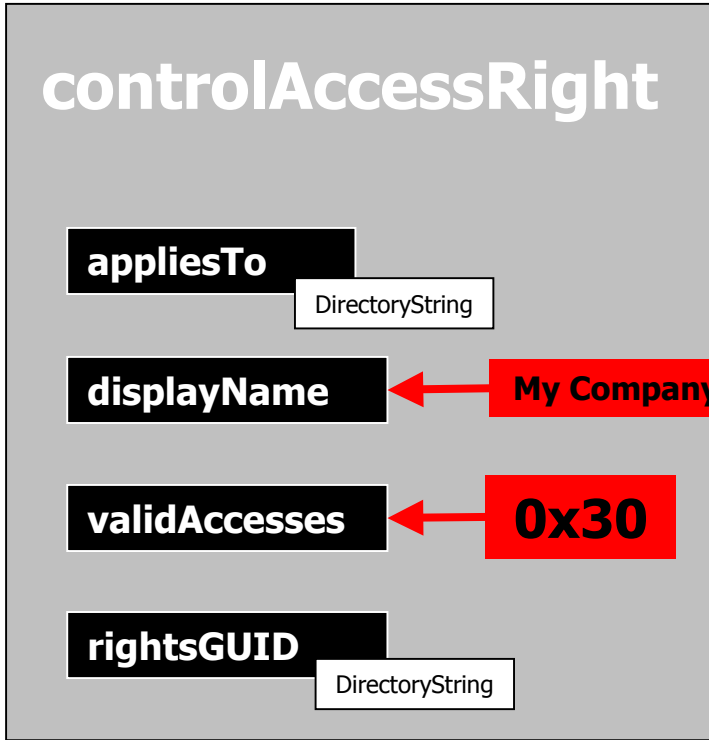
[Add] [Remove]

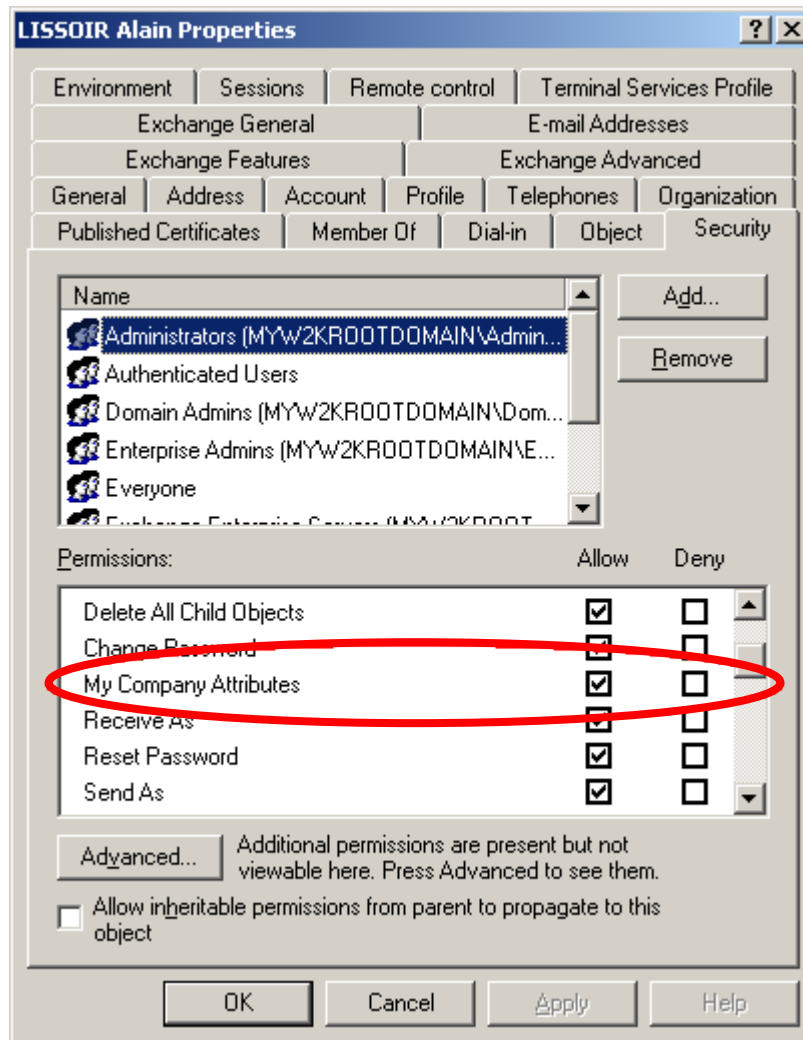
[OK] [Cancel] [Apply]



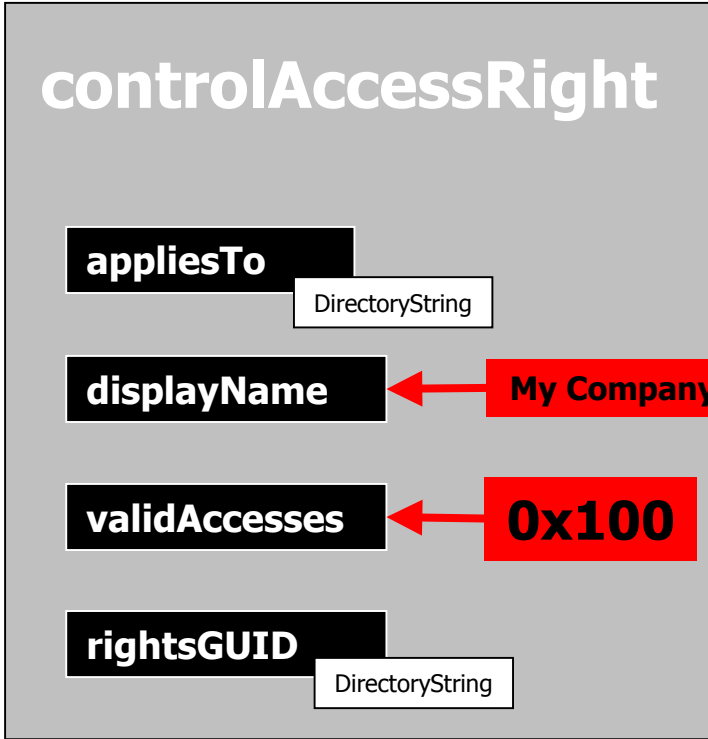


This type of right is enforced by Active Directory.

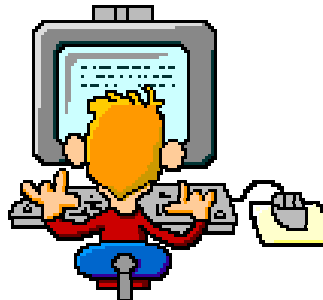




This is the application responsibility to validate the right.



Extended Rights Creation and Assignments



Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

Origin

DMTF=Distributed Management Task Force

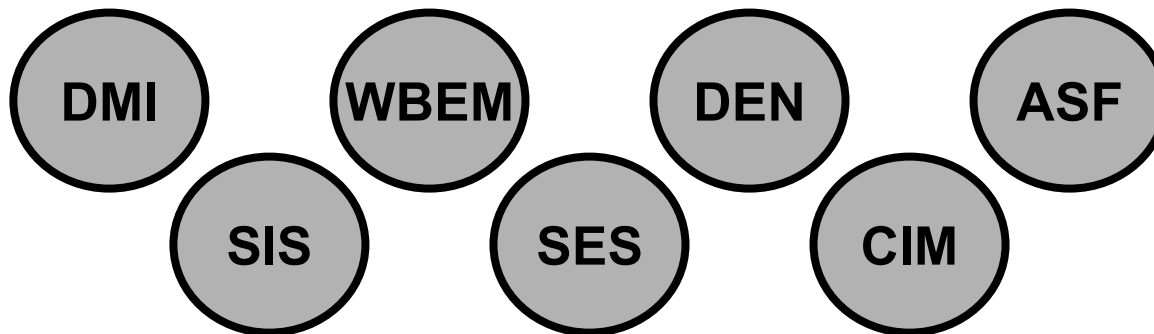
Originates from DMTF founded in 1992

DMTF members



<http://www.dmtf.org>

Provides a standard for enterprise system managers.



DMTF initiatives

DMI=Desktop Management Interface
(Standard for managing and tracking components in a PCs)

WBEM=Web-Based Enterprise Management
(Unify the management of enterprise computing environments)

CIM=Common Information Model
(Implementation-neutral schema to describe overall management information)

DEN=Directory Enabled Network
(Specification designed to provide building blocks for intelligent networks)

ASF=Alert Standard Forum
(Defining management that best serve clients' OS-absent environments)

SIS=Service Incident Standard and SES=Solution Exchange Standard
(Standards for customer support and helpdesk applications)

DMTF initiatives

WBEM=Web-Based Enterprise Management
(Unify the management of enterprise computing environments)

CIM=Common Information Model
(Implementation-neutral schema to describe overall management information)

Windows NT 4.0: ± 15 WMI providers
Windows 2000: ± 29 WMI providers
Windows Server 2003: ± 84 WMI Providers

WMI features

Various Windows components

DFS



Power Management

Cluster



Server Session

NT Event Logs

IIS



Terminal Server

Windows Clock



Operating System

AD replication

Disk Quota

Ping

Registry

VSS

Trust monitoring

SNMP

IP Routing



RSOP



Event Consumers

Network Load Balancing

MSI

Security

High Performance Data Access

Windows Applications

Exchange

Office

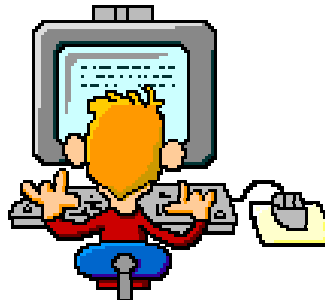
SQL

SMS

MOM

Management and monitoring (events)

WMI Security Group Monitoring Demo



Topics

- WSH review
- ADSI review
 - ADSI NT Security Descriptor
 - Extended Rights
- What is WMI?
- Resources

Windows & .NET Magazine

- Diving into the Active Directory Schema
<http://www.winnetmag.com/Articles/Index.cfm?ArticleID=21839>
- Extending the Active Directory Schema
<http://www.winnetmag.com/Articles/Index.cfm?ArticleID=22540>
- Secure Script Execution with WSH 5.6
<http://www.winscriptingsolutions.com/Articles/Index.cfm?ArticleID=25644>
- Exchange 2000 SP2 CDOEXM updates
<http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=27211>
- Exchange 2000 SP2 WMI updates
<http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=38190>

Microsoft MSDN

- Microsoft ADSI MSDN Library (SDK)

http://msdn.microsoft.com/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp

- Active Directory Access Control

http://msdn.microsoft.com/library/en-us/netdir/ad/controlling_access_to_active_directory_objects.asp

- Microsoft WMI MSDN Library (SDK)

http://msdn.microsoft.com/library/en-us/wmisdk/wmi/wmi_start_page.asp

Microsoft TechNET

- Automating Exchange 2000 Management with Windows Script Host

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/maintain/featusability/ex2kwsh.asp>

Compaq/HP White Papers

■ Compaq Active Answers

(Alain Lissor – Hewlett Packard)

Part 1 - Understanding Microsoft WSH and ADSI in Windows 2000.

Part 2 - The powerful combination of WSH and ADSI under Windows 2000.

Part 1 - Introduction to the use of Exchange 2000 with Windows Script Host.

Part 2 - Managing Exchange with Scripts - Advanced Topics.

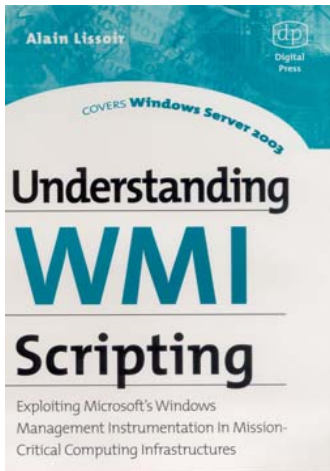
<http://activeanswers.compaq.com/ActiveAnswers/Render/1,1027,2366-6-100-225-1,00.htm>

Under the « Available Information » selection box,

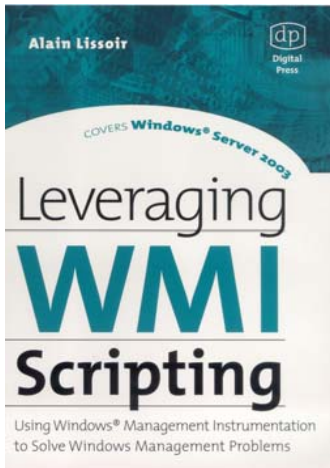
select the « Technology » section ,

next, select « Windows 2000 and Exchange ».

WMI Books covering Windows Server 2003 (from NT 4.0)



- Understanding WMI Scripting (Volume 1)
 - ISBN 1555582664 – Digital Press
(Alain Lissoir – Hewlett Packard)
 - April 2003
 - More on <http://www.LissWare.Net>



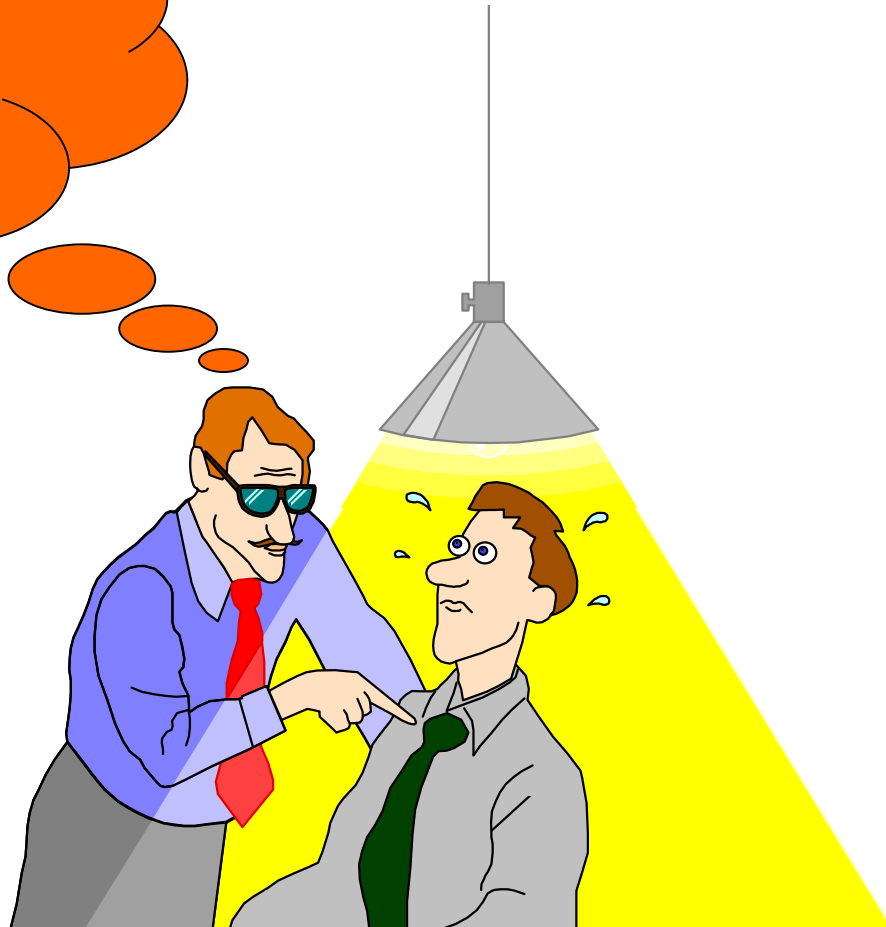
- Leveraging WMI Scripting (Volume 2)
 - ISBN 1555582990 – Digital Press
(Alain Lissoir – Hewlett Packard)
 - June 2003
 - More on <http://www.LissWare.Net>

Demonstration scripts

- Demo Kit available at:

[http://users.skynet.be/alain.lissoir/conferences/Managing%20Windows%20with%20Secure%20Scripting%20\(ScriptKit\).zip](http://users.skynet.be/alain.lissoir/conferences/Managing%20Windows%20with%20Secure%20Scripting%20(ScriptKit).zip)

***Any
questions?***





i n v e n t