

# The Experts s Conference

## An In-Depth Look at AdminSDHolder, Protected Objects, and SDPROP

John Policelli

Presented by:



Sponsored by:



# Agenda

- Overview
- AdminSDHolder
- Protected Objects
- Security Descriptor Propagator
- Recommendations

# Overview

## The Requirements

- Provide additional protection for privileged security principals
- Restrict the permissions to modify and delete privileged security principals
- Ensure the modification of a privileged security principal's Security Descriptor does not reduce the protection

# Overview

## The Solution

- Defines the security principals that must be protected
- Applies a separate and more secure Security Descriptor on protected objects
- Enforces the Security Descriptor on protected objects

# Overview

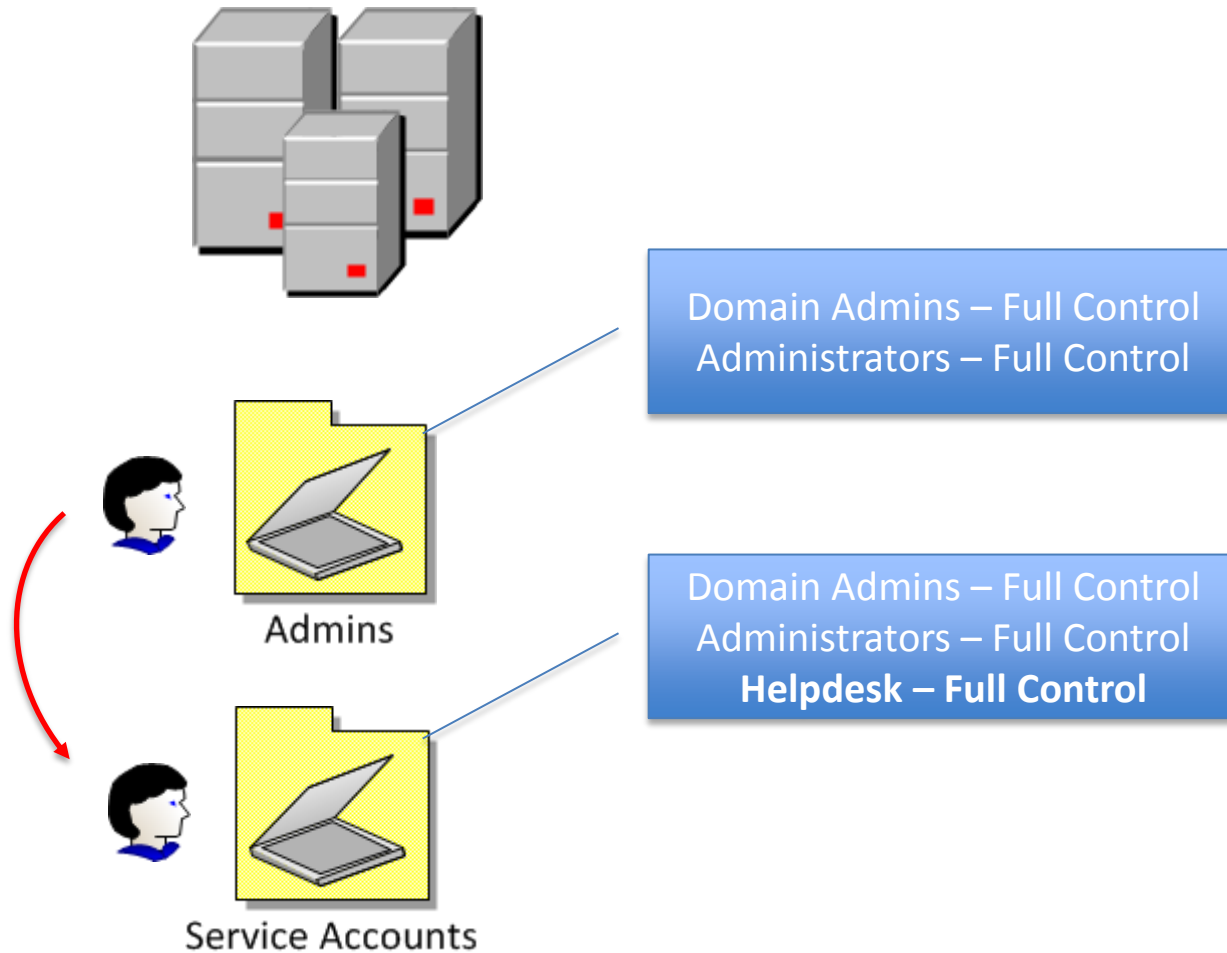
## The Components

- AdminSDHolder
- Protected Objects
- Security Descriptor Propagator

# Demo

## Active Directory Permissions without AdminSDHolder

# Active Directory Permissions without AdminSDHolder



# AdminSDHolder

- How AdminSDHolder Works
- The AdminSDHolder Background Process
- Default Security Descriptor on the AdminSDHolder Object
- The Frequency AdminSDHolder Runs
- Forcing AdminSDHolder to Run

# How AdminSDHolder Works

- **Domain-wide AdminSDHolder object**
  - CN=AdminSDHolder,CN=System,DC=domain,DC=local
- **Unique Security Descriptor**
  - More secure
- **Protected Objects**
  - Active Directory groups and users that should be protected by AdminSDHolder
- **Background process that runs on DCs**
  - Ensures the Security Descriptor on protected objects and the Security Descriptor on the AdminSDHolder object match

# The AdminSDHolder Background Process

- A process that runs every 60 minutes on PDC Emulators
- Compares the Security Descriptor on protected objects against the Security Descriptor on the AdminSDHolder object
- If the Security Descriptors are different, overwrites the Security Descriptor with that of the AdminSDHolder object

# Default Security Descriptor on the AdminSDHolder Object

- More stringent than default Domain, OU, and container Security Descriptors
  - Default Owner is Domain Admins
  - Inheritance is disabled by default
- Write, Create, and Delete permissions are limited to the Administrators, Domain Admins, and Enterprise Admins groups

# The Frequency AdminSDHolder Runs

- AdminSDProtectFrequency subkey can be used to modify frequency AdminSDHolder runs
  - Between 1 minute to 2 hours
  - HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
- Addition of subkey does not take effect until LSA reinitializes
  - Reboot
  - Restart of NTDS service (WS08 + WS08R2)
- Modifying this subkey is not recommended

# Forcing AdminSDHolder to Run

- Windows Server 2008 R2
  - runProtectAdminGroupsTask rootDSE modify operation
  - Forces the DC to run the AdminSDHolder protection operation
  - Must be run on the PDC to have an effect
  - Requires "Run-Protect-Admin-Groups-Task" control access right
- Windows 2000 Server - Windows Server 2008 R2
  - fixupInheritance rootDSE modify operation
  - Does not actually force the AdminSDHolder protection operation
  - DC recomputes inherited security permissions to ensure they conform to Security Descriptor requirements
  - Takes longer to complete
  - Requires "Recalculate-Security-Inheritance" control access right

# Demo

## Forcing AdminSDHolder to Run

# Protected Objects

- Default Protected Objects
- Excluding Operator Groups Protected by AdminSDHolder
- Using dSHeuristics to Exclude Operator Groups
- Using dSHeuristics to Exclude Multiple Operator Groups
- Determining whether an Object is Protected
- Orphaned Protected Objects

# Default Protected Objects

Win2K RTM Win2K with SP1 Win2K with SP2 Win2K with SP3	Win2K with SP4 WS03 RTM	WS03 with SP1 WS03 with SP2	WS08 RTM WS08 R2
Administrators	Account Operators	Account Operators	Account Operators
Domain Admins	Administrator	Administrator	Administrator
Enterprise Admins	Administrators	Administrators	Administrators
Schema Admins	Backup Operators	Backup Operators	Backup Operators
	Domain Admins	Domain Admins	Domain Admins
	Domain Controllers	Domain Controllers	Domain Controllers
	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Krbtgt	Krbtgt	Krbtgt
	Print Operators	Print Operators	Print Operators
	Replicator	Replicator	Replicator
	Schema Admins	Schema Admins	Schema Admins
	Server Operators	Server Operators	Server Operators
	Cert Publishers		Read-Only Domain Controllers

# Excluding Operator Groups Protected by AdminSDHolder

- The forest-wide dSHeuristics flag can be used to control which Operator groups are protected by AdminSDHolder
  - Account Operators
  - Server Operators
  - Print Operators
  - Backup Operators
- Functionality is included with Windows Server 2003 SP2 and later
- Hotfix is required for pre-Windows Server 2003 SP2 - [KB817433](#)

# Using dSHeuristics to Exclude Operator Groups

- A Unicode string in which each character contains a value for a single forest-wide setting - *0000000000100000X*
- 16<sup>th</sup> character is for the Operator group(s) you want to exclude
- The valid values of this field are characters from the set "0"–"9" and "a"–"f"

Bit	Group to Exclude	Binary Value	Hexadecimal Value
0	Account Operators	0001	1
1	Server Operators	0010	2
2	Print Operators	0100	4
3	Backup Operators	1000	8

# Using dSHeuristics to Exclude Multiple Operator Groups

- Add the binary value of each group and then convert the result to a hexadecimal value

Group(s) To Exclude	Binary	Hex
None (Default)	0000	0
Account Operators	0001	1
Server Operators	0010	2
Account Operators Server Operators	$0001 + 0010 = \mathbf{0011}$	3
Print Operators	0100	4
Account Operators Print Operators	$0001 + 0100 = \mathbf{0101}$	5
Server Operators Print Operators	$0010 + 0100 = \mathbf{0110}$	6
Account Operators Server Operators Print Operators	$0001 + 0010 + 0100 = \mathbf{0111}$	7
Backup Operators	1000	8
Account Operators Backup Operators	$0001 + 1000 = \mathbf{1001}$	9

Group(s) To Exclude	Binary	Hex
Server Operators Backup Operators	$0010 + 1000 = \mathbf{1010}$	a
Account Operators Server Operators Backup Operators	$0001 + 0010 + 1000 = \mathbf{1011}$	b
Print Operators Backup Operators	$0100 + 1000 = \mathbf{1100}$	c
Account Operators Print Operators Backup Operators	$0001 + 0100 + 1000 = \mathbf{1101}$	d
Server Operators Print Operators Backup Operators	$0010 + 0100 + 1000 = \mathbf{1110}$	e
Account Operators Server Operators Print Operators Backup Operators	$0001 + 0010 + 0100 + 1000 = \mathbf{1111}$	f

# Determining whether an Object is Protected

- Security principals are protected if they have direct or transitive membership in a security or distribution group
- The adminCount attribute can be queried to determine if an object is protected by AdminSDHolder
- To find all user objects in a domain that are protected by AdminSDHolder:

```
Get-ADUser -LDAPFilter "(objectcategory=person)(samaccountname=*)(admincount=1)"
```

- To find all groups in a domain that are protected by AdminSDHolder:

```
Get-ADGroup -LDAPFilter "(objectcategory=group)(admincount=1)"
```

# Orphaned Protected Objects

- The adminCount attribute on the object does not change and the status of inheritance is not changed
  - Same for users, groups, and excluded groups
- When an object is removed from a protected group:
  - The object no longer receives its ACL from the AdminSDHolder object
  - By default, object does not inherit any permissions from parent objects
- No automated method for dealing with orphaned AdminSDHolder objects
- MS VBScript: [KB817433](#)

# Demo



## Using dSHeuristics to Exclude Multiple Operator Groups

# Demo

## Determining whether an Object is Protected

# Security Descriptor Propagator

- Used to propagate the changes of inheritable ACEs to descendent objects
- DCs run a background task called the Security Descriptor Propagator Update task
- Task is triggered by a modification to the security descriptor for an object or when an object is moved
- Is not responsible for AdminSDHolder protection

# Recommendations

- Avoid Excluding Operator Groups from AdminSDHolder Protection
- Implement a Regular Process for Orphaned Protected Objects
- Follow Security Best Practices
- Avoid Adding ACEs to the AdminSDHolder Object
- Use Dsacls.exe to add ACEs to AdminSDHolder

# Avoid Excluding Operator Groups from AdminSDHolder Protection

- Operator groups are protected because they have significant privileges

User Rights Assignment	Account Operators	Backup Operators	Print Operators	Server Operators
Allow log on locally	◆	◆	◆	◆
Back up files and directories		◆		◆
Change the system time				◆
Force shutdown from a remote system				◆
Load and unload device drivers			◆	
Log on as a batch job		◆		
Restore files and directories		◆		◆
Shut down the system		◆	◆	◆

- Keep Operator groups protected OR remove their User Rights Assignments

# Follow Security Best Practices

- Use separate accounts for administration
  - Do not use day-to-day accounts for administration
  - Do not add day-to-day accounts to protected groups
- Harden GPOs applied to DCs
- Regularly audit membership in protected groups

# Avoid Adding ACEs to the AdminSDHolder Object

- Common issue for AdminSDHolder escalation stems from the use of day-to-day accounts for administration
- Typically addressed by adding ACEs to AdminSDHolder object
- Adding ACEs to AdminSDHolder object can cause security risks
- Use separate accounts for administration, which eliminates the need to add ACEs to AdminSDHolder

# Implement a Regular Process for Orphaned Protected Objects

- When an object is removed from a protected group, adminCount and the status of inheritance is not changed
- You must address permissions and inheritance when an object goes from protected to not protected
- Use the MS VBScript in [KB817433](#) or develop your own scheduled process

# Use Dsaccls.exe to add ACEs to AdminSDHolder

- Security tab of the AdminSDHolder object does not display all properties
- You are unable to configure fields that are associated with user accounts or groups
  - [KB301188](#)
- AdminSDHolder is a container object used only as a template to store permissions
- Modify the permissions of this object through Dsaccls.exe or write an ADSI script

# Additional Information

- <http://policelli.com/blog>
- [Understanding AdminSDHolder and Protected Groups](#)
- [Ask the Directory Services Team – Five common questions about and AdminSDHolder and SDProp](#)
- [Description and Update of the Active Directory AdminSDHolder Object](#)
- [Manually initializing the SD propagator thread to evaluate inherited permissions for objects in Active Directory](#)
- [Delegated permissions are not available and inheritance is automatically disabled](#)
- [rootDSE Modify Operations Open Specifications Document](#)
- [runProtectAdminGroupsTask Open Specifications Document](#)
- [AdminSDHolder Open Specifications Document](#)
- [LDAP modify operations](#)