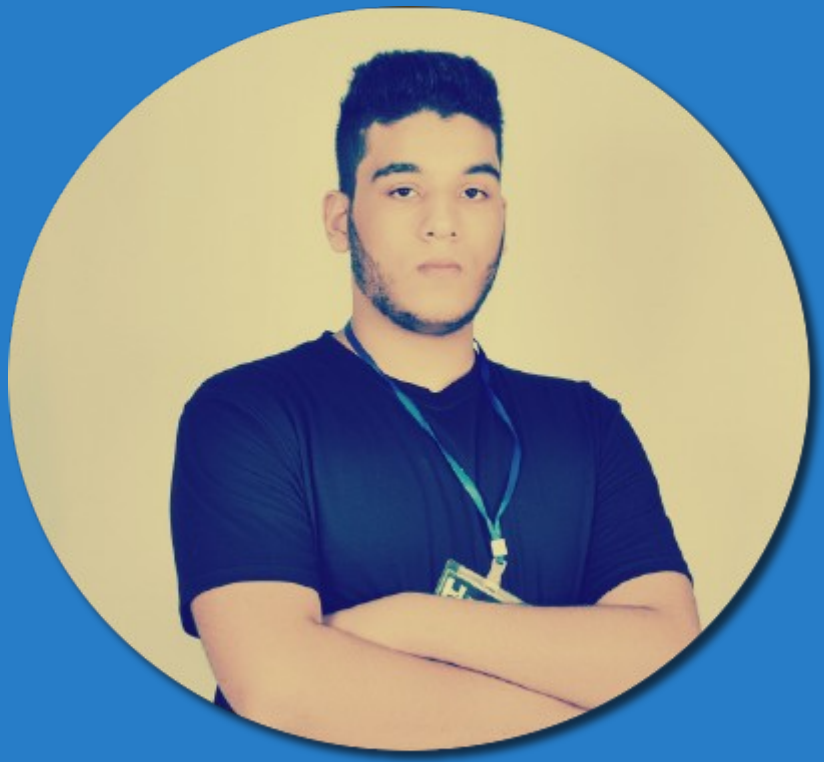
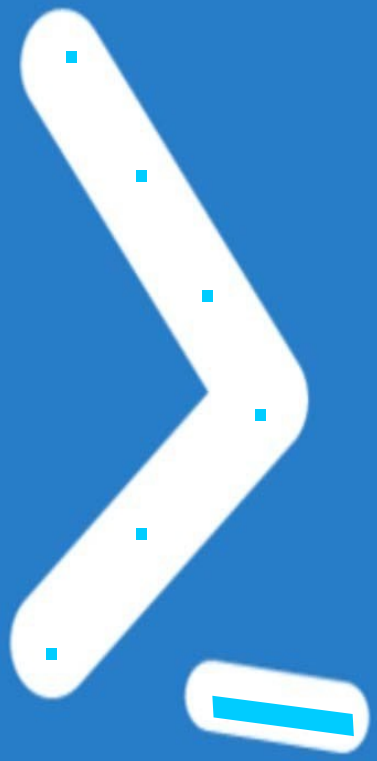
@Authors

@DanielUlrichs



@matt-homjx0ie

@matt-homjx0ie



1 Environment Active Directory/A-D

2 Protection materials in A-D

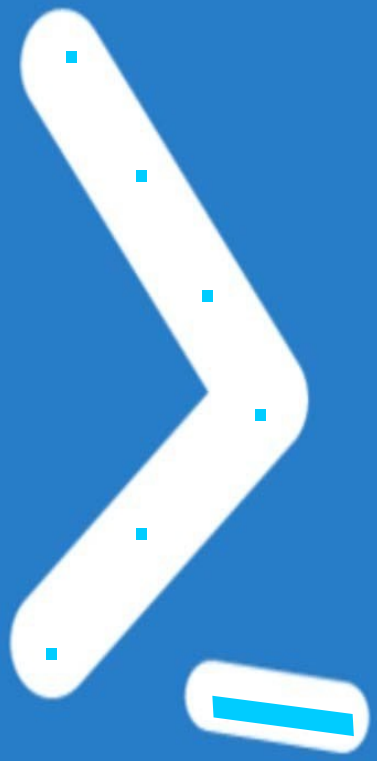
3 What is Environment A-D

4 And What is Protection materials in A-D

Example / ACLS/DACL/ACES/ !

@matt-homjx0ie

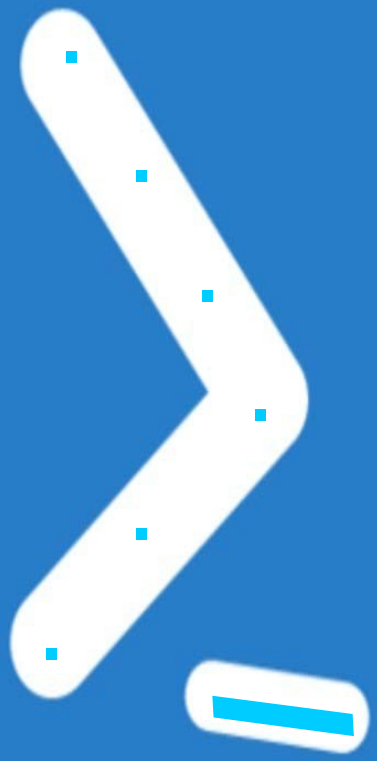
What is Environment Active Directory/A-D 1 //



Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.[1][2] Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.[3]

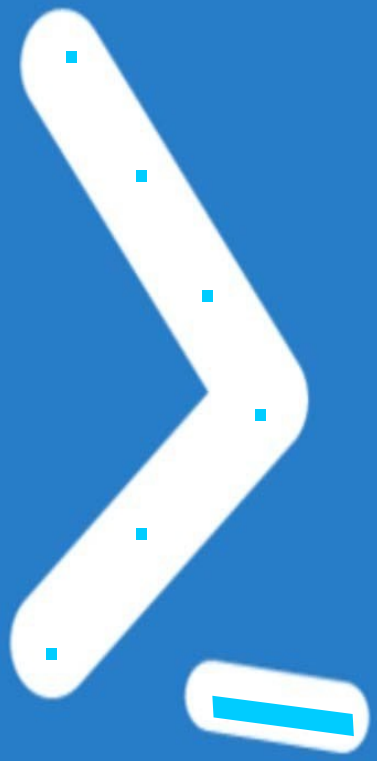
@matt-homjx0ie

What is Environment Active Directory/A-D 2 //



A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.[4] Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Federated Services, Lightweight Directory Services and Rights Management Services.[5]

@matt-homjx0ie



// ACLS-Active Directory

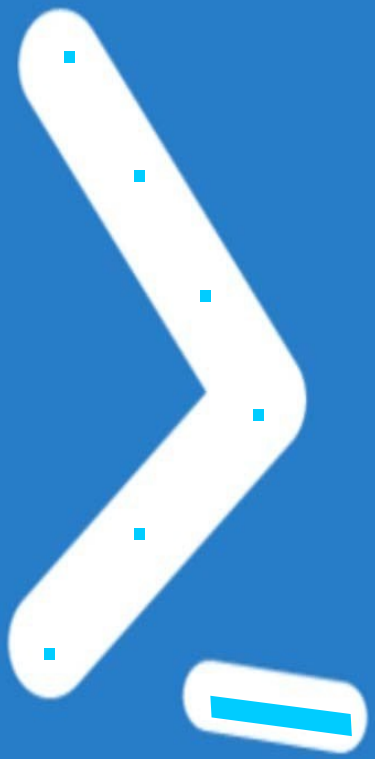
ACLS

ACE

DACL

@matt-homjx0ie

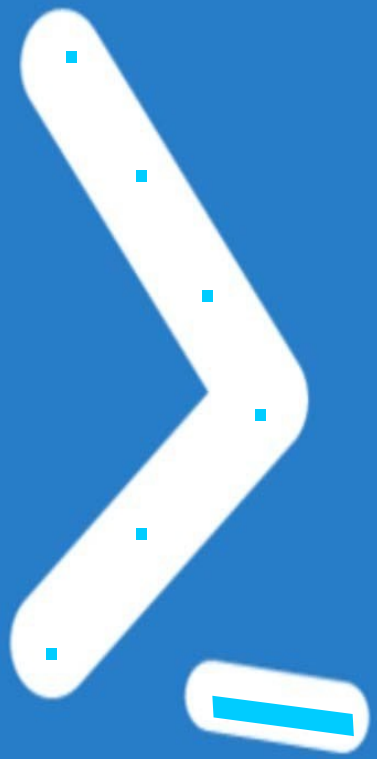
What is ACLS



ACLs, Access Control List is a security concept, where a list of individual users or groups can have specific access to certain actions to a file. An example would be in respect to the above overview image, where the accountant can have write access to update the file. The sales manager can review the file, and other users are denied access /

@matt-homjx0ie

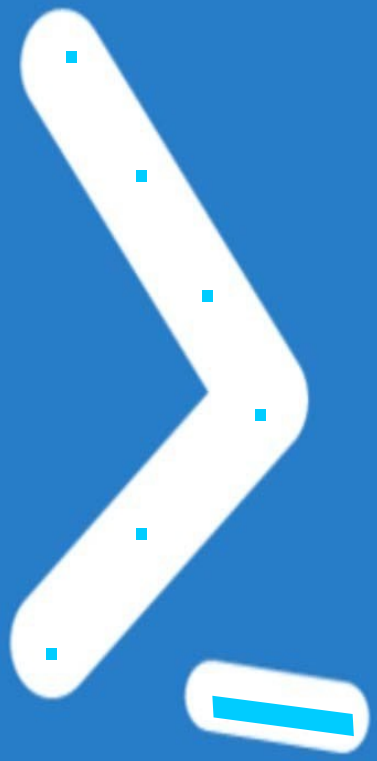
What is ACLS 2



Windows ACL allows the QNAP NAS administrator to configure file and folder permissions for the local and domain users on the NAS from Windows Explorer. The administrator can add, modify, and remove Windows ACL permissions of the NAS on Windows XP, Vista, Windows 7, Windows Server 2003, and Windows 2008 /

@matt-homjx0ie

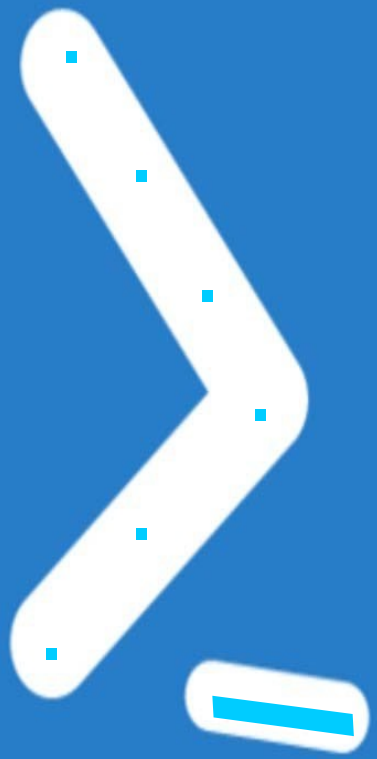
What Is / ACE / Access Control Cntries



Each permission ACE is made up of several pieces of information:
Trustee
The SID of the user or group to which the ACE applies, such as the SID for the
group COHOVINES\Domain Admins.
ACE Type
Determines whether the ACE is an allow or a deny.
Object Type
The schemaIDGUID for the attribute or object class that the ACE applies to or the
rightsGuid for the property set, validated write, or extended right that the ACE
applies to (such as the member attribute, Personal Information property set,
Change Password extended right, or user objects). For

@matt-homjx0ie

What is / Access Control Cntries / 2



And Delete or Create Child Ob
jects permissions, the objectType should be configured to the schemaIDGUID of the
object class delegated.

Inherited Object Type

The schemaIDGUID for the types of object that the ACE applies to when an attribute,
property set, or validated right is specified or when the ACE is inherited—e.g., user
objects.

Access Mask

A bit flag that describes the type of access, such as Read, Write, List, Create, Delete,
Control Access, etc. See Table 16-1 for more detail.

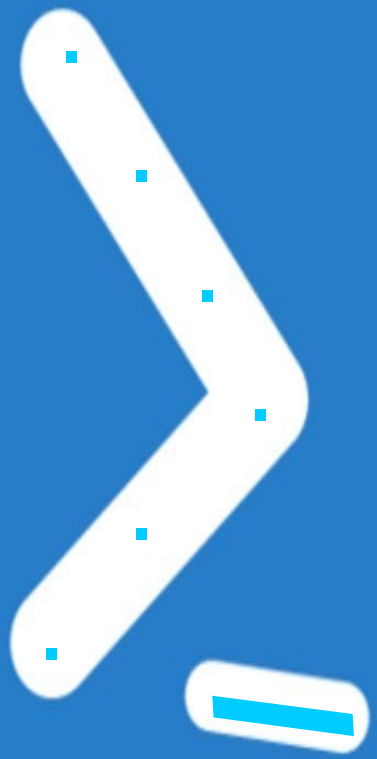
Flags

There are actually two different fields for flags. The flags specify inheritance settings
such as ACE is inherited, ACE is allowed to be inherited, ACE is not inheritable,
etc.

Table 16-1. Contents of an ACE’s properties

@matt-homjx0ie

What is / Access Control Cntries / 2



And Delete or Create Child Ob
jects permissions, the objectType should be configured to the schemaIDGUID of the
object class delegated.

Inherited Object Type

The schemaIDGUID for the types of object that the ACE applies to when an attribute,
property set, or validated right is specified or when the ACE is inherited—e.g., user
objects.

Access Mask

A bit flag that describes the type of access, such as Read, Write, List, Create, Delete,
Control Access, etc. See Table 16-1 for more detail.

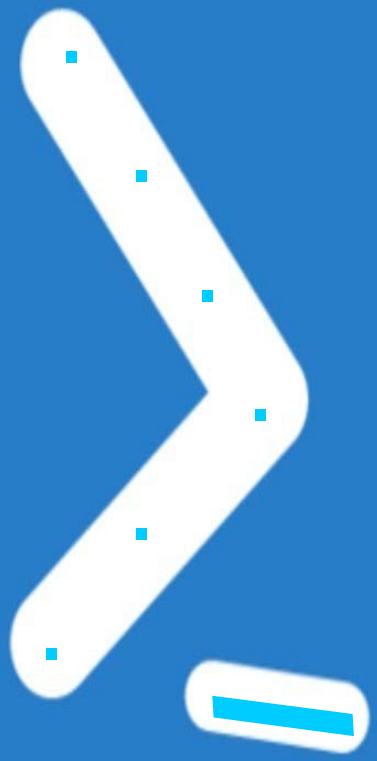
Flags

There are actually two different fields for flags. The flags specify inheritance settings
such as ACE is inherited, ACE is allowed to be inherited, ACE is not inheritable,
etc.

Table 16-1. Contents of an ACE’s properties

@matt-homjx0ie

What is / Access Control Cntries / 3

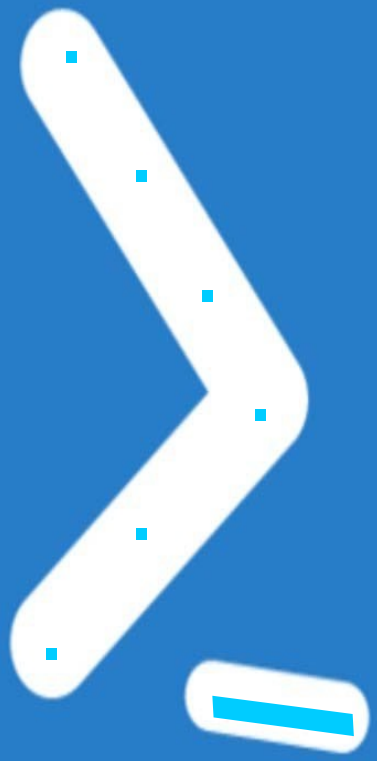


The Local Security Authority (LSA) evaluates the ACE list in the order of first looking for Explicit Deny or Allow ACEs. And second on Inherited Deny or Allow ACEs.

When a user tries to access an object in Active Directory the LSA gets the users' access token. The security subsystem compares the users SID and Group SIDs and the objects DACLs with the underlying ACEs to evaluate an access denied or granted. If no match can be done with users access token it will implicit deny user access to the object.

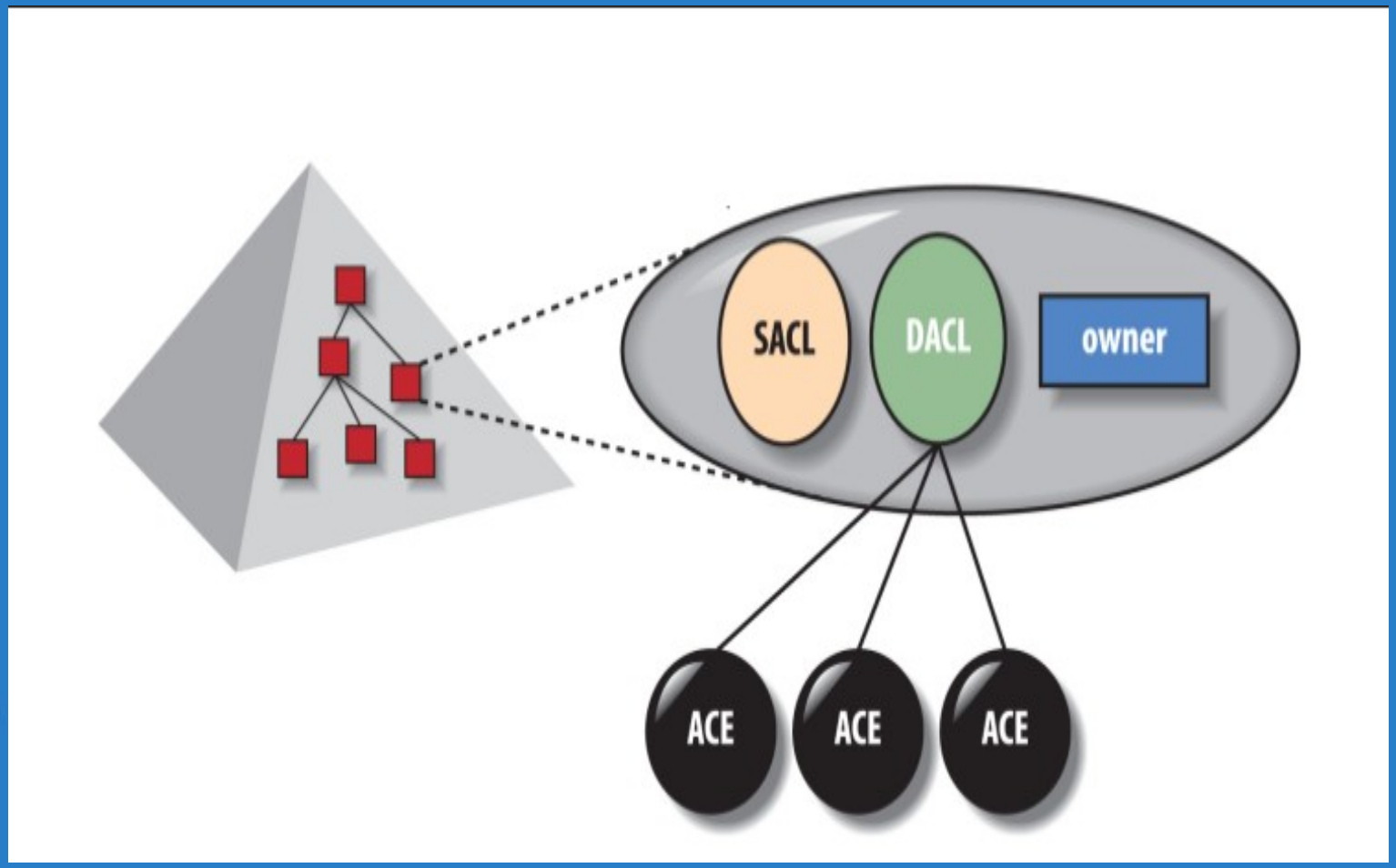
@matt-homjx0ie

What is DACL / Discretionary Access Control List /



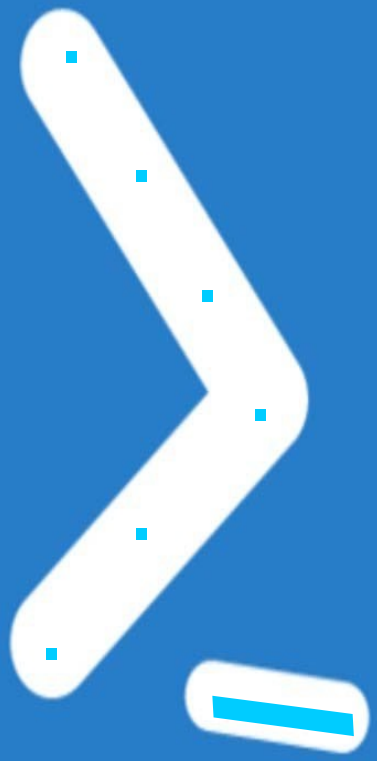
A DACL (often mentioned as the ACL) identify the users and groups that are assigned or denied access permissions on an object. It contains a list of paired ACEs (Account + Access Right) to the securable object.

@matt-homjx0ie



@matt-homjx0ie

What IS System Access Control List (SACL)



SACLs makes it possible to monitor access to secured objects. ACEs in a SACL determine what types of access is logged in the Security Event Log. With monitoring tools this could raise an alarm to the right people if malicious users tries to access the secured object, and in an incident scenario we can use the logs to trace the steps back in time. And last, you can enable logging for troubleshoot access issues.

@matt-homjx0ie

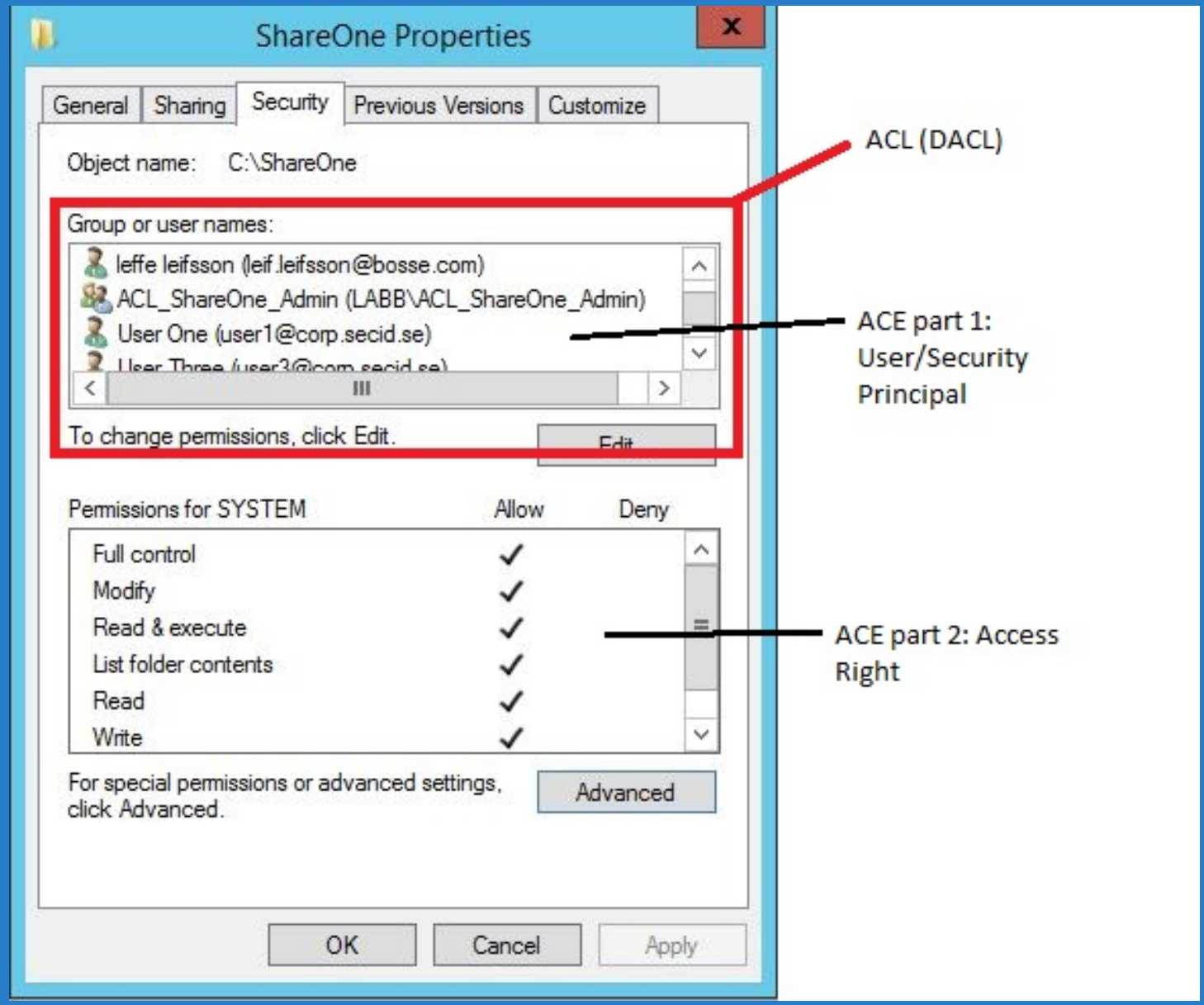
To Add List Advanced security to context menu

Download File Reg.. To add the List

https://www.tenforums.com/attachments/tutorials/380100d1442510264-advanced-security-add-context-menu-windows-8-10-a-add_advanced_security_to_context_menu.reg

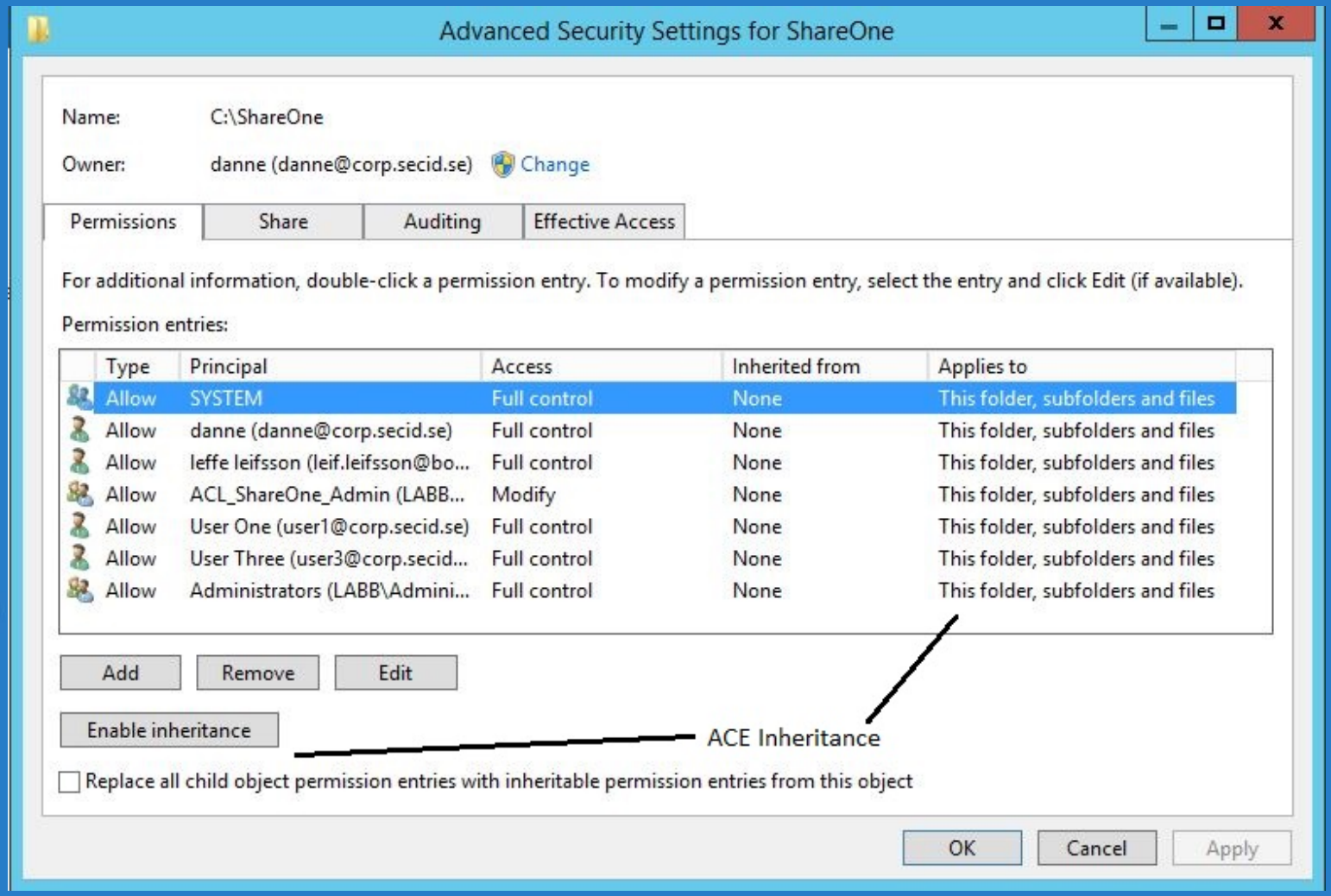
@DanielUlrichs

This is the classic security tab of a folder showing the ACL, DACL and ACEs



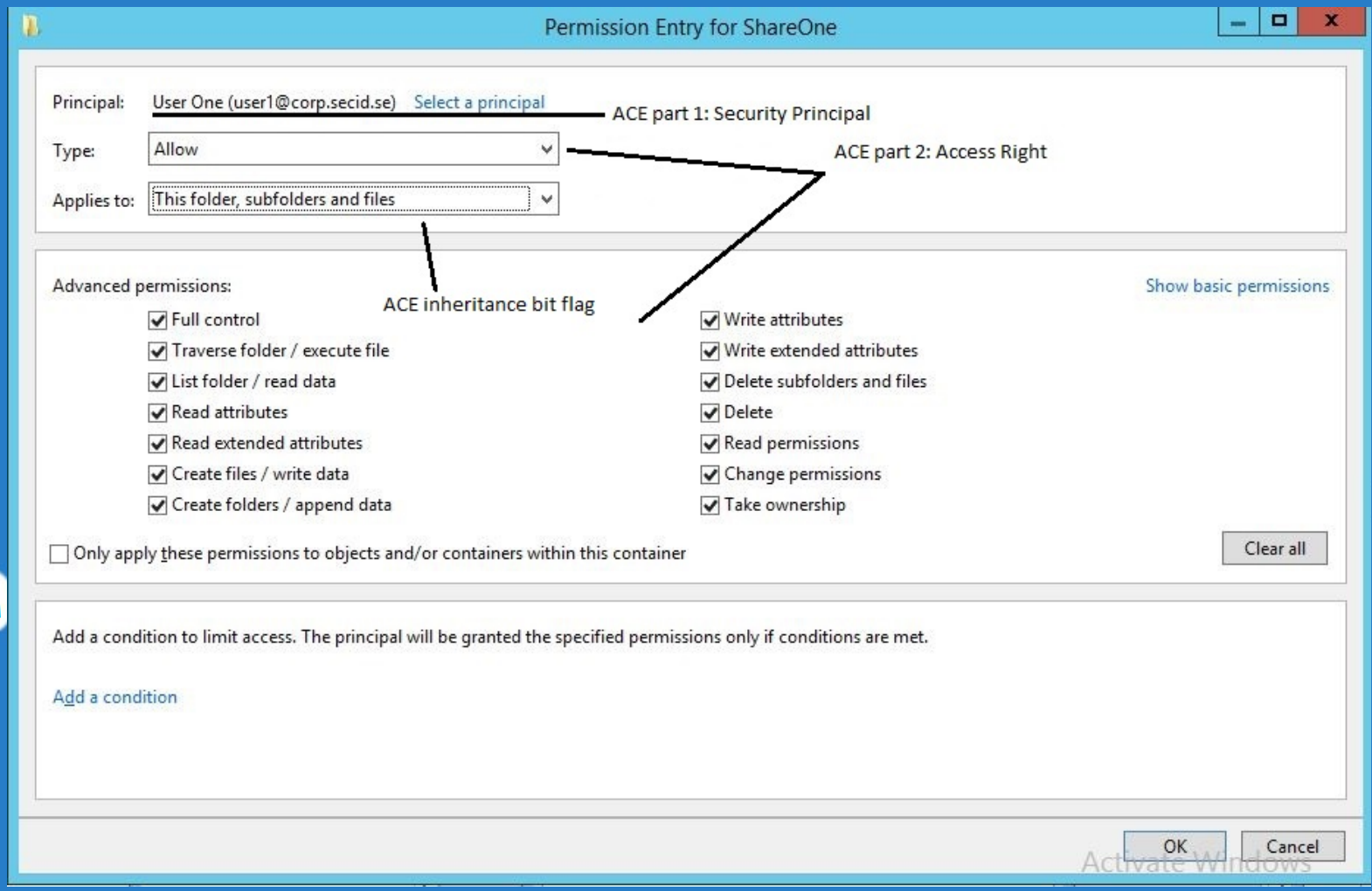
@DanielUlrichs

If we click the Advanced button we will get more options like inheritance:



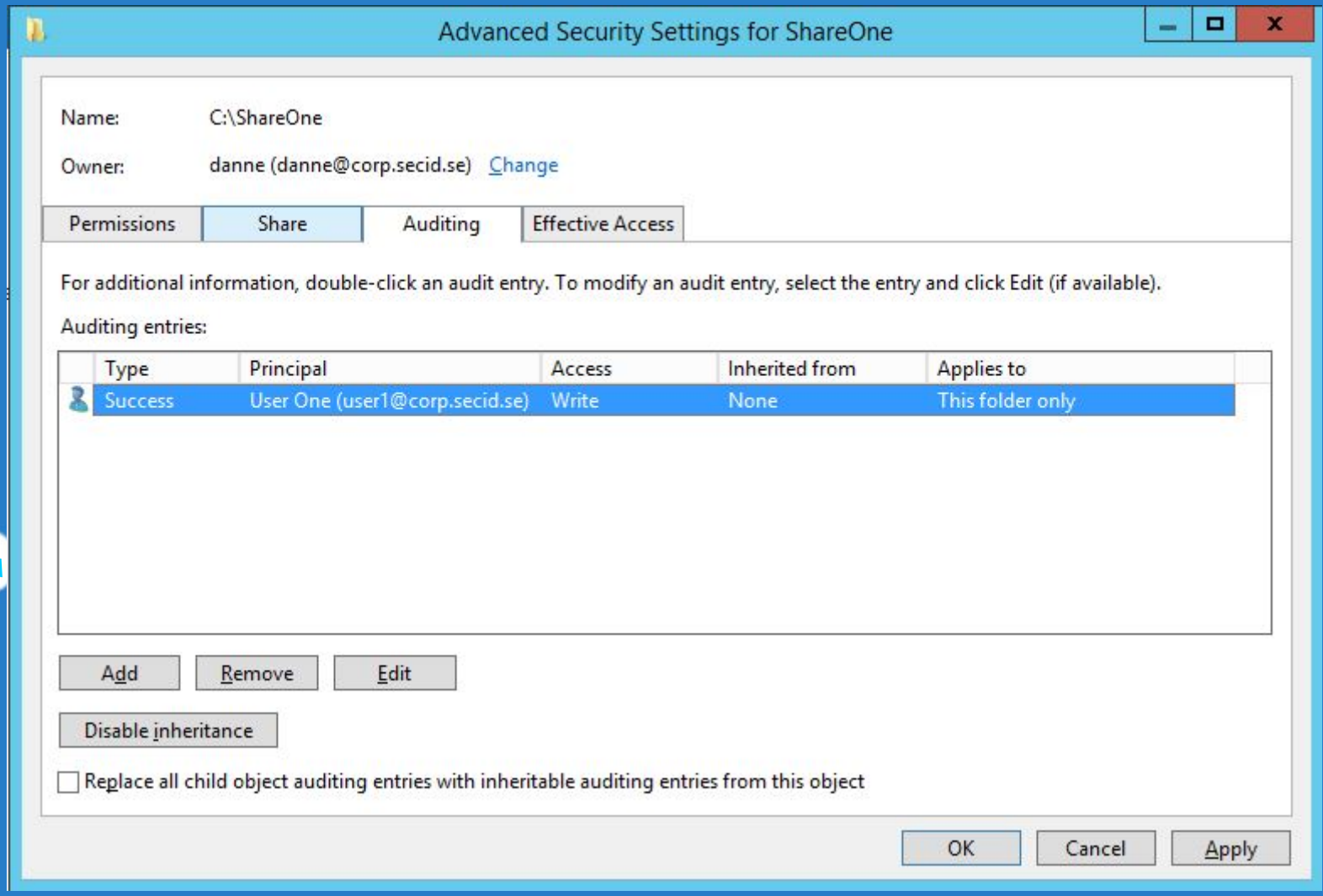
@DanielUlrichs

And if you add or edit a Security Principal:!



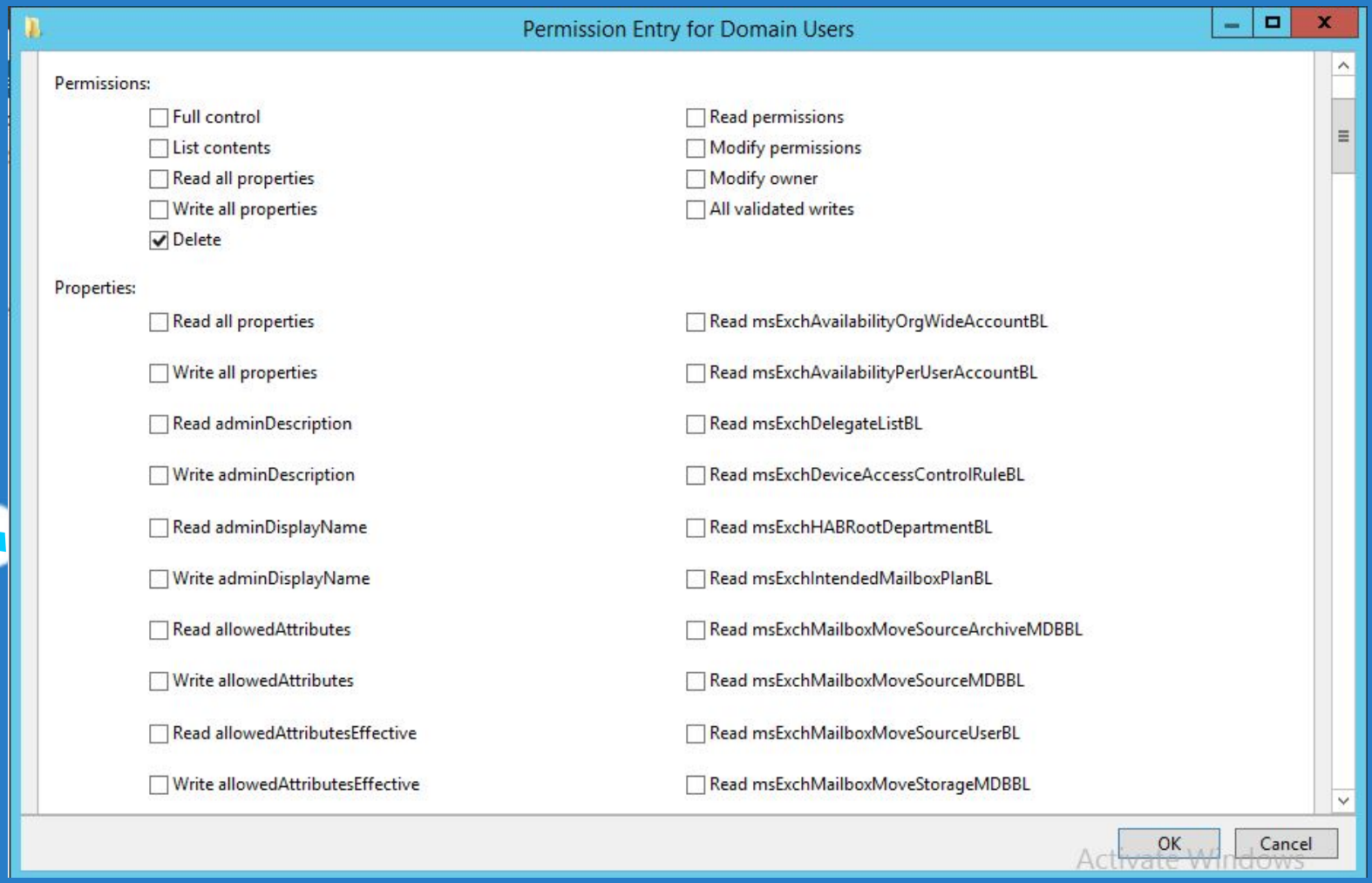
@DanielUlrichs

And last we have the SACL in the Auditing tab:!

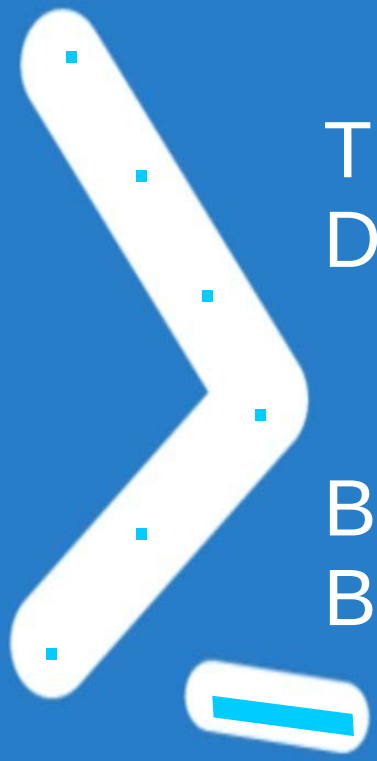


@DanielUlrichs

If you choose all descendant account objects you will see a list of all properties of user objects you could delegate control for a specific Security Principal.



@matt-homjx0ie



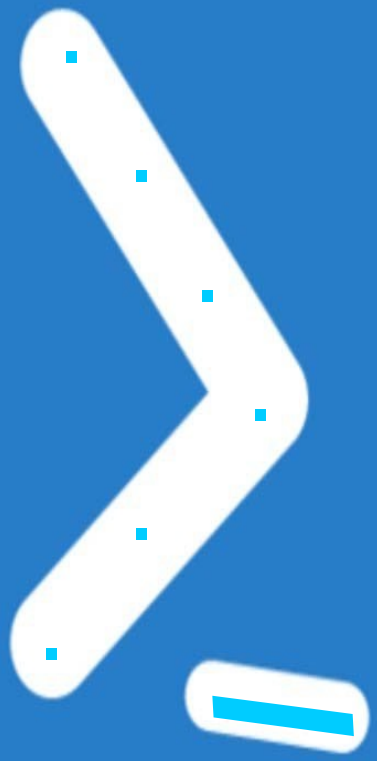
This the info / to environment Active Directory And So be able to use

BloodHound/Framework And to understand BloodHound/Framework

With environment Active Directory

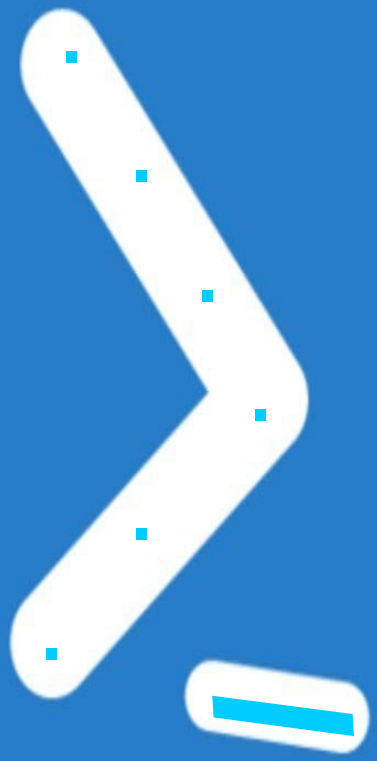
@matt-homjx0ie

Ok good /Bye All ! C-You ///



Twiiter :

Twitter Mr : @DanielUlrichs



https://twitter.com/DanielUlrichs

Twitter Matt-homjxi0e

https://twitter.com/homjxi0e