MODERN OPERATING SYSTEMS

LECTURE 6

AUTHOR: DR. ZVEREVA OLGA M.

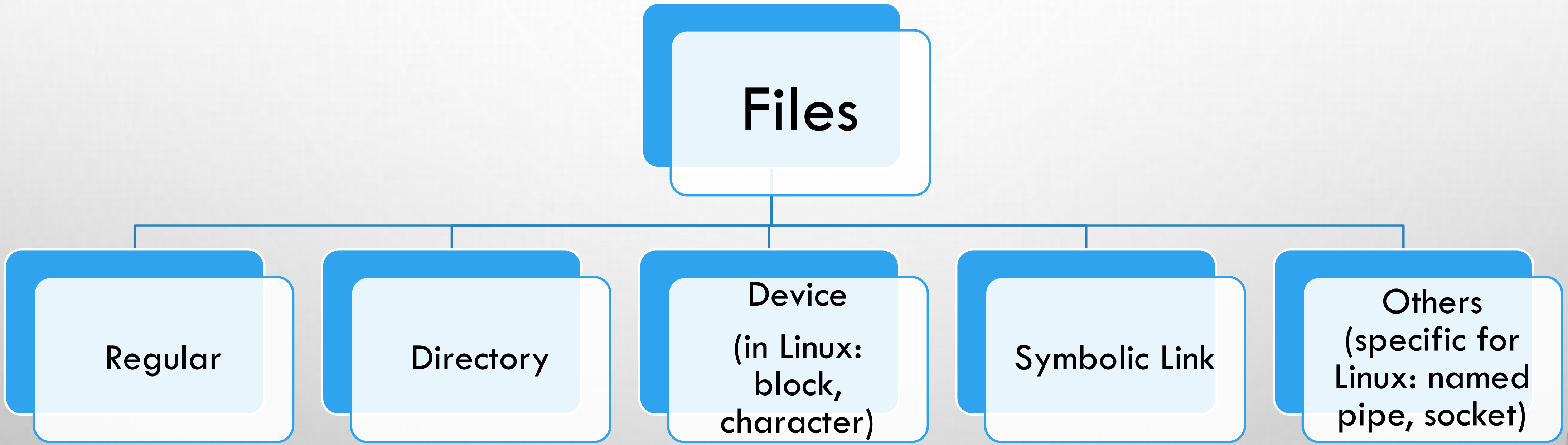
AGENDA

- ✓ FILE SYSTEMS
- ✓ DEFINITION AND CONCEPTS
- ✓ PECULIARITIES OF VARIOUS FILE SYSTEMS
- ✓ FAT VERSIONS
- ✓ NTFS
- ✓ NTFS OPERATING PECULIARITIES

DEFINITIONS & MAIN CONCEPTS

- FILE IS A LINEAR ARRAY OF BYTES, STORED PERSISTENTLY AND HAVING A NAME
- SEVERAL USERS CAN SHARE INFORMATION STORED IN A FILE
- IN EVERY FILE SYSTEM THERE IS A UNIQUE STRUCTURE (RECORD IN MFT (NTFS), INDEXED NODE, INODE (EXT2FS, EXT3FS)) WHICH IDENTIFIES A FILE
- THERE ARE FILES OF VARIOUS TYPES IN A FILE SYSTEM

TYPES OF FILES


Files
Regular
Directory
Device (in Linux: block, character)
Symbolic Link
Others (specific for Linux: named pipe, socket)

FILE SYSTEM

FILE SYSTEM IS A SYSTEM WHICH MAIN GOAL IS TO SUPPORT FILE ORGANIZATION, AND WHICH IS COMPRISED OF 3 MAIN COMPONENTS:

- A SET OF VARIOUS TYPE FILES
- SPECIAL DATA STRUCTURES (OFTEN IN THE FORM OF TABLES WHICH HELP TO FIND THE NECESSARY DATA IN THE DISK, I.E. SUPPORT THE PROCESS OF CONVERTING SYMBOLIC FILE NAMES INTO PHYSICAL ADDRESSES)
- PROGRAMS WHICH REALIZES ALL THE OPERATIONS WITH FILES (E.G. READING, WRITING, DELETING, AND ETC.)

FILE BLOCK

- **FILE SYSTEM BLOCK (CLUSTER IN NTFS & FAT)** IS A GROUP OF CONSECUTIVE SECTORS (THE NUMBER OF SECTORS IS ANY DEGREE OF 2 – IT COULD BE 1, 2, 4, 8, … SECTORS) THAT OPTIMIZE STORAGE ADDRESSING.
- IT IS THE MINIMAL SIZE OF A FILE IN A FILE SYSTEM (MINIMAL ADDRESSING VOLUME)
- MODERN FILE SYSTEMS GENERALLY USE BLOCK SIZES FROM 1 TO 128 SECTORS (512-64K BYTES).

CRITERIA OF FILE SYSTEM EVALUATION

- EFFICIENCY (I.E. THE RATE OF ACCESS TO FILES)
- LEVEL OF FRAGMENTATION (WHETHER FILE DATA ARE TO BE PLACED IN THE NEIGHBORING BLOCKS OR SCATTERED ON THE DISK SURFACE)
- MAXIMUM VOLUME SUPPORTED BY THIS FS (MAXIMAL FILE SIZE)
- CHANCE TO FILE SYSTEM RECOVERY

FILE SYSTEMS (FS) IN WINDOWS

- FAT (FAT12, FAT16, FAT32) – FILE ALLOCATION TABLE – THE MAIN FS STRUCTURE
- NTFS – NEW TECHNOLOGY FS
- *REFS (RESILIENT FILE SYSTEM)*
  - ✓ IS THE LATEST PRODUCT OF MICROSOFT INTRODUCED WITH WINDOWS 8 AND NOW AVAILABLE FOR WINDOWS 10.
  - ✓ THE FILE SYSTEM ARCHITECTURE ABSOLUTELY DIFFERS FROM OTHER WINDOWS FILE SYSTEMS AND IS MAINLY ORGANIZED IN A FORM OF THE B+-TREE.
  - ✓ *REFS* HAS HIGH TOLERANCE TO FAILURES DUE TO NEW FEATURES INCLUDED INTO THE SYSTEM

FAT

- *FAT* (FILE ALLOCATION TABLE) IS ONE OF THE SIMPLEST FILE SYSTEM TYPES, WHICH HAS BEEN AROUND SINCE THE 1980S
- ITS VERSIONS: FAT12, FAT16, FAT32.
- 12, 16, 32 STAND FOR THE NUMBER OF BITS USED TO ENUMERATE FILE SYSTEM BLOCKS
- FAT CONSISTS OF:
  - THE FILE SYSTEM *DESCRIPTOR SECTOR* (BOOT SECTOR OR SUPERBLOCK),
  - *THE FILE SYSTEM BLOCK ALLOCATION TABLE* (REFERRED AS THE FILE ALLOCATION TABLE)
  - *PLAIN STORAGE SPACE* FOR STORING FILES AND FOLDERS.
- FILES IN FAT ARE STORED IN DIRECTORIES. EACH DIRECTORY IS AN ARRAY OF *32-BYTE RECORDS*, EACH DEFINING A FILE OR EXTENDED ATTRIBUTES OF A FILE (E.G. A LONG FILE NAME). A FILE RECORD ATTRIBUTES THE FIRST BLOCK OF A FILE.
- ANY NEXT BLOCK CAN BE FOUND THROUGH THE BLOCK ALLOCATION TABLE BY USING IT AS A LINKED LIST.

EXAMPLE OF A FILE ALLOCATION TABLE

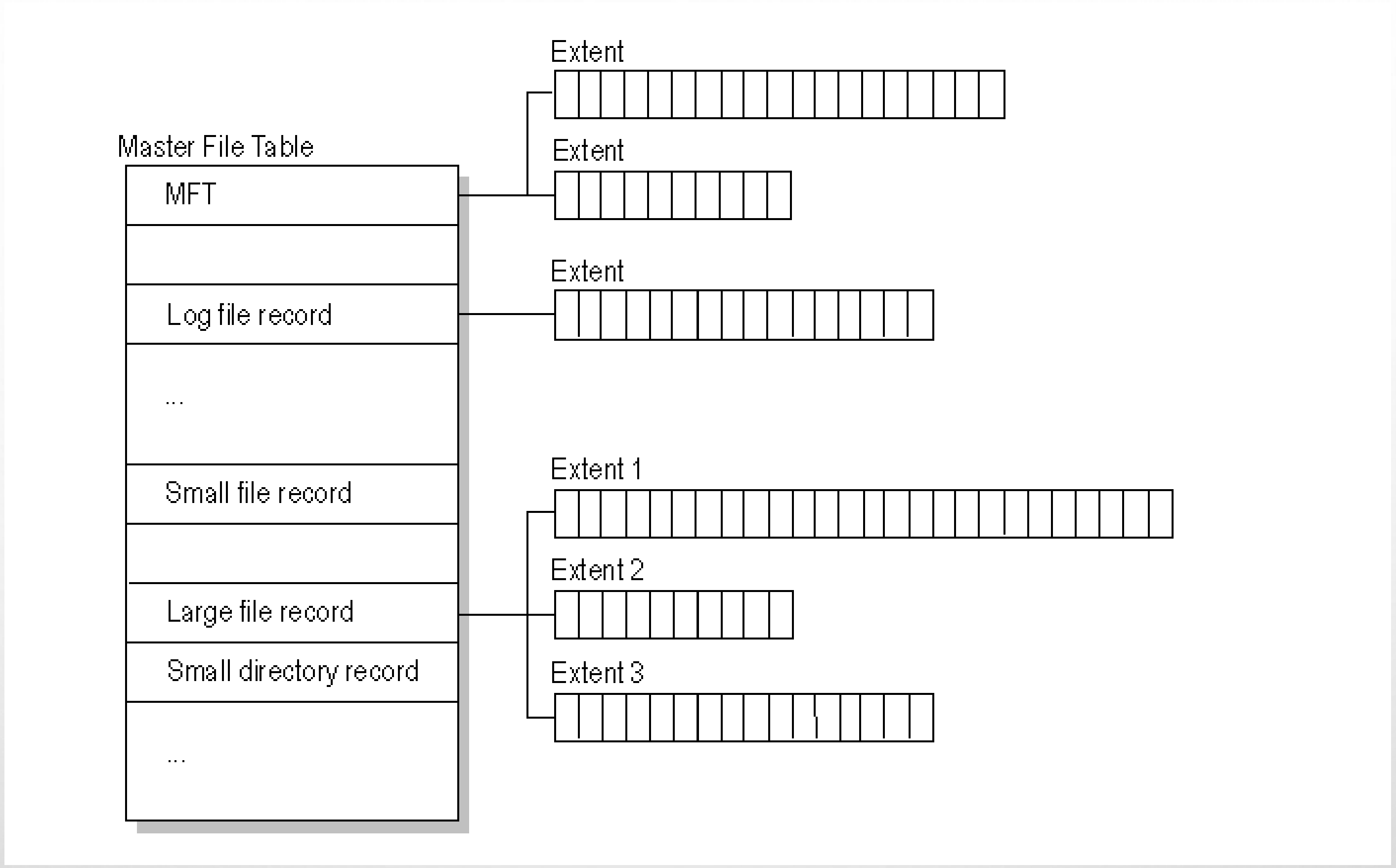
2	3	4	5	6	7	8	9	10	11	12
0	0	5	6	EOF	9	0	EOF	EOF	0	0

NTFS

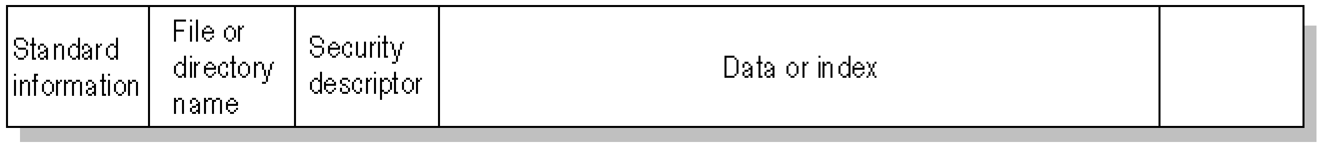
- THE MAIN SYSTEM STRUCTURE OF NTFS IS “MFT – MASTER FILE TABLE”. IN NTFS, DISK IS DIVIDED INTO MFT SPACE AND SPACE FOR FILE STORAGE. THE MFT PART OCCUPIES AROUND 12% OF THE DISK TO STORE THE MFT METAFILE AND REST 88% SPACE IS USED FOR DATA STORAGE.
- EACH FILE ON AN NTFS VOLUME IS REPRESENTED BY A RECORD (OR SEVERAL RECORDS) IN THE MASTER FILE TABLE (MFT).
- NTFS RESERVES THE FIRST 16 RECORDS OF THE TABLE FOR SPECIAL INFORMATION (META FILES)
- THE FIRST RECORD OF THIS TABLE DESCRIBES THE MASTER FILE TABLE ITSELF, FOLLOWED BY A MFT *MIRROR RECORD*.
- THE THIRD RECORD OF THE MFT IS THE LOG FILE, USED FOR FILE RECOVERY

META FILES

- THE META FILE NAMES ARE PREFIXED BY A '$'SIGN FOR EXAMPLE: $MFT, $BOOT (BOOT SECTOR), $LOGFILE (JOURNALING SUPPORT FILE), $.(ROOT DIRECTORY) ETC.
- $VOLUME - CONTAINS INFORMATION ABOUT THE VOLUME, NAMELY THE VOLUME OBJECT IDENTIFIER, VOLUME LABEL, FILE SYSTEM VERSION, AND VOLUME FLAGS
- $ATTRDEF - A TABLE OF MFT ATTRIBUTES THAT ASSOCIATES NUMERIC IDENTIFIERS WITH NAMES
- . - ROOT DIRECTORY
- $BITMAP - AN ARRAY OF BIT ENTRIES: EACH BIT INDICATES WHETHER ITS CORRESPONDING CLUSTER IS USED (ALLOCATED) OR FREE (AVAILABLE FOR ALLOCATION)
- $BOOT - VOLUME BOOT RECORD. THIS FILE IS ALWAYS LOCATED AT THE FIRST CLUSTERS ON THE VOLUME. IT CONTAINS BOOTSTRAP CODE
- $BADCLUS - A FILE THAT CONTAINS ALL THE CLUSTERS MARKED AS HAVING BAD SECTORS. THIS FILE SIMPLIFIES CLUSTER MANAGEMENT BY THE CHKDSK UTILITY



MFT Record for a Small File or Directory:



LINUX FILE SYSTEMS OF LINUX

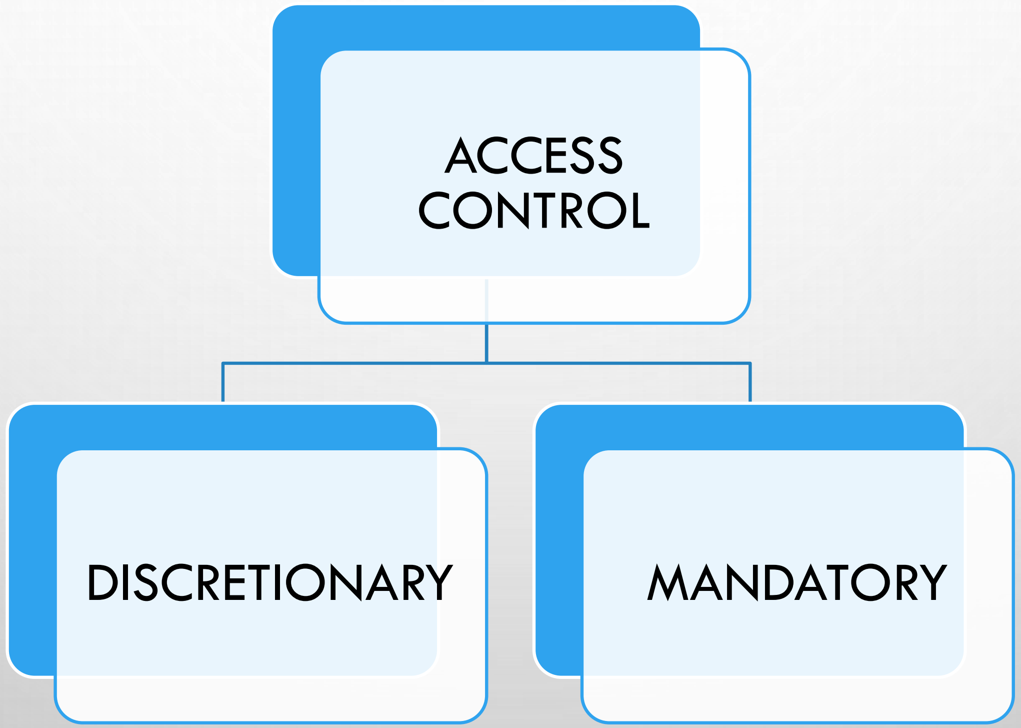
- **EXT2, EXT3, EXT4** - A “NATIVE” LINUX FILE SYSTEM. THIS FILE SYSTEM FALLS UNDER ACTIVE DEVELOPMENTS AND IMPROVEMENTS.
  - **EXT3** FILE SYSTEM IS JUST AN EXTENSION OF **EXT2** THAT USES TRANSACTIONAL FILE WRITING OPERATIONS WITH A **JOURNAL**.
  - **EXT4** IS A FURTHER DEVELOPMENT OF EXT3, EXTENDED WITH THE SUPPORT OF OPTIMIZED FILE ALLOCATION INFORMATION (EXTENTS) AND EXTENDED FILE ATTRIBUTES. THIS FILE SYSTEM IS FREQUENTLY USED AS A "ROOT" FILE SYSTEM FOR MOST LINUX INSTALLATIONS.
- **REISERFS** - AN ALTERNATIVE LINUX FILE SYSTEM OPTIMIZED FOR STORING OF **SMALL FILES**. IT HAS GOOD CAPABILITY OF FILES SEARCH AND ENABLES COMPACT FILES ALLOCATION. HOWEVER, THIS FILE SYSTEM NO LONGER RECEIVES ACTIVE SUPPORT.
- **XFS** - A FILE SYSTEM DERIVED FROM SGI COMPANY AND WAS INITIALLY USED FOR COMPANY’S IRIX SERVERS. NOW XFS SPECIFICATIONS ARE IMPLEMENTED IN LINUX. XFS FILE SYSTEM HAS GREAT PERFORMANCE AND IS WIDELY USED TO STORE FILES. OPTIMIZED FOR STORING **BIG FILES**
- **JFS** - A FILE SYSTEM DEVELOPED BY IBM FOR THE COMPANY’S POWERFUL COMPUTING SYSTEMS. JFS1 USUALLY STANDS FOR **JFS, JFS2** IS THE SECOND RELEASE. CURRENTLY, THIS FILE SYSTEM IS OPEN-SOURCE AND IMPLEMENTED IN MOST MODERN LINUX VERSIONS.
- **BTRFS** - A FILE SYSTEM DESIGNED BY ORACLE SUPPORTED BY THE MAINLINE LINUX KERNEL SINCE 2009. THE FILE SYSTEM IS AIMED AT BETTER **RELIABILITY AND SCALABILITY**, OFFERING HIGHER FAULT TOLERANCE, EASIER ADMINISTRATION, ETC. TOGETHER WITH A NUMBER OF ADVANCED FEATURES, BUT STILL CANNOT BE CONSIDERED FULLY STABLE.

FILE SYSTEMS OF MAC OS

- *HFS+*, AN EXTENSION TO THEIR OWN HFS FILE SYSTEM
  - ✓ USES B-TREES FOR PLACING AND LOCATING FILES
  - ✓ THE INFORMATION CONCERNING FREE AND USED FILE BLOCKS IS KEPT IN THE ALLOCATION FILE
  - ✓ ALL BLOCKS ASSIGNED TO EACH FILE AS EXTENDS ARE RECORDED IN THE EXTENDS OVERFLOW FILE
  - ✓ ALL FILE ATTRIBUTES ARE LISTED IN THE ATTRIBUTES FILE
  - ✓ DATA RELIABILITY IS IMPROVED THROUGH JOURNALING
- RECENTLY RELEASED *APFS*
  - ✓ IS AIMED TO ADDRESS FUNDAMENTAL ISSUES PRESENT IN ITS PREDECESSOR AND WAS DEVELOPED TO EFFICIENTLY WORK WITH MODERN FLASH STORAGES AND SOLID-STATE DRIVES
  - ✓ ALL THE FILE CONTENTS AND METADATA ABOUT FILES, FOLDERS ALONG WITH OTHER APFS STRUCTURES ARE KEPT IN THE APFS CONTAINER.
  - ✓ **THE CONTAINER SUPERBLOCK** STORES INFORMATION ABOUT THE NUMBER OF BLOCKS IN THE CONTAINER, THE BLOCK SIZE, ETC.
  - ✓ INFORMATION ABOUT ALL ALLOCATED AND FREE BLOCKS OF THE CONTAINER IS MANAGED WITH THE HELP OF BITMAP STRUCTURES.

WORKING IN NTFS

ACCESS CONTROL TYPES



DISCRETIONARY ACCESS CONTROL (DAC)

- IS A TYPE OF ACCESS CONTROL DEFINED AS A MEANS OF RESTRICTING ACCESS TO OBJECTS BASED ON IDENTITY OF SUBJECTS AND/OR GROUPS TO WHICH THEY BELONGS;
- IS "DISCRETIONARY IN THE SENSE THAT A SUBJECT WITH A CERTAIN ACCESS PERMISSION IS CAPABLE OF PASSING THAT PERMISSION ON TO ANY OTHER SUBJECT

(OBJECTS – FILES AND FOLDERS, SUBJECTS – USERS OR THEIR APPLICATIONS)

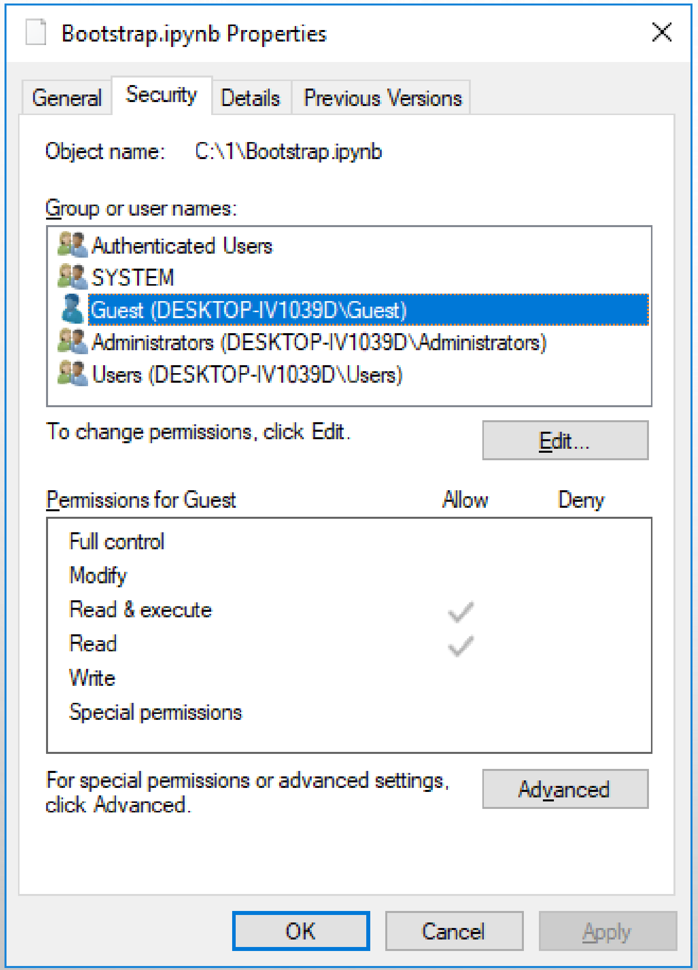
MAIN ISSUES OF DAC FOR A FILE SYSTEM

- EVERY FILE MUST HAVE AN OWNER (THERE IS NO “NO ONE’S” FILES OR FOLDERS). THE USER WHO CREATES THE FILE (FOLDER) HAS BECOME ITS OWNER
- THE OWNER SET PERMISSIONS FOR WORING WITH THE FILE (FOLDER) FOR ALL OTHER USERS, AND THESE PERMISSIONS COULD BE INTERPRETED IN THE ONLY ONE WAY
- THERE IS A SUPER USER IN THE SYSTEM WHO IS ABLE TO BECOME THE OWNER OF ANY FILE (FOLDER) IN THE SYSTEM

MAIN ISSUES OF ACCESS CONTROL IN NTFS

- DAC IS REALIZED FOR THIS FILE SYSTEM, THUS ROLE OF THE “OWNER” IS IMMENSELY IMPORTANT IN NTFS
- THE OWNER CAN “ALLOW” OR “DENY” SOME OPERATIONS FOR VARIOUS USERS AND GROUPS
- YOU MUST TAKE IN ACCOUNT INTERACTIONS BETWEEN THESE “ALLOW” AND “DENY”, AS IF THEY CAN BE SET FOR THE USERS INDIVIDUALLY, AND FOR DIFFERENT GROUPS WHERE THESE USERS TOOK PART AS WELL
- IT IS NECESSARY TO PAY ATTENTION TO PERMISSION INHERITANCE

"SECURITY" TAB IN FILE/FOLDER "PROPERTIES" WINDOW



Bootstrap.ipynb Properties

General | Security | Details | Previous Versions

Object name: C:\1\Bootstrap.ipynb

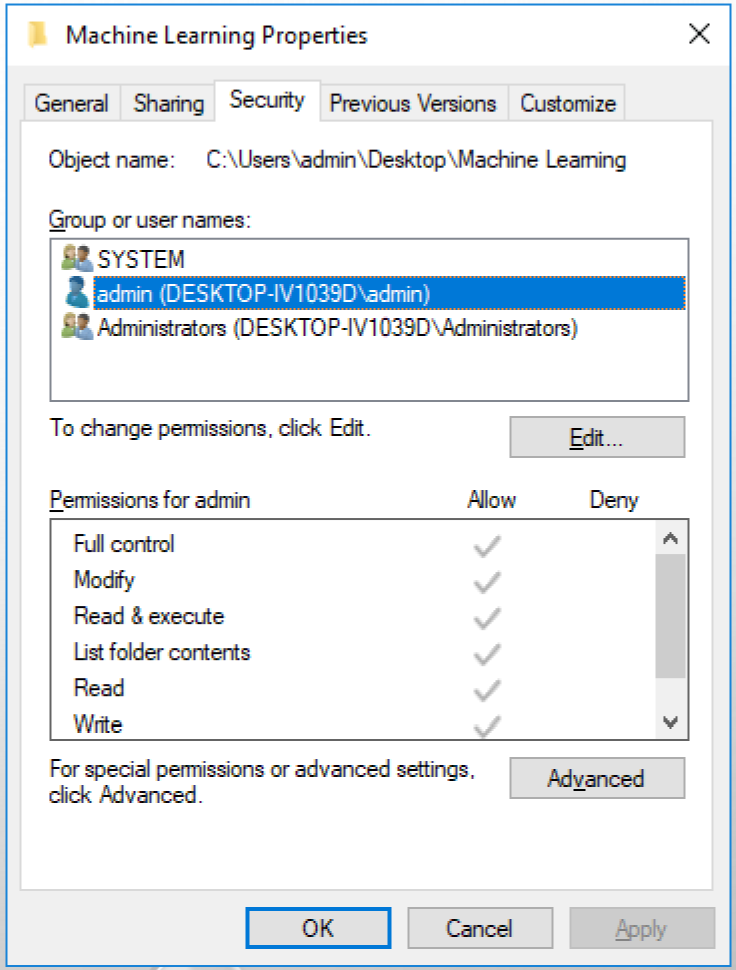
Group or user names:

- Authenticated Users
- SYSTEM
- Guest (DESKTOP-IV1039D\Guest)
- Administrators (DESKTOP-IV1039D\Administrators)
- Users (DESKTOP-IV1039D\Users)

To change permissions, click Edit.

Permissions for Guest	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.



Machine Learning Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\admin\Desktop\Machine Learning

Group or user names:

- SYSTEM
- admin (DESKTOP-IV1039D\admin)
- Administrators (DESKTOP-IV1039D\Administrators)

To change permissions, click Edit.

Permissions for admin	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

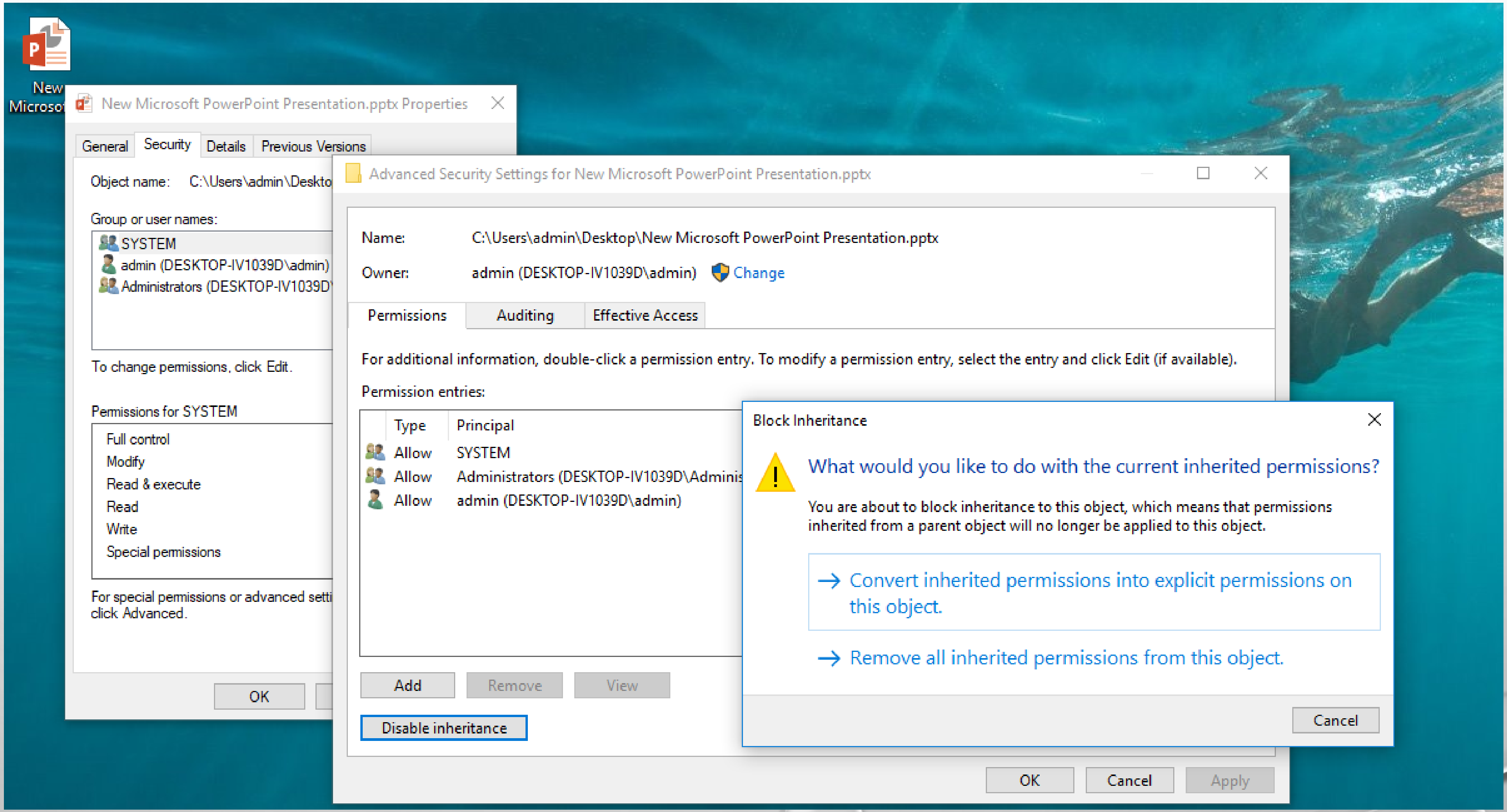
For special permissions or advanced settings, click Advanced.

RULES

- ALL PERMISSIONS (INDICATED AS “ALLOW‘”) FOLLOW THE RULE OF ADDITION (THEY ARE SUMMARIZED)
- ALL “DENY” SETTINGS HAVE THE HIGHER PRIORITY IN COMPARISON WITH “ALLOW” SETTINGS

(EXAMPLE: IF THE USER NAMED “USER1” HAS ALLOWANCE TO READ PERSONALLY, AND READING IS DENIED FOR THEM AS A MEMBER OF THE GROUP “USERS”, “USER1” WILL NOT BE ABLE TO READ THIS FILE)

INHERITANCE


New Microsoft PowerPoint Presentation.pptx Properties

General | Security | Details | Previous Versions

Object name: C:\Users\admin\Deskto

Group or user names:

SYSTEM
admin (DESKTOP-IV1039D\admin)
Administrators (DESKTOP-IV1039D

To change permissions, click Edit.

Permissions for SYSTEM

Full control
Modify
Read & execute
Read
Write
Special permissions

For special permissions or advanced setti
click Advanced.

OK

Advanced Security Settings for New Microsoft PowerPoint Presentation.pptx

Name: C:\Users\admin\Desktop\New Microsoft PowerPoint Presentation.pptx

Owner: admin (DESKTOP-IV1039D\admin) Change

Permissions | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal
Allow	SYSTEM
Allow	Administrators (DESKTOP-IV1039D\Adminis
Allow	admin (DESKTOP-IV1039D\admin)

Add | Remove | View

Disable inheritance

OK | Cancel | Apply

Block Inheritance

What would you like to do with the current inherited permissions?

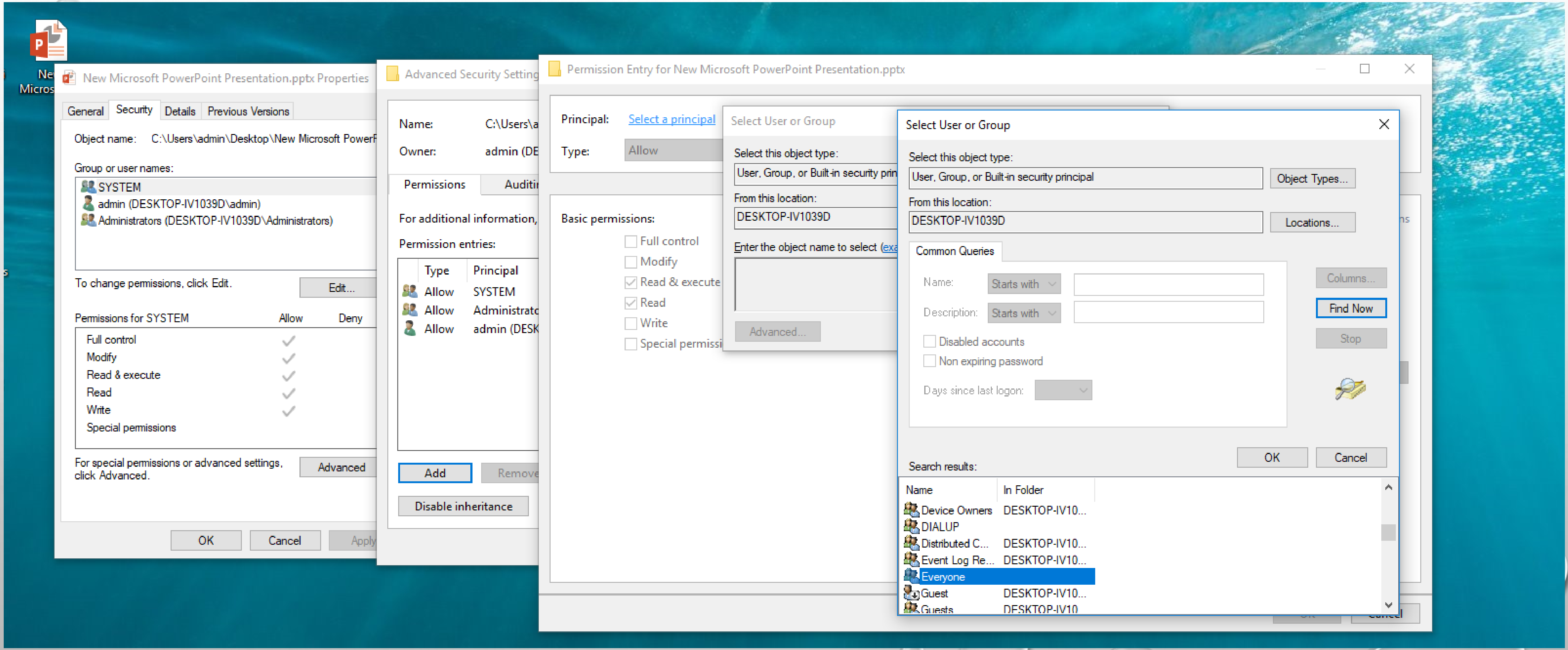
You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

Cancel

SECURITY SETTINGS



New Microsoft PowerPoint Presentation.pptx Properties

General | Security | Details | Previous Versions

Object name: C:\Users\admin\Desktop\New Microsoft PowerP

Group or user names:

- SYSTEM
- admin (DESKTOP-IV1039D\admin)
- Administrators (DESKTOP-IV1039D\Administrators)

To change permissions, click Edit. Edit...

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced. Advanced

OK | Cancel | Apply

Advanced Security Setting

Name: C:\Users\a

Owner: admin (DE

Permissions | Auditi

For additional information,

Permission entries:

Type	Principal
Allow	SYSTEM
Allow	Administrato
Allow	admin (DESK

Add | Remove

Disable inheritance

Permission Entry for New Microsoft PowerPoint Presentation.pptx

Principal: Select a principal

Type: Allow

Basic permissions:

- [ ] Full control
- [ ] Modify
- [x] Read & execute
- [x] Read
- [ ] Write
- [ ] Special permissi

Select User or Group

Select this object type:

User, Group, or Built-in security prin

From this location:

DESKTOP-IV1039D

Enter the object name to select (exa

Advanced...

Select User or Group

Select this object type:

User, Group, or Built-in security principal | Object Types...

From this location:

DESKTOP-IV1039D | Locations...

Common Queries

Name: Starts with

Description: Starts with

- [ ] Disabled accounts
- [ ] Non expiring password

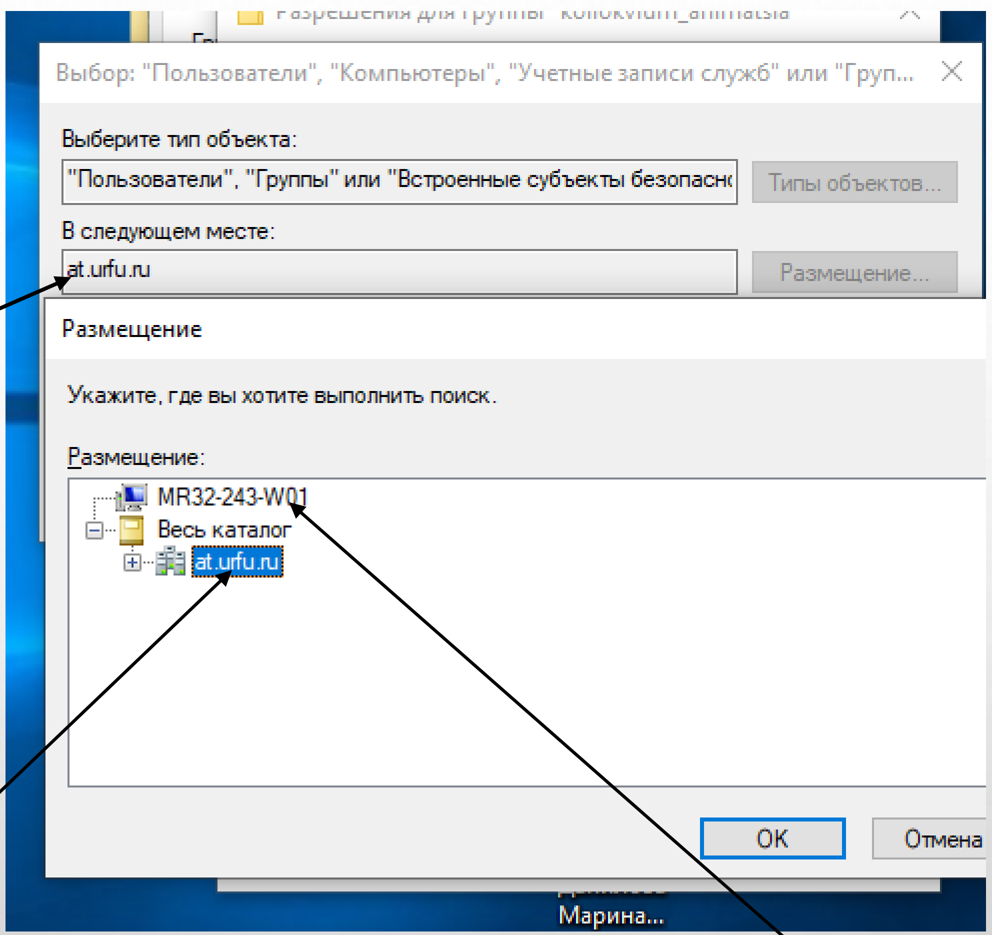
Days since last logon:

Columns... | Find Now | Stop

OK | Cancel

Search results:

Name	In Folder
Device Owners	DESKTOP-IV10...
DIALUP	
Distributed C...	DESKTOP-IV10...
Event Log Re...	DESKTOP-IV10...
Everyone	
Guest	DESKTOP-IV10...
Guests	DESKTOP-IV10



Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Груп...

Выберите тип объекта:

"Пользователи", "Группы" или "Встроенные субъекты безопасн

В следующем месте:

at.urfu.ru

Размещение

Укажите, где вы хотите выполнить поиск.

Размещение:

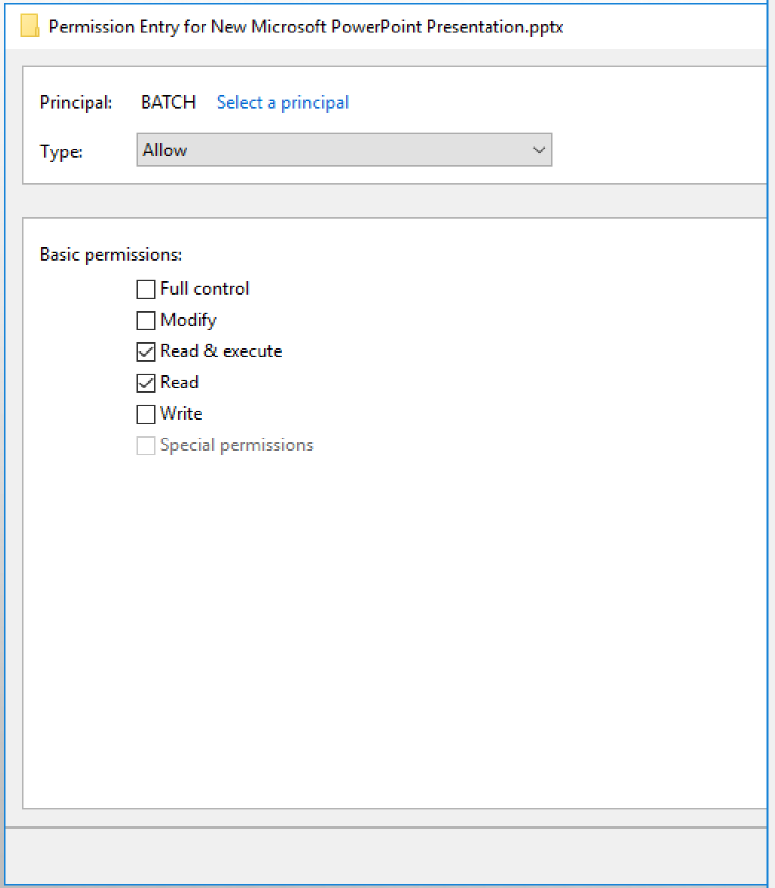
MR32-243-W01
Весь каталог
at.urfu.ru

It is necessary to pay attention from which data base (domain or local) you choose the account

Domain data base (domain user)

Local data base (local user)

DIFFERENT TYPES OF PERMISSIONS

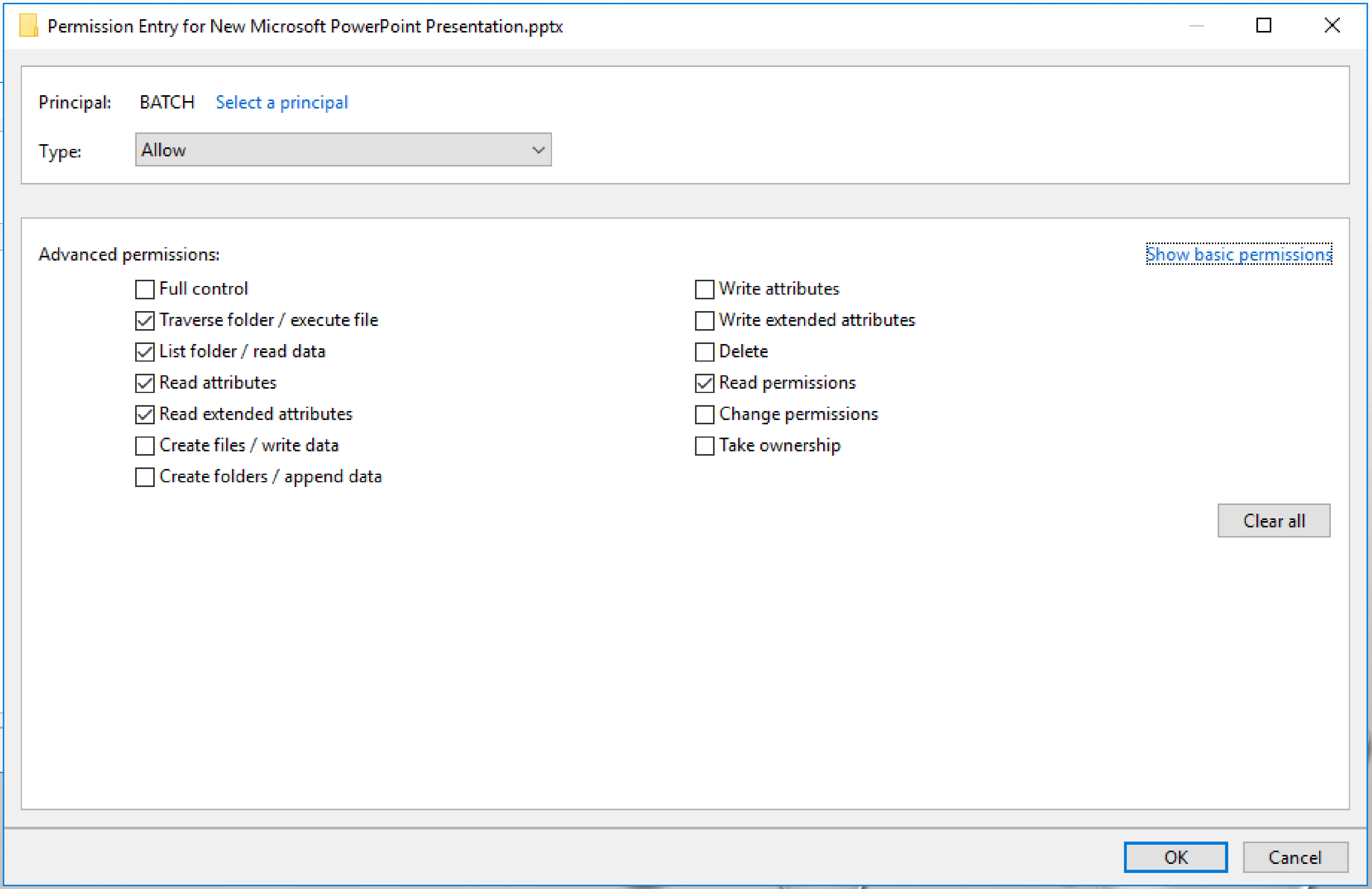

Permission Entry for New Microsoft PowerPoint Presentation.pptx

Principal: BATCH Select a principal

Type: Allow

Basic permissions:

- [ ] Full control
- [ ] Modify
- [x] Read & execute
- [x] Read
- [ ] Write
- [ ] Special permissions


Permission Entry for New Microsoft PowerPoint Presentation.pptx

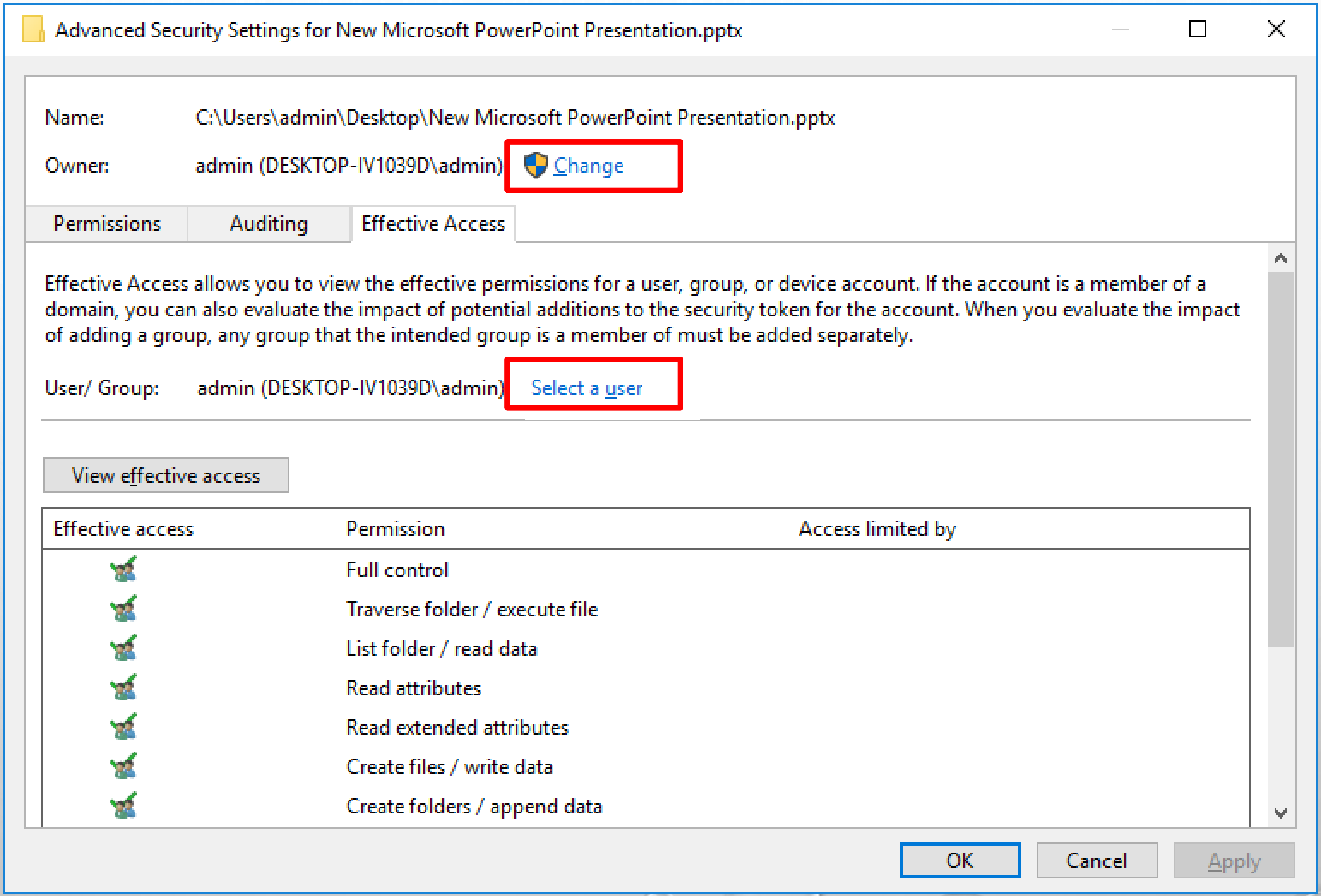
Principal: BATCH Select a principal

Type: Allow

Advanced permissions: Show basic permissions

- [ ] Full control
- [x] Traverse folder / execute file
- [x] List folder / read data
- [x] Read attributes
- [x] Read extended attributes
- [ ] Create files / write data
- [ ] Create folders / append data
- [ ] Write attributes
- [ ] Write extended attributes
- [ ] Delete
- [x] Read permissions
- [ ] Change permissions
- [ ] Take ownership

"EFFECTIVE ACCESS" TAB IN "ADVANCED SECURITY SETTINGS" WINDOW



Advanced Security Settings for New Microsoft PowerPoint Presentation.pptx

Name: C:\Users\admin\Desktop\New Microsoft PowerPoint Presentation.pptx

Owner: admin (DESKTOP-IV1039D\admin) Change

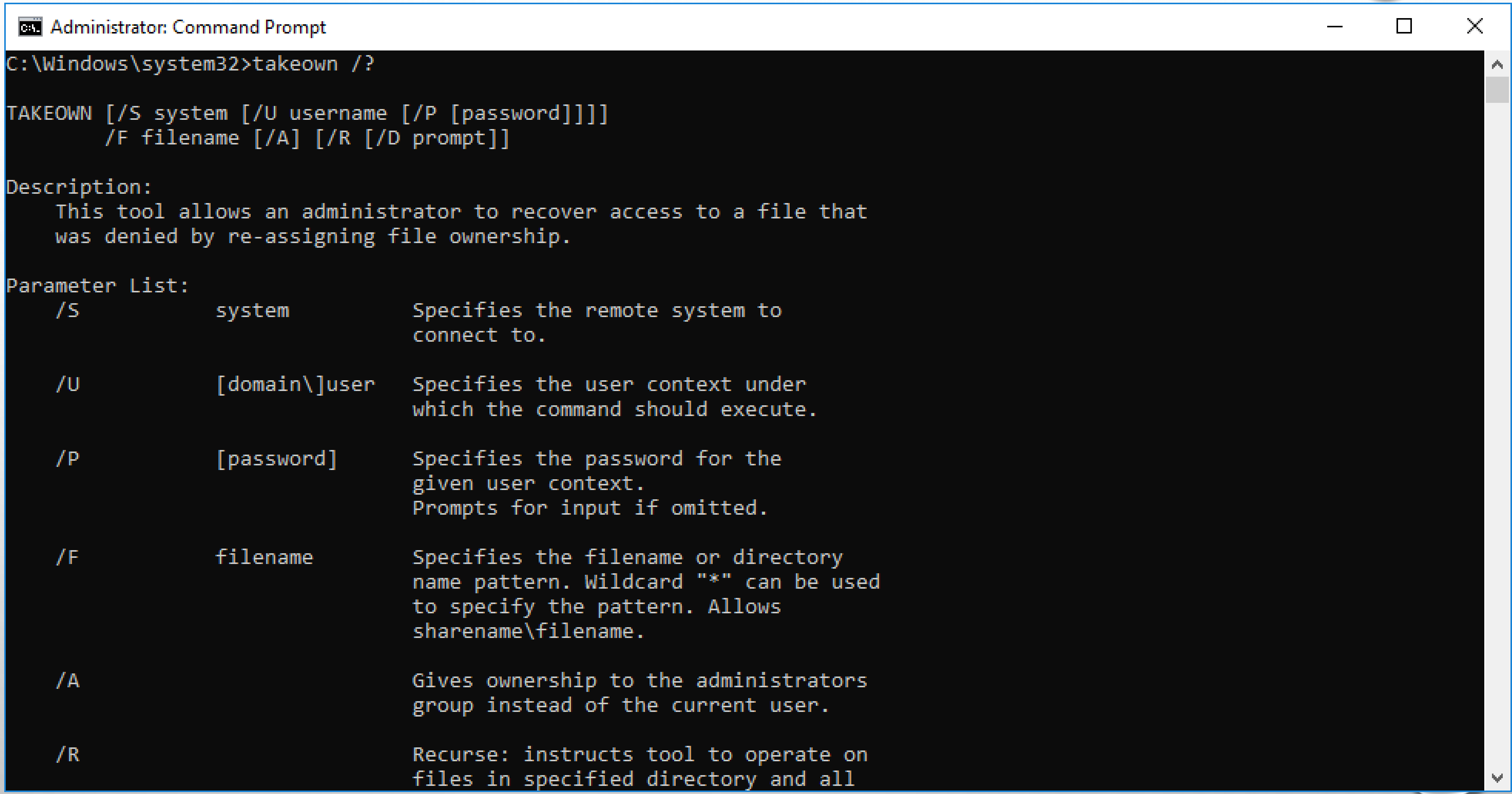
Effective Access allows you to view the effective permissions for a user, group, or device account. If the account is a member of a domain, you can also evaluate the impact of potential additions to the security token for the account. When you evaluate the impact of adding a group, any group that the intended group is a member of must be added separately.

User/ Group: admin (DESKTOP-IV1039D\admin) Select a user

Effective access	Permission	Access limited by
✓	Full control	
✓	Traverse folder / execute file	
✓	List folder / read data	
✓	Read attributes	
✓	Read extended attributes	
✓	Create files / write data	
✓	Create folders / append data	

TO CHANGE THE OWNER

- GRAPHICAL INTERFACE (PREVIOUS SLIDE)
- “TAKEOWN” COMMAND (FROM THE COMMAND LINE)


Administrator: Command Prompt

```
C:\Windows\system32>takeown /?

TAKEOWN [/S system [/U username [/P [password]]]]
        /F filename [/A] [/R [/D prompt]]

Description:
    This tool allows an administrator to recover access to a file that
    was denied by re-assigning file ownership.

Parameter List:
    /S           system          Specifies the remote system to
                                 connect to.

    /U           [domain\]user   Specifies the user context under
                                 which the command should execute.

    /P           [password]      Specifies the password for the
                                 given user context.
                                 Prompts for input if omitted.

    /F           filename        Specifies the filename or directory
                                 name pattern. Wildcard "*" can be used
                                 to specify the pattern. Allows
                                 sharename\filename.

    /A                           Gives ownership to the administrators
                                 group instead of the current user.

    /R                           Recurse: instructs tool to operate on
                                 files in specified directory and all
```

EXAMPLE

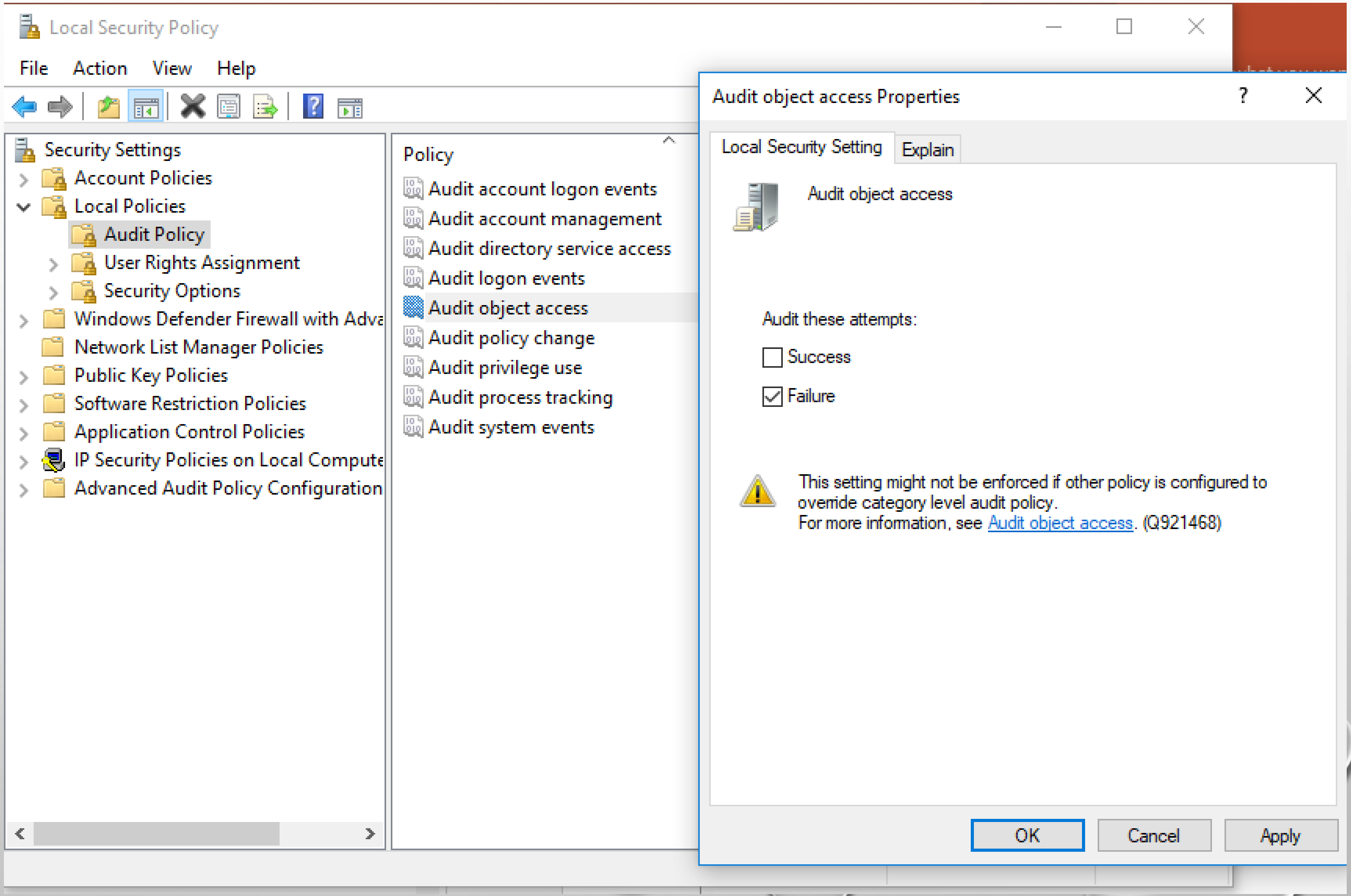
```
TAKEOWN /F C:\WINDOWS\SYSTEM32\ACME.EXE
```

```
TAKEOWN /F %WINDIR%\*.TXT
```

(IF YOU DO NOT USE KEY “/A” THEN THE CURRENT USER BECOMES FILE/FOLDER OWNER”)

AUDIT

- A FILE ACCESS AUDIT IS MONITORING AND RECORDING THE ACTIONS OF VARIOUS TYPE ACCESS TO FILES/FOLDERS
- TO SET THIS TYPE AUDIT IT IS NECESSARY TO USE THE "LOCAL SECURITY POLICY" UTILITY (1ST STAGE)


Local Security Policy

File Action View Help

Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Defender Firewall with Adva
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration

Policy
- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

Audit object access Properties

Local Security Setting | Explain

Audit object access

Audit these attempts:

☐ Success

☑ Failure

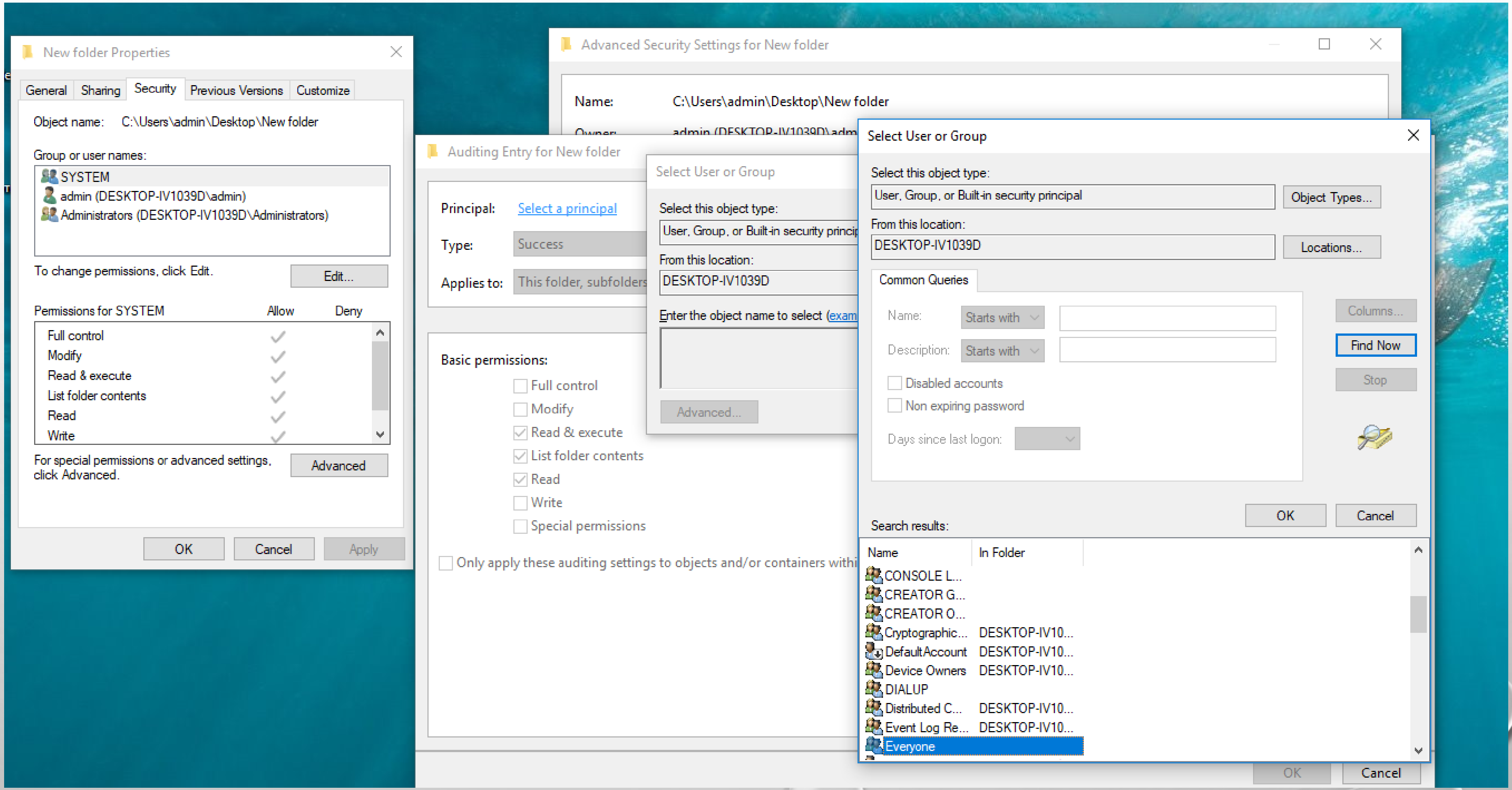
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit object access. (Q921468)

OK | Cancel | Apply

TYPES OF AUDIT

- “SUCCESS”: IF AN ACTION HAD BEEN ALLOWED TO THE USER (OR USERS) AND THIS USER WAS A SUCCESS IN REALIZING THIS ACTION
- “FAILURE”: IF AN ACTION HAD BEEN DENIED, BUT THE USER TRIED TO REALIZE THIS ACTION, THEY WAS NOT PERMITTED AND FAILED
- BOTH TYPE ATTEMPTS COULD BE FIXED IN THE SPECIAL SYSTEM LOG (JOURNAL)

2ND STAGE OF AUDIT: IDENTIFYING THE OBJECT, ACTION AND USER/USERS



New folder Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\admin\Desktop\New folder

Group or user names:
- SYSTEM
- admin (DESKTOP-IV1039D\admin)
- Administrators (DESKTOP-IV1039D\Administrators)

To change permissions, click Edit. Edit...

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

Advanced Security Settings for New folder

Name: C:\Users\admin\Desktop\New folder

Owner: admin (DESKTOP-IV1039D\adm

Auditing Entry for New folder

Principal: Select a principal

Type: Success

Applies to: This folder, subfolders

Basic permissions:
- [ ] Full control
- [ ] Modify
- [✓] Read & execute
- [✓] List folder contents
- [✓] Read
- [ ] Write
- [ ] Special permissions

[ ] Only apply these auditing settings to objects and/or containers withi

Select User or Group

Select this object type:
User, Group, or Built-in security princip

From this location:
DESKTOP-IV1039D

Enter the object name to select (exam

Advanced...

Select User or Group

Select this object type:
User, Group, or Built-in security principal — Object Types...

From this location:
DESKTOP-IV1039D — Locations...

Common Queries

Name: Starts with

Description: Starts with

[ ] Disabled accounts

[ ] Non expiring password

Days since last logon:

Columns... Find Now Stop

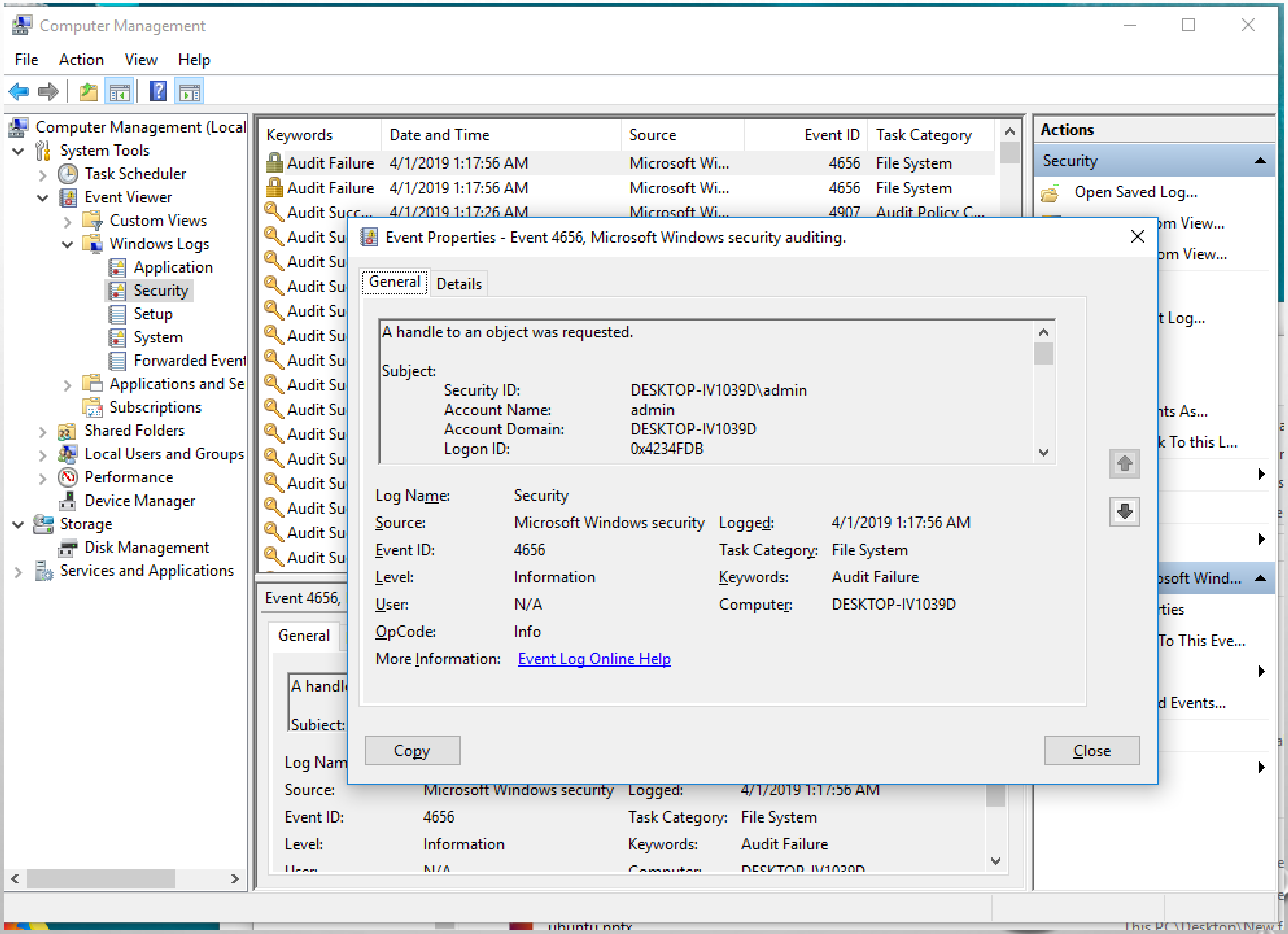
OK Cancel

Search results:

Name	In Folder
CONSOLE L...	
CREATOR G...	
CREATOR O...	
Cryptographic...	DESKTOP-IV10...
DefaultAccount	DESKTOP-IV10...
Device Owners	DESKTOP-IV10...
DIALUP	
Distributed C...	DESKTOP-IV10...
Event Log Re...	DESKTOP-IV10...
Everyone	

OK Cancel

3RD STAGE: AUDIT RESULTS



Keywords	Date and Time	Source	Event ID	Task Category
Audit Failure	4/1/2019 1:17:56 AM	Microsoft Wi...	4656	File System
Audit Failure	4/1/2019 1:17:56 AM	Microsoft Wi...	4656	File System
Audit Succ...	4/1/2019 1:17:26 AM	Microsoft Wi...	4907	Audit Policy C...

Event Properties - Event 4656, Microsoft Windows security auditing.

```
A handle to an object was requested.

Subject:
        Security ID:        DESKTOP-IV1039D\admin
        Account Name:       admin
        Account Domain:     DESKTOP-IV1039D
        Logon ID:           0x4234FDB
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          4/1/2019 1:17:56 AM
Event ID:          4656                         Task Category:   File System
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        DESKTOP-IV1039D
OpCode:            Info
More Information:  Event Log Online Help
```

TO STOP FILE ACCESS AUDITING

- FOR A FILE/FOLDER (PROPERTIES|SECURITY| ADVANCED SECURITY SETTINGS|AUDITING -> DELETE UNNECESSARY AUDITING)
- FOR THE SYSTEM IN A WHOLE (IMPLEMENTING THE “LOCAL SECURITY POLICY” UTILITY)