



Gold partner:



Generální partner:



How Active Directory Database Really Works

Michael Grafnetter
www.dsinternals.com

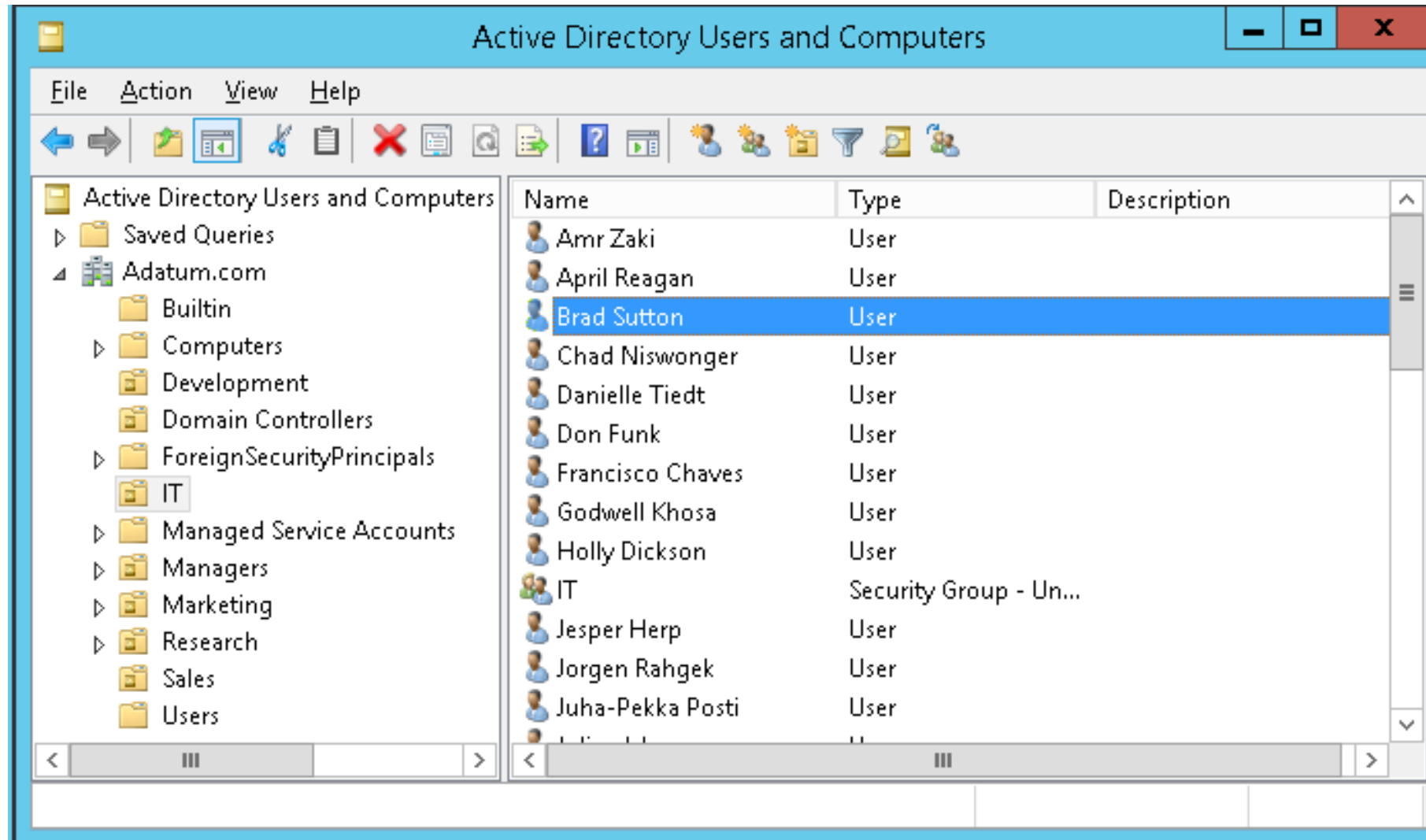
18. – 21. května 2015

Tech·Ed
DevCon 

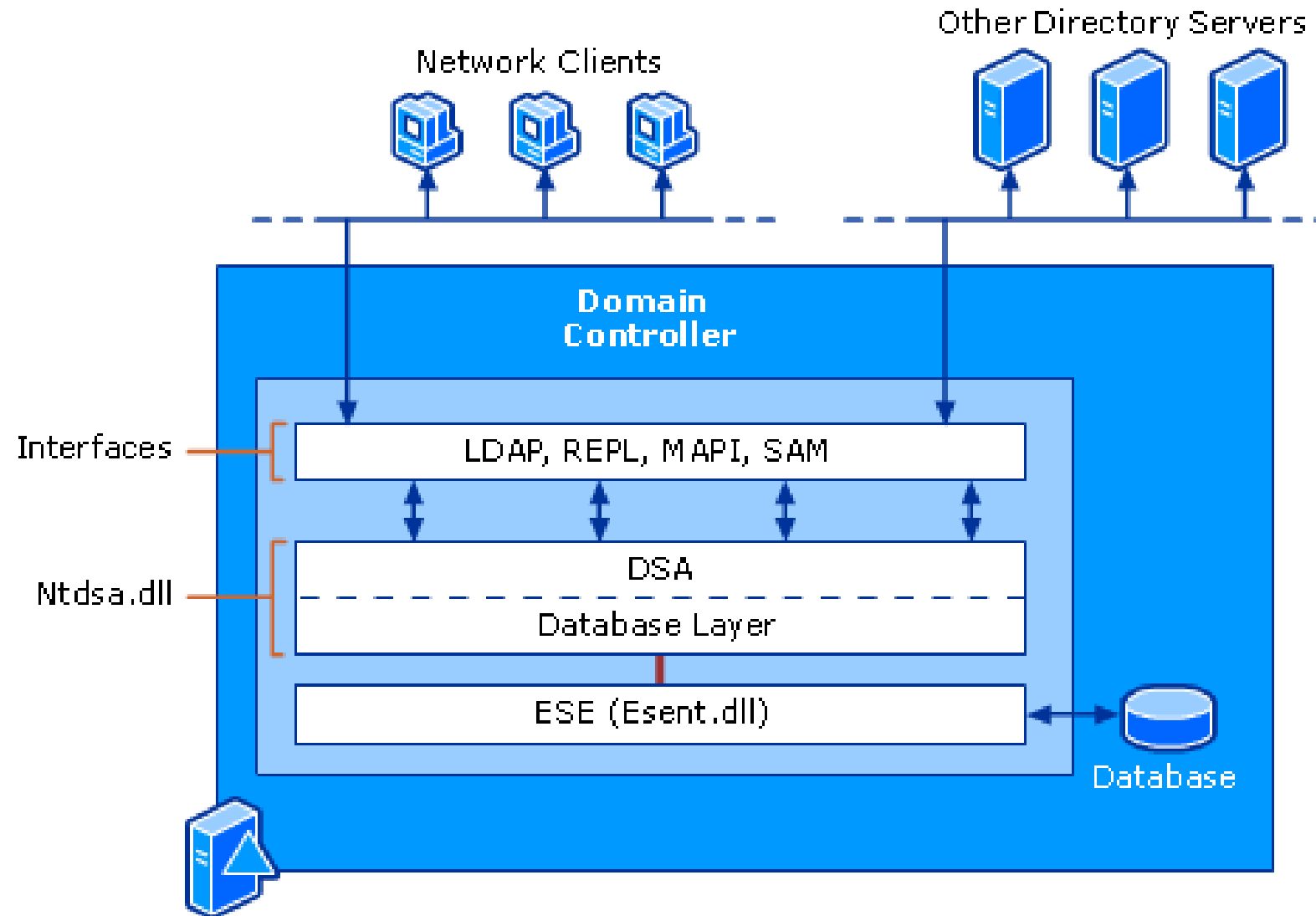
Agenda

- AD Database Structure
 - Tables
 - Columns
 - Links
 - Indices
- Query Optimization
- DB Maintenance

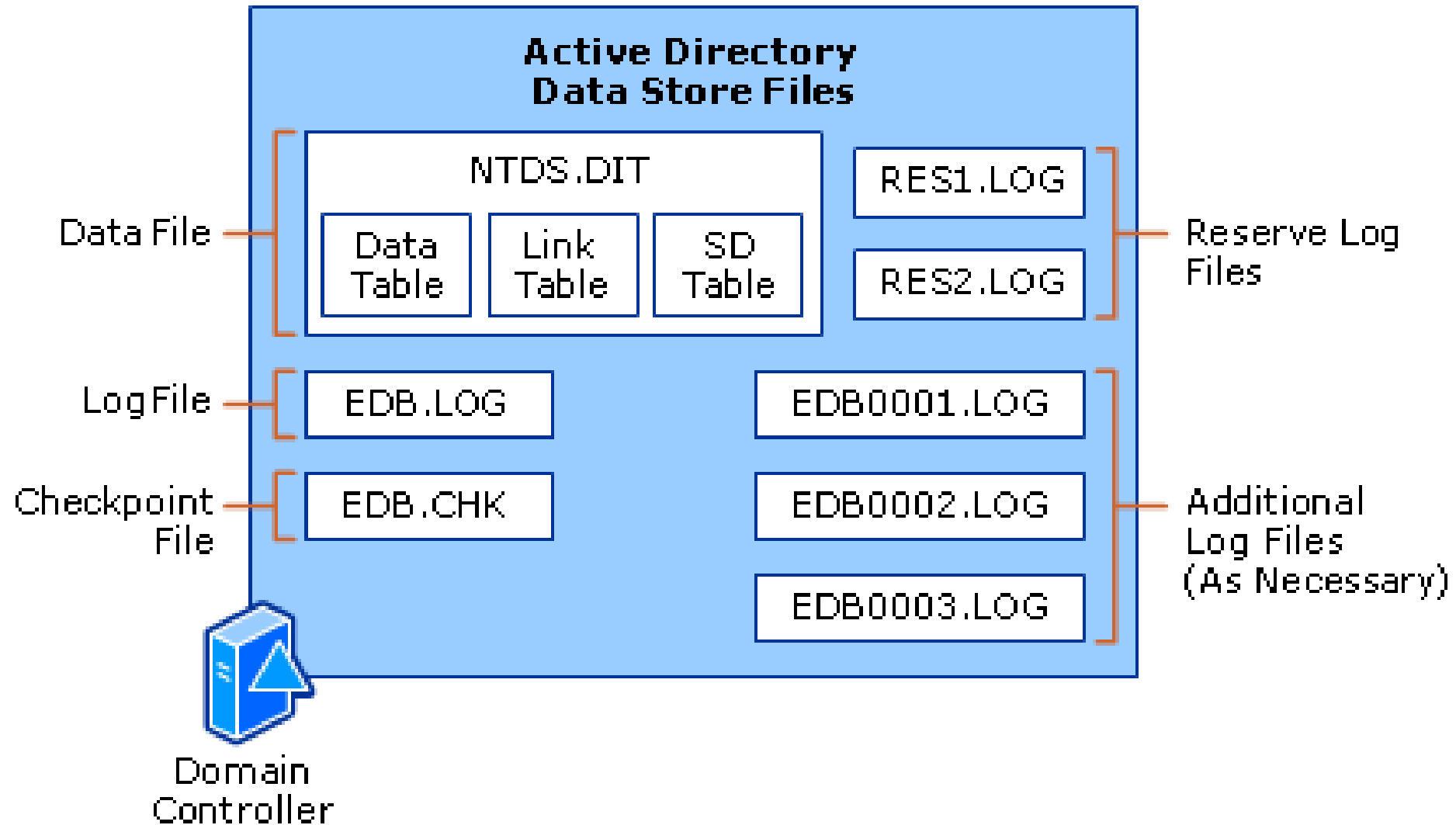
Active Directory



Active Directory Architecture



Active Directory Data Store



Dsomain

```
Administrator: Command Prompt
C:\>dsomain -dbpath C:\$SNAP_200803060849_UOLUMEC$\Windows\NTDS\ntds.dit -ldappo
rt 10389
EVENTLOG <Informational>: NTDS General / Service Control : 1000
Microsoft Active Directory Domain Services startup complete, version 6.0.6001.18
000
EVENTLOG <Informational>: NTDS General / Service Control : 1004
Active Directory Domain Services was shut down successfully.
C:\>_
```

Change Directory Server

Current Directory Server:
LON-DC1.Adatum.com

Change to:

☐ Any writable Domain Controller

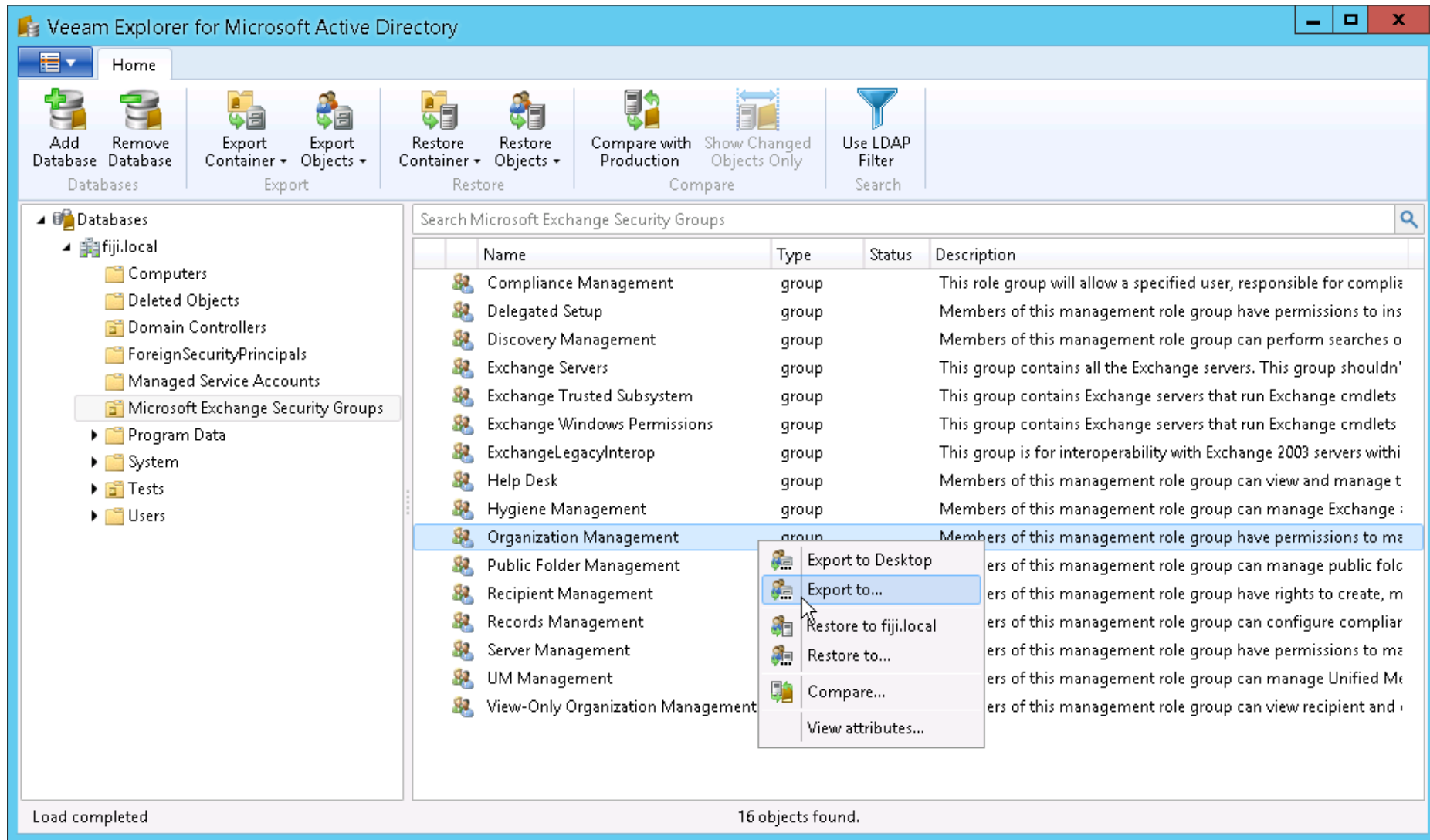
☒ This Domain Controller or AD LDS instance

Name	Site	DC Type	DC Version	Status
lon-dc1:10389				Pending...
LON-DC1.Adatum.com	Default-First-Site-Name	GC	Windows...	Online

☐ Save this setting for the current console

OKCancelHelp

Veeam Explorer for Active Directory



Esent Workbench

The screenshot displays the ESENT Workbench application window. The title bar reads "Esent Workbench". The menu bar includes "Database", "Schema", "Tools", and "Help".

Schema Tree (Left Panel):

- Schema
 - datatable
 - Columns
 - Indexes
 - DNT_index
 - DNT_col
 - Ancestors_index
 - Ancestors_col
 - delttime_not_recycled_ind
 - time_col
 - DRA_USN_CREATED_inde
 - NCDNT_col
 - ATTq131091
 - ATTi590692
 - DRA_USN_CRITICAL_inde
 - NCDNT_col

Schema Properties (Bottom Left):

☐ Descriptions

Editable

Comment	
---------	--

Non-Editable

Name	
Source File	ntds.dit
Table Count	9
Version	1

Database Properties (Bottom Right):

bkinfoCopyPrev	JET_BKINFO(0-0:JET_LGPOS(0x0,0,0):JET_BKLOGTIME(0:0:0:0:0:0:0x0:0x0))
bkinfoDiffPrev	JET_BKINFO(0-0:JET_LGPOS(0x0,0,0):JET_BKLOGTIME(0:0:0:0:0:0:0x0:0x0))
bkinfoFullCur	JET_BKINFO(0-0:JET_LGPOS(0x0,0,0):JET_BKLOGTIME(0:0:0:0:0:0:0x0:0x0))

Table List (Main Panel):

ntds.dit (34.0 MB) Max Browse Rows: 500 Export

*	Name	Columns	Indexes	Rows	Id		
	datatable	1307	176	4266	JET_TABLEID(0x92c0020)	Browse Data	Export
	hiddentable	12	0	1	JET_TABLEID(0x92c02a0)	Browse Data	Export
	link_history_table	15	8	0	JET_TABLEID(0x92c03e0)	Browse Data	Export
	link_table	10	13	457	JET_TABLEID(0x92c02a0)	Browse Data	Export
	quota_rebuild_progress_table	3	0	1	JET_TABLEID(0x92c03e0)	Browse Data	Export
	quota_table	4	1	26	JET_TABLEID(0x92c02a0)	Browse Data	Export
	sd_table	4	2	140	JET_TABLEID(0x92c03e0)	Browse Data	Export
	sdpropcounttable	1	0	1	JET_TABLEID(0x92c02a0)	Browse Data	Export
	sdproptable	7	4	0	JET_TABLEID(0x92c03e0)	Browse Data	Export

Status Bar: C:\SW\NTDS\Demos\Dump\ntds.dit 8:17:14 AM

DEMO

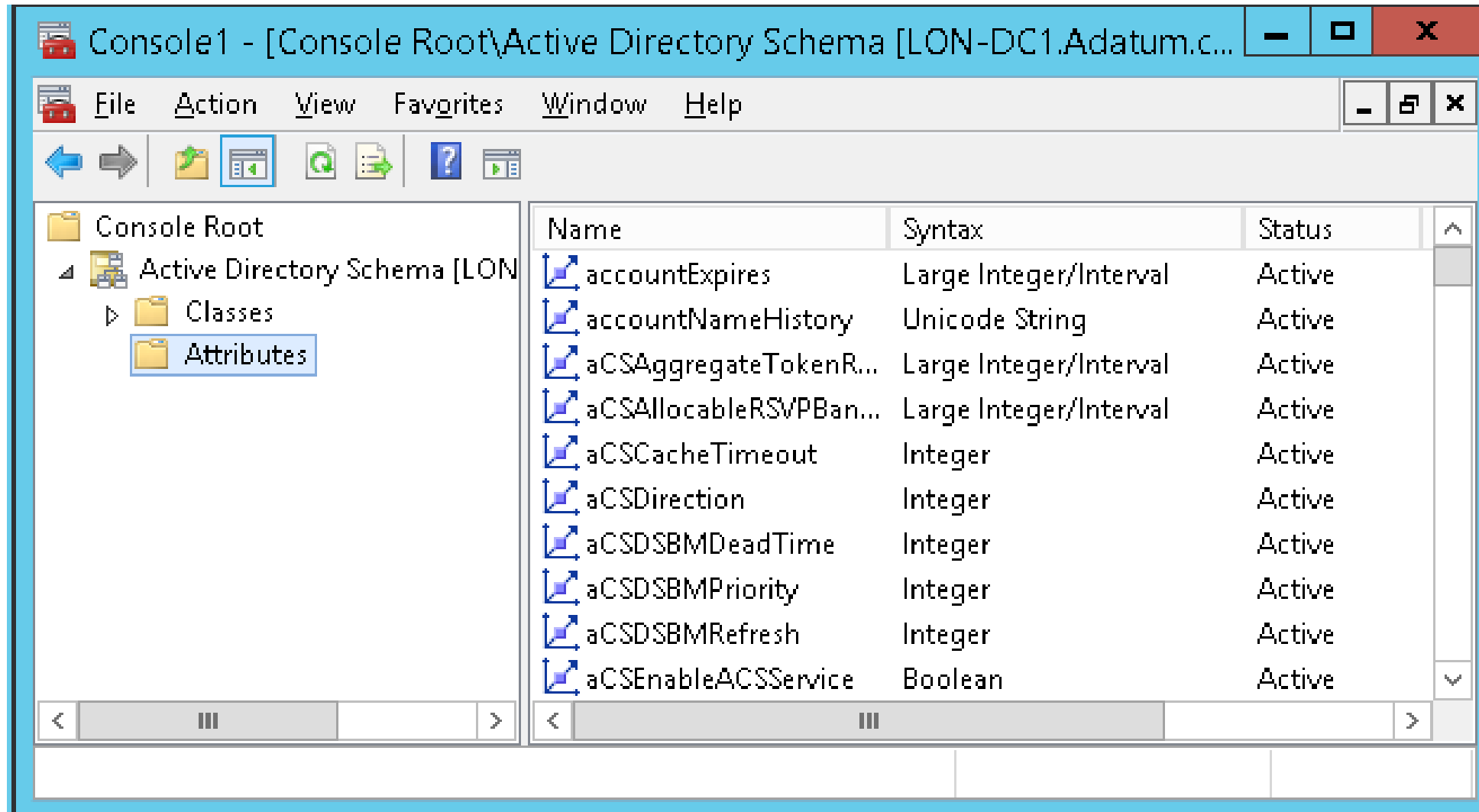
Datatable

DNT	PDNT	RDN	objectClass	sAMAccountName	unicodePwd	isDeleted
50	10	contoso	domain			false
100	50	Employees	ou			false
101	100	Bob	user	bob	2c4871c894...	false
102	100	John	user	john	d70c62e716...	false
200	50	Computers	container			false
201	200	PC01	computer	PC01\$	8bc50a4045...	false

Partitions

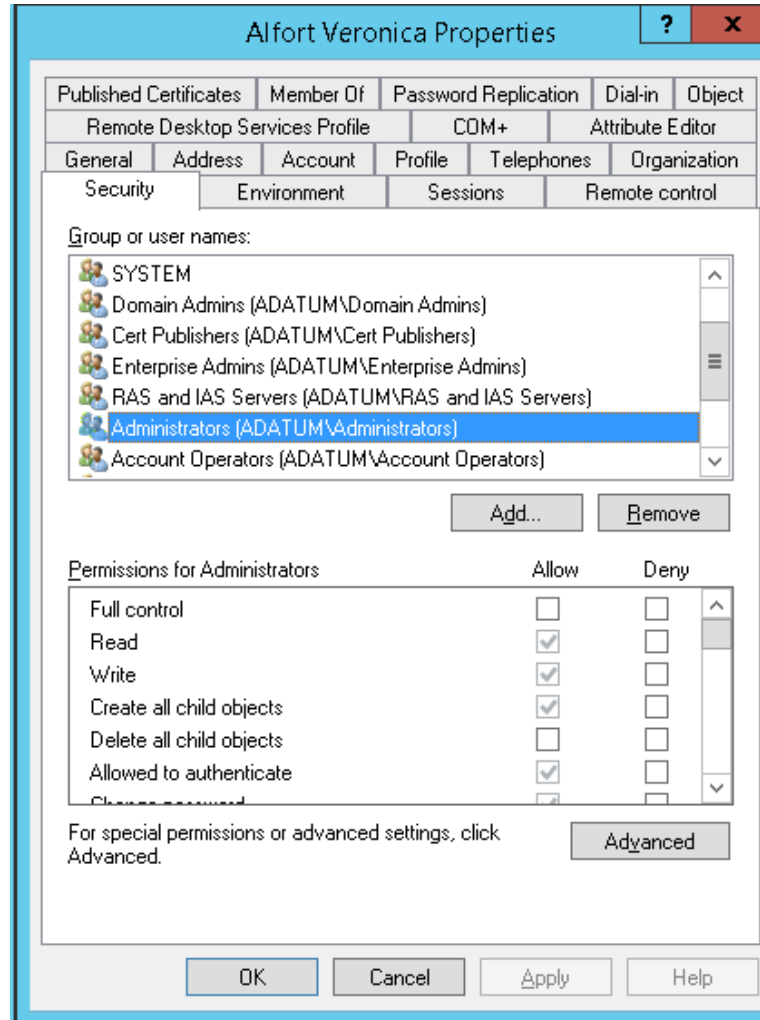
Domain Partition	DNT	PDNT	NCDNT	OBJ	RDN	objectguid
	1787	2	-	FALSE	local	-
	1788	1787	2	TRUE	contoso	c9e9a085-9bef-4067-9d21-d2fabecbb866
	1795	1788	1788	TRUE	Users	9d43690b-176b-44dc-b0ba-25ab36d5bbd3
	3830	1795	1788	TRUE	Dave	de7c3334-6ba2-4c91-a988-099a269200ed
Configuration	1789	1788	2	TRUE	Configuration	3b1a5b3a-050e-4133-9b19-a75a587f2ea3
	1790	1789	1789	TRUE	Sites	38452447-ed00-4aa0-b7d9-b3b32757370d
Schema	5	4	-	FALSE	Schema	c0245e4c-0f09-4068-a778-196a86719439
	1730	5	-	FALSE	User-Principal-Name	c62ebec9-4fdb-43f6-9138-ffd1a073aeaf
Global Catalog	3849	1788	1788	TRUE	child	42c7cf2d-ffc3-4e1d-9c18-a2f8782fa94a
	3862	3849	3849	TRUE	Domain Controllers	2f7249cf-a892-4568-af48-73b764da587d
	4054	3862	3849	TRUE	ChildDC	3ca6371b-fcfb-4ddf-ab1d-d56c3f474e86

Schema



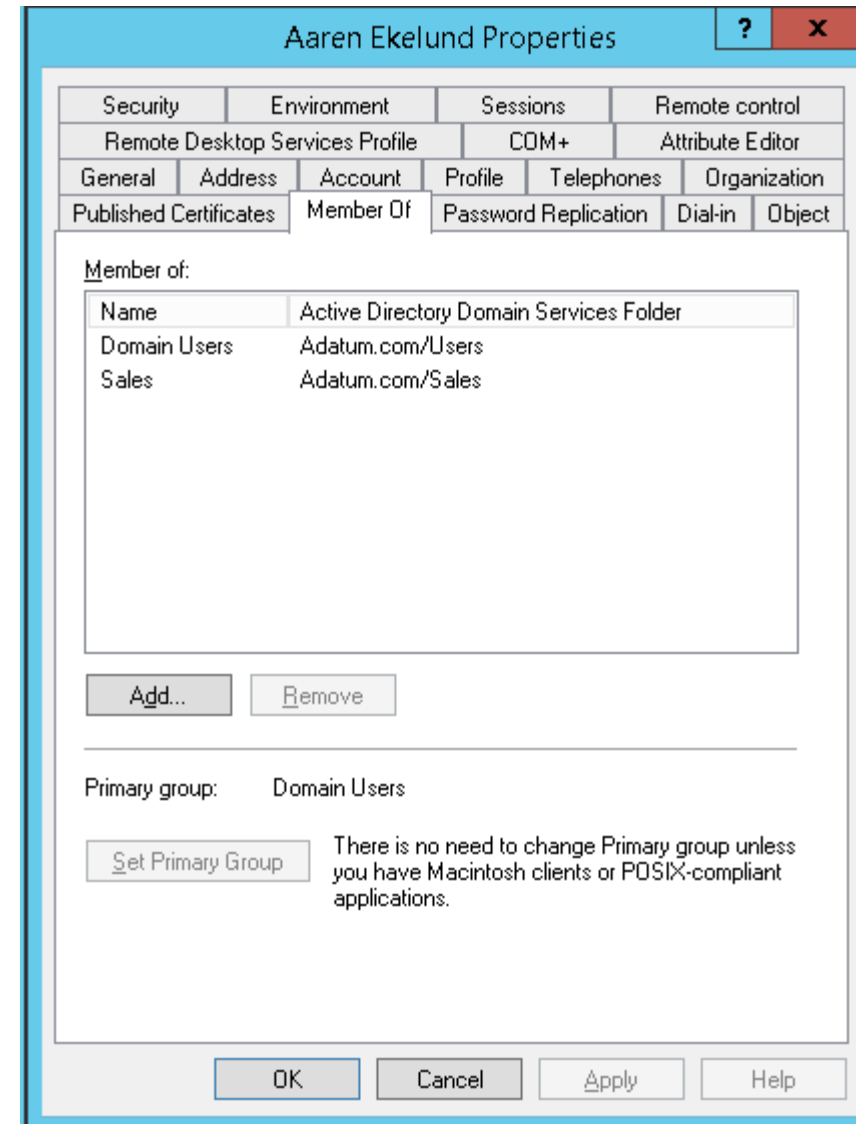
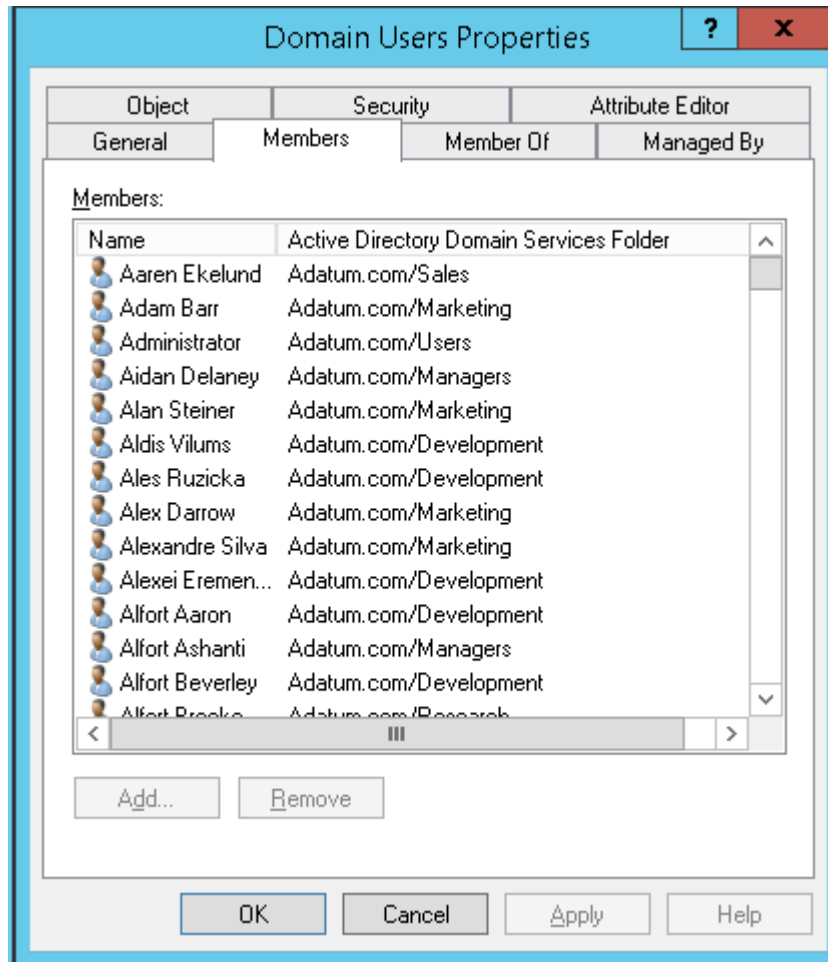
DEMO

Security Descriptors

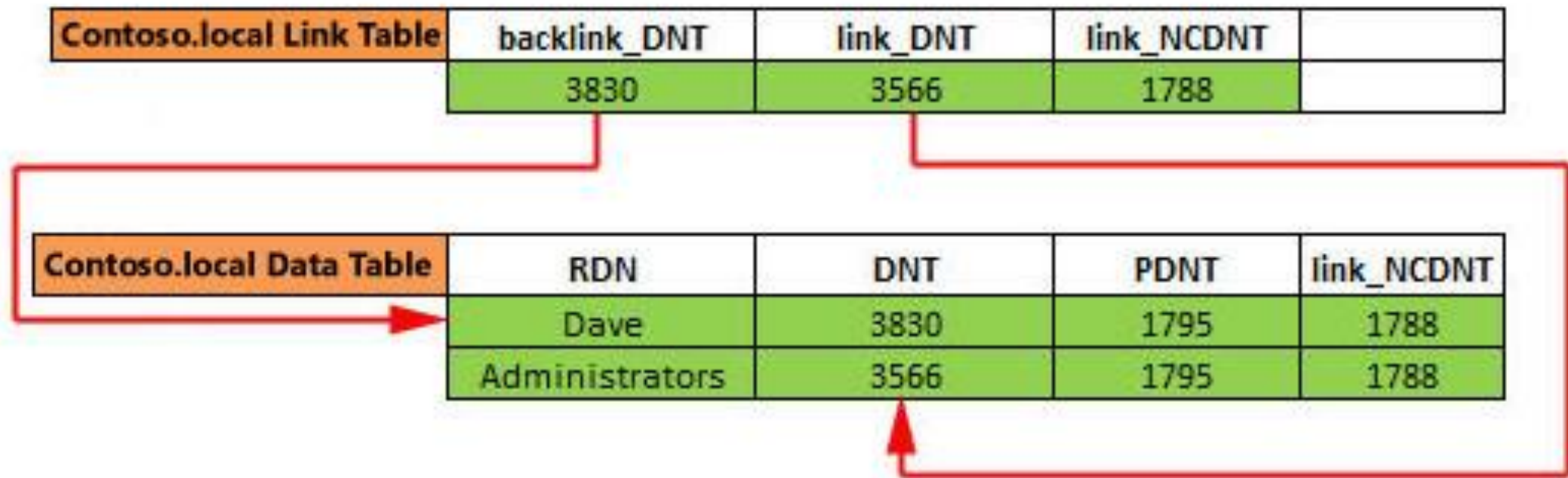


DEMO

Linked Multivalued Attributes



Linked Multivalued Attributes



DEMO

Phantom Objects

Child.contoso.local Data Table	DNT	PDNT	NCDNT	OBJ	RDN	objectguid
	5584	1788	-	FALSE	Users	-
Phantom Object →	5585	5584	-	FALSE	Dave	de7c3334-6ba2-4c91-a988-099a269200ed
	3567	2467	3849	TRUE	Administrators	f5893334-2ab6-4c91-b678-7880abced021

Operations Masters

RID PDC Infrastructure

The infrastructure master ensures consistency of objects for inter-domain operations. Only one server in the domain performs this role.

Operations master:
LON-DC1.Adatum.com

To transfer the operations master role to the following computer, click Change.
LON-DC1.Adatum.com

Change...

Close Cancel

Hidden Table

- DC Object Link
- DC OS Version
- Highest Committed USN
- Epoch
- Last Backup USN
- ...

DEMO

Query Optimization

Query Performance Matters

```
PS C:\> Measure-Command { Get-ADUser -Filter { TelephoneNumber -eq '609788135' } }
```

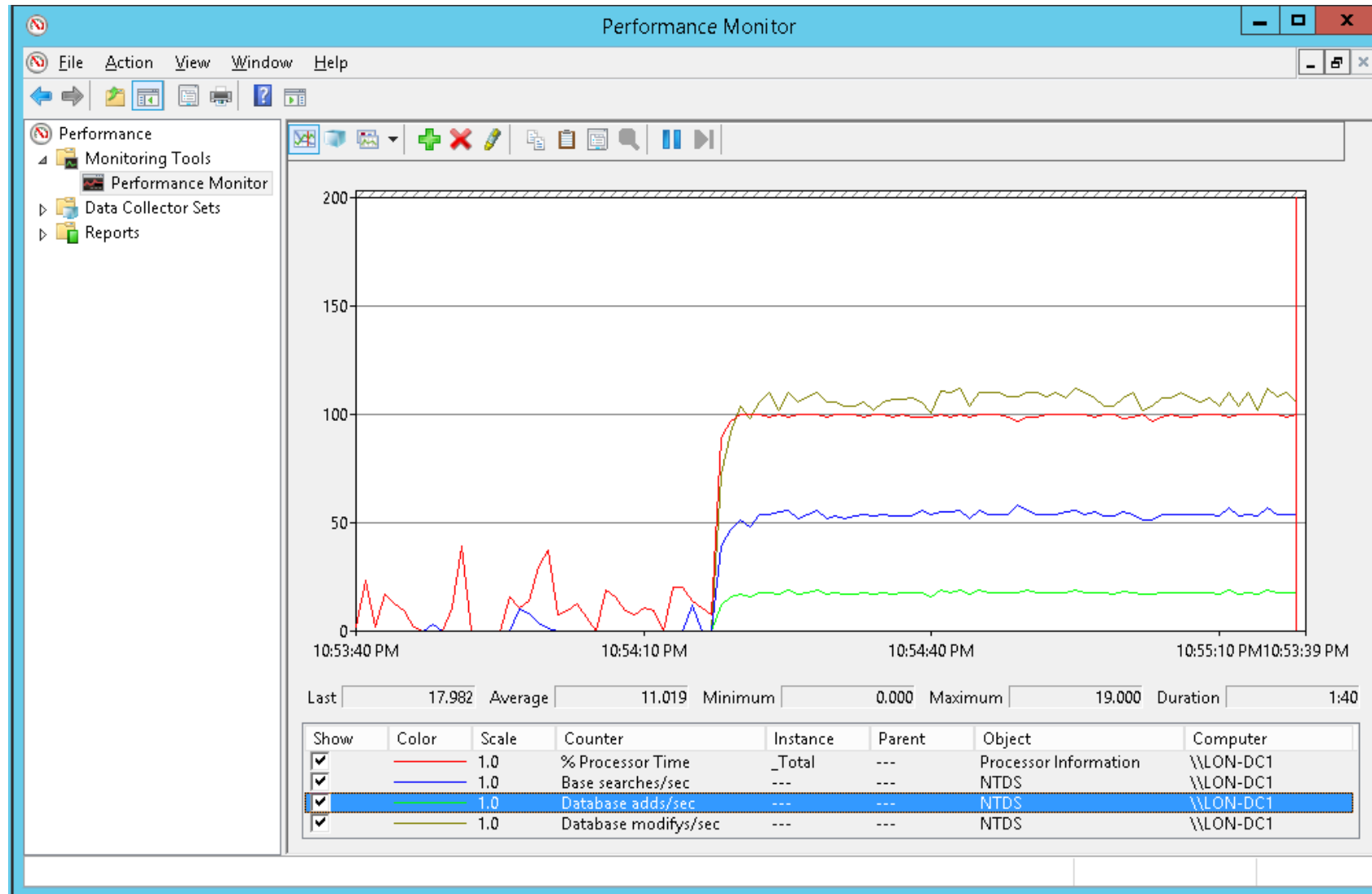
```
Days           : 0
Hours          : 0
Minutes        : 0
Seconds        : 11
Milliseconds    : 540
Ticks          : 115401199
TotalDays      : 0.000133566202546296
TotalHours     : 0.00320558886111111
TotalMinutes   : 0.192335331666667
TotalSeconds   : 11.5401199
TotalMilliseconds : 11540.1199
```

```
PS C:\> Measure-Command { Get-ADUser -Filter { Surname -eq 'Zaki' } }
```

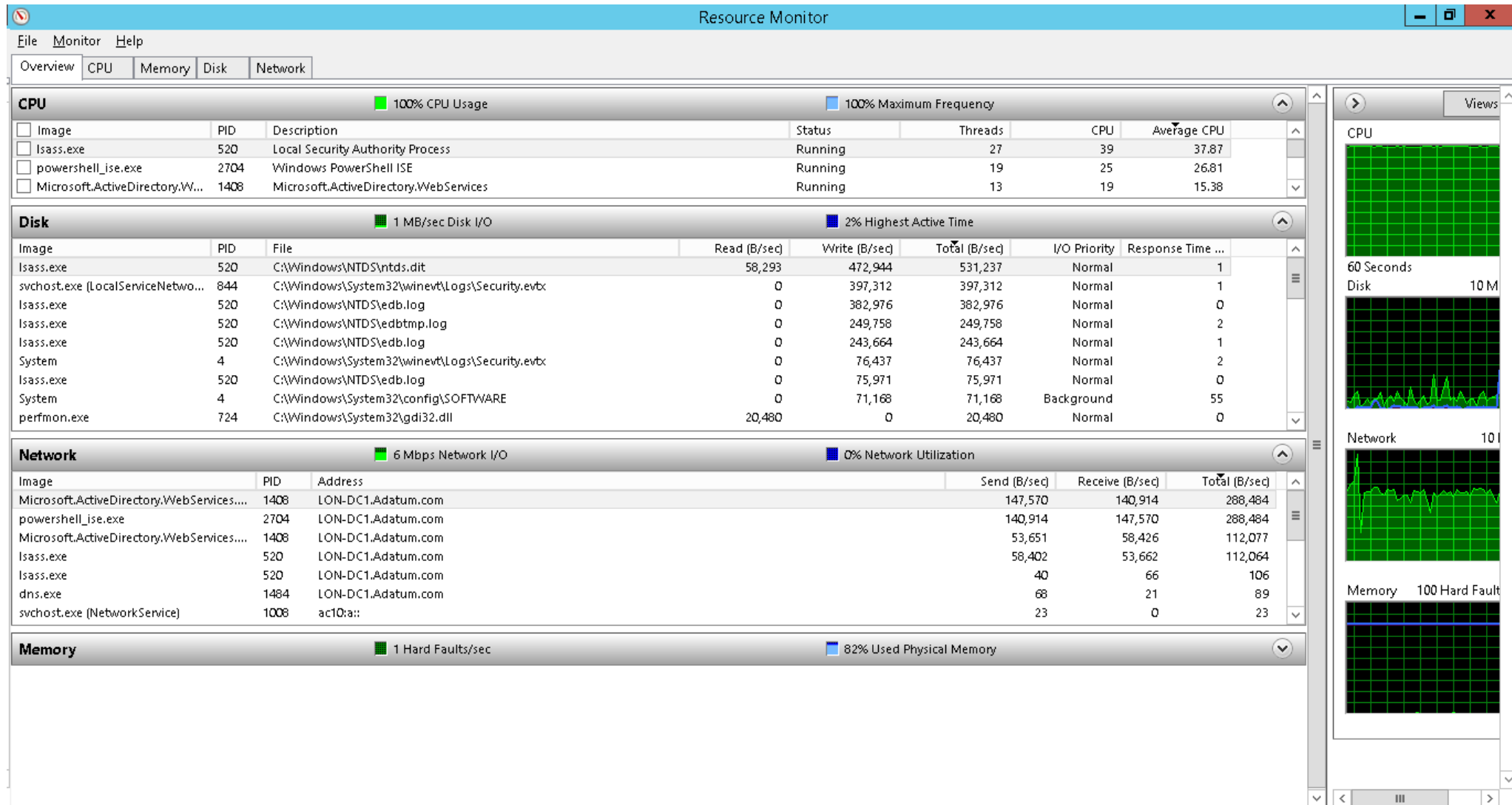
```
Days           : 0
Hours          : 0
Minutes        : 0
Seconds        : 0
Milliseconds    : 30
Ticks          : 304094
TotalDays      : 3.51960648148148E-07
TotalHours     : 8.44705555555556E-06
TotalMinutes   : 0.000506823333333333
TotalSeconds   : 0.0304094
TotalMilliseconds : 30.4094
```

DEMO

Creating a Large AD Database



Creating a Large AD Database



Active Directory Index Types

- Attribute Index
- Containerized Index (PDNT+Attribute)
- Tuple Index
- Subtree Index (Virtual List View Support)

The screenshot shows the 'sn Properties' dialog box with the following details:

- General Tab:**
 - Description:** Surname
 - Common Name:** Surname
 - X.500 OID:** 2.5.4.4
 - Syntax and Range:**
 - Syntax:** Unicode String
 - Minimum:** 1
 - Maximum:** 64
 - This attribute is single-valued.**
- Checkboxes:**
 - ☒ Attribute is active
 - ☒ Index this attribute
 - ☐ Ambiguous Name Resolution (ANR)
 - ☒ Replicate this attribute to the Global Catalog
 - ☐ Attribute is copied when duplicating a user
 - ☐ Index this attribute for containerized searches

Tuple Index

"Active Dir"

"ctive Dire"

"tive Direc"

"ive Direct"

"ve Directo"

"e Director"

" Directory"

"Directory"

"irectory"

"rectory"

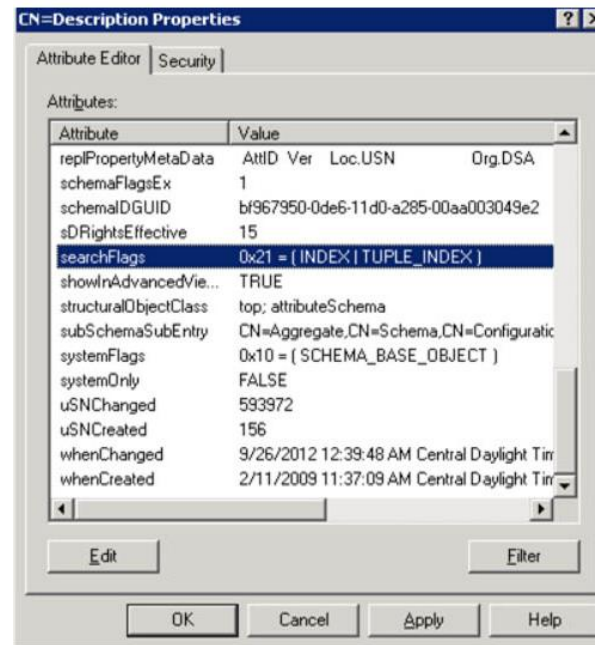
"ectory"

"ctory"

"tory"

"ory"

SearchFlags Attribute



Type	Read-Only Domain Controller FAS	Disable Auditing	Confidential	Subtree Index (VLV)	Tuple Index	Copy	Preserve on Deletion	Ambiguous Name Resolution (ANR)	Containerized Index	Attribute Index
Value Hex	0x00000200	0x00000100	0x00000080	0x00000040	0x00000020	0x00000010	0x00000008	0x00000004	0x00000002	0x00000001
Value Decimal	512	256	128	64	32	16	8	4	2	1
Bit	1000000000	0100000000	0010000000	0001000000	0000100000	0000010000	0000001000	0000000100	0000000010	000000000001

Indexed Attributes

Name	Syntax	Description
common-Name	Unicode String	Common-Name
display-Name	Unicode String	Display-Name
given-Name	Unicode String	Given-Name
group-Type	Integer	Group-Type
LDAP-Display-Name	Unicode String	LDAP-Display-Name
location	Unicode String	Location
Mail	Unicode String	E-mail-Addresses
name	Unicode string	RDN
object-Guid	Octet string	Object-Guid
object-Sid	SID	Object-Sid
organizational-Unit-Name	Unicode string	Organizational-Unit-Name
sAM-Account-Name	Unicode string	SAM-Account-Name
service-Principal-Name	Unicode string	Service-Principal-Name
sID-History	SID	SID-History
surname	Unicode string	Surname
user-Account-Control	Integer	User-Account-Control
user-Principal-Name	Unicode string	User-Principal-Name



ANR Queries

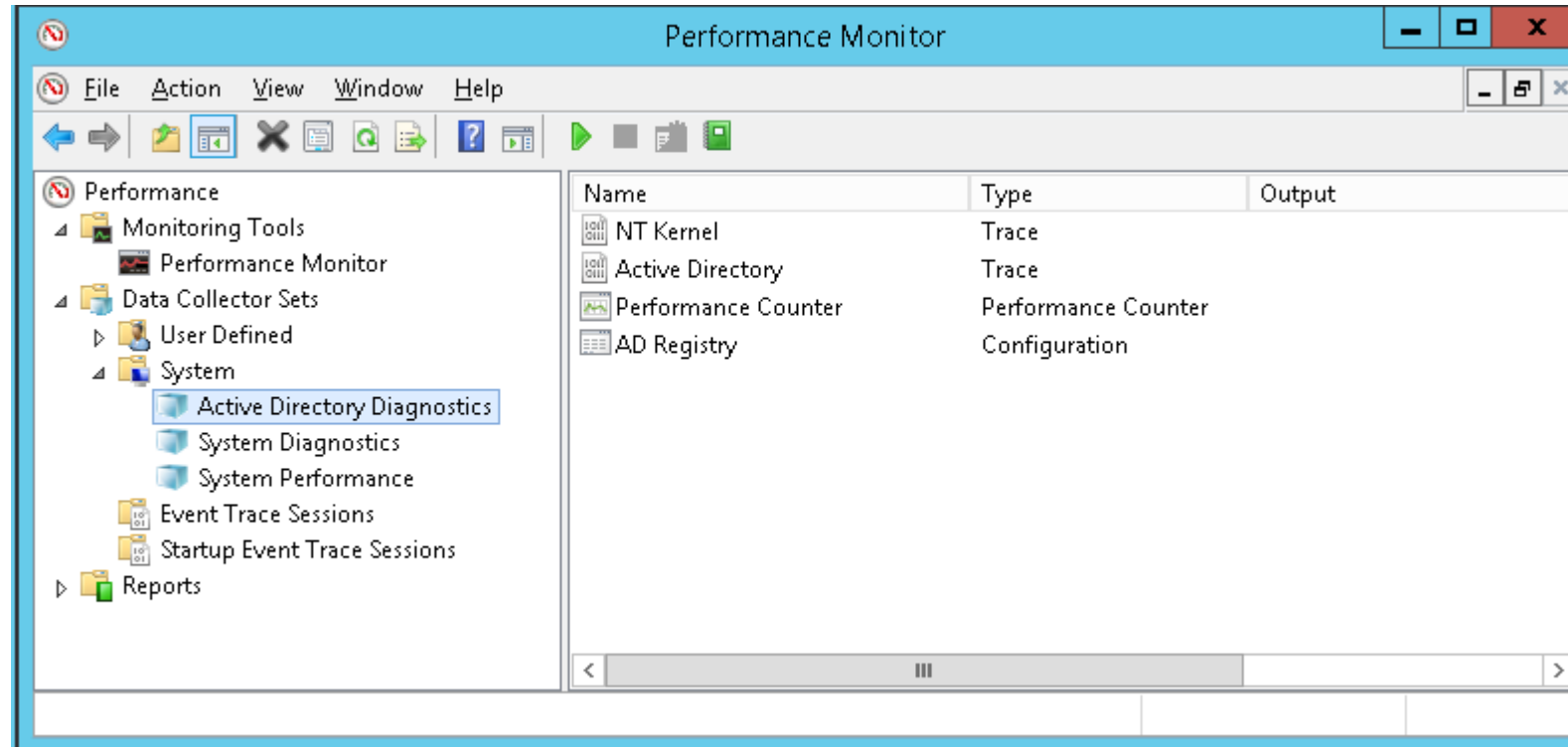
The screenshot shows the 'sn Properties' dialog box with the 'General' tab selected. The dialog contains the following fields and options:

- Description:** Surname
- Common Name:** Surname
- X.500 OID:** 2.5.4.4
- Syntax and Range:**
 - Syntax:** Unicode String
 - Minimum:** 1
 - Maximum:** 64
- This attribute is single-valued.**
- Attribute is active:** ☒
- Index this attribute:** ☒
- Ambiguous Name Resolution (ANR):** ☐ (highlighted with a dotted border)
- Replicate this attribute to the Global Catalog:** ☒
- Attribute is copied when duplicating a user:** ☐
- Index this attribute for containerized searches:** ☐



Buttons at the bottom: OK, Cancel, Apply, Help.


DEMO

Active Directory Diagnostics



Active Directory Diagnostics

LDAP Request Status Codes 					Top: 4 of 4
Exit ID	Result	Requests/sec	Response Time(ms)	CPU%	
4	Size Limit Exceeded	0.2	421	6.22	
0	Success	31.5	1	1.53	
14		0.0	31	0.00	
32	No Such Object	0.0	3	0.00	

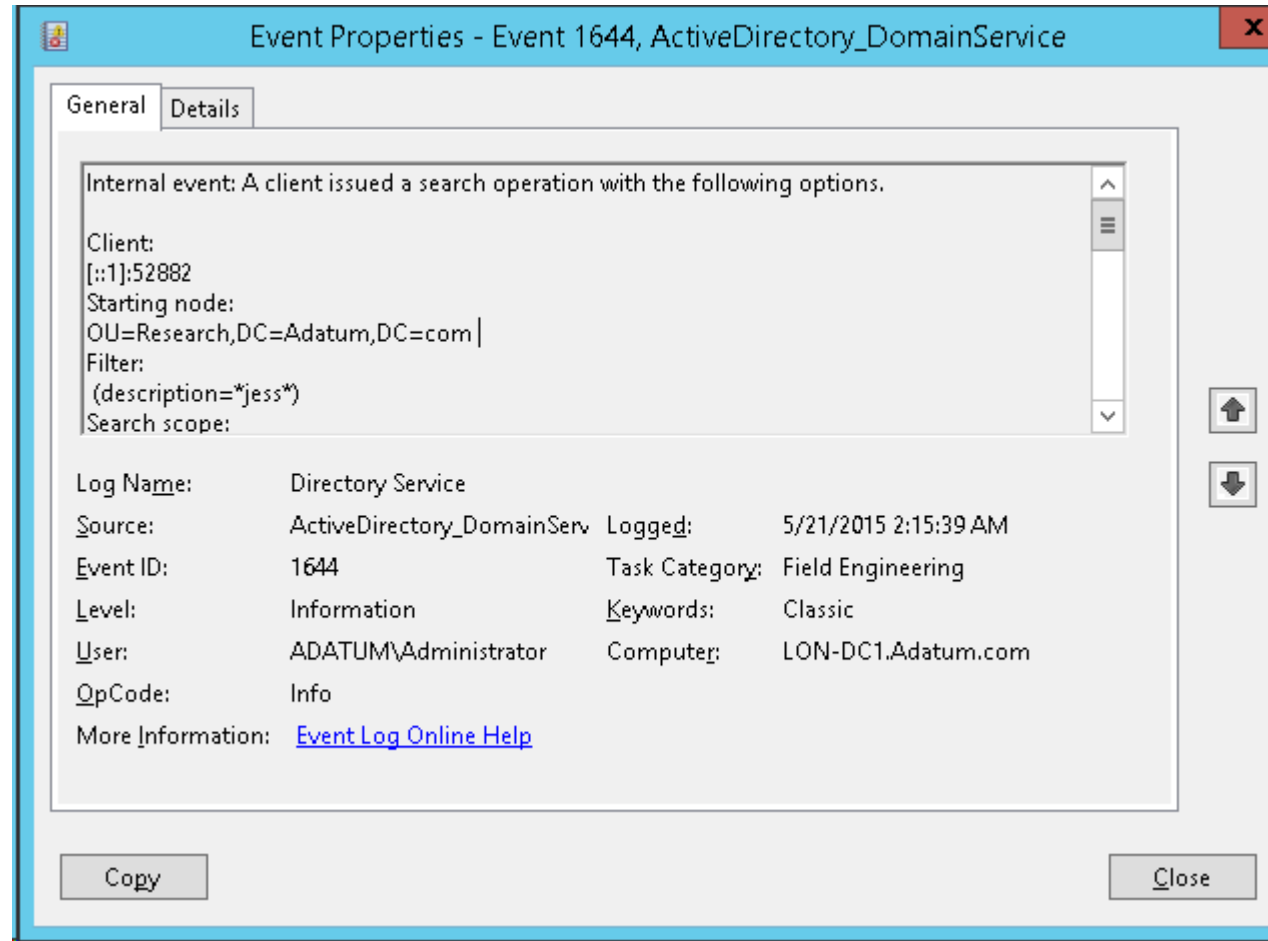
Unique Searches 												Top: 25 of 25
Client	Instance	Scope	Object Name	Filter Name	Index	Status	Visited	Found	Requests/sec	Response Time(ms)	CPU%	
[fe80::c19:dd46:4bf1:7be%11]:64374	NTDS	deep	[]	(description="test")	DNT_index:815955:N;	0	16,248	1,000	0.2	358	5.0	
[fe80::c19:dd46:4bf1:7be%11]:64381	NTDS	deep	DC=temores,DC=org	(description="test")	DNT_index:815955:N;	0	16,448	1,000	0.0	534	0.3	
[fe80::c19:dd46:4bf1:7be%11]:64372	NTDS	one-level	ou=user,DC=temores,DC=org	(description="test")	DNT_index:250224:N;	0	16,449	1,000	0.0	135	0.1	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	(TRUE)	PDNT_index:0:N;	0	257	256	0.0	51	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	769	768	0.0	35	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	513	512	0.0	26	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	1,025	1,024	0.0	26	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	2,049	2,048	0.0	23	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	1,281	1,280	0.0	21	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	2,305	2,304	0.0	19	0.0	
[fe80::c19:dd46:4bf1:7be%11]:64382	NTDS	one-level	CN=Schema,CN=Configuration,DC=temores,DC=org	[]	[]	0	3,585	3,584	0.0	20	0.0	

DEMO

Enabling Diagnostic Events

- Expensive queries: Visit too many objects
- Inefficient queries: return less than 10% of visited objects
- HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
 - 15 Field Engineering = 5 (Default = 0)
- HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
 - Expensive Search Results Threshold = 10 000
 - Inefficient Search Results Threshold = 1 000

Inefficient Query Event



DEMO

LDAP Search Statistics Control

Controls

Object Identifier:

Value:

Control Type: ☒ Server ☐ Client

☐ Critical

Description:

Load Predefined:

<< Check Out Check in >> OK

***Searching...

ldap_search_ext_s(ld, "DC=temores,DC=org", 2, "(description=*test*)", attrList, 0, svrCtrls, CntCtrls, 60, 1000, &msg)

Error: Search: Size Limit Exceeded. <4>

Server error:

Result <4>:

Stats:

Call Time: 1968 (ms)
Entries Returned: 1000
Entries Visited: 16199
Used Filter: (description=*test*)
Used Indexes: DNT_index:594082:N;
Pages Referenced: 91712
Pages Read From Disk: 103
Pages Pre-read From Disk: 2848
Clean Pages Modified: 0
Dirty Pages Modified: 0
Log Records Generated: 0
Log Record Bytes Generated: 0

Getting 1000 entries:

<Skipping search results display (search options)...>

Used Indexes: INTERSECT_INDEX:7027:I;

Index Name.

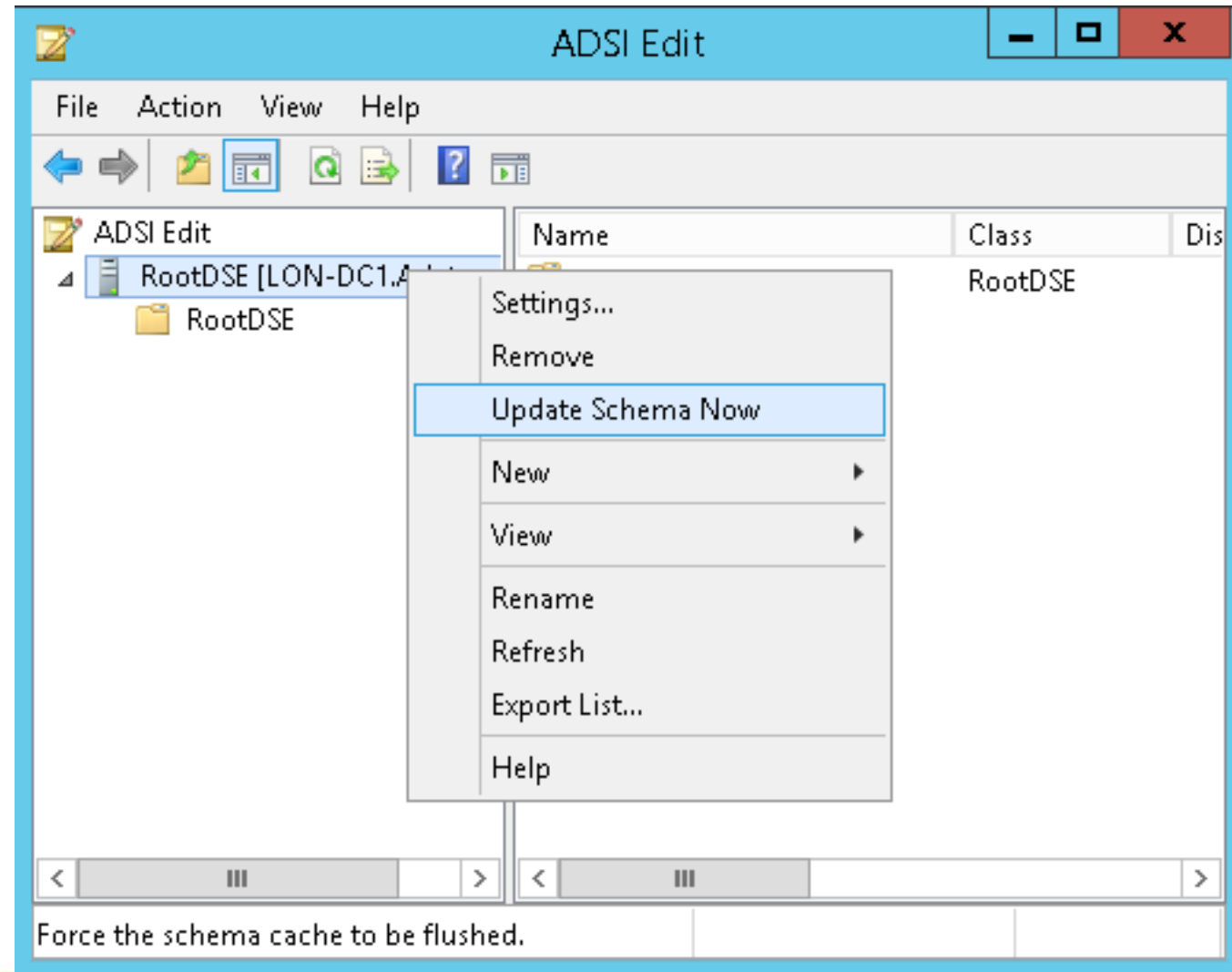
- Approximate record count.

- Index Type:

- o N is Normal;
- o P is containerized;
- o I is Intersection Index (the result is a temporary Table)
- o T is Tuple Index.

DEMO

Deferred Index Creation (2012+)



Database Maintenance

IFM Backup

```
Administrator: Command Prompt
D:\Users\Administrator>ntdsutil "activate instance ntds" ifm "create full test"
quit quit
ntdsutil: activate instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: create full test
Creating snapshot...
Snapshot set {e598c389-e490-4d15-ae2e-2c9790b4e54f} generated successfully.
Snapshot {d8ff1291-cfe9-4cda-8a51-690eea384012} mounted as D:\$SNAP_200808112131_UOLUMED$\
Snapshot {d8ff1291-cfe9-4cda-8a51-690eea384012} is already mounted.
Initiating DEFRAGMENTATION mode...
Source Database: D:\$SNAP_200808112131_UOLUMED$\Windows\NTDS\ntds.dit
Target Database: D:\Users\Administrator\test\Active Directory\ntds.dit

Defragmentation Status (% complete)

0    10   20   30   40   50   60   70   80   90  100
|---|---|---|---|---|---|---|---|---|---|
.....

Copying registry files...
Copying D:\Users\Administrator\test\registry\SYSTEM
Copying D:\Users\Administrator\test\registry\SECURITY
Snapshot {d8ff1291-cfe9-4cda-8a51-690eea384012} unmounted.
IFM media created successfully in D:\Users\Administrator\test
ifm: quit
ntdsutil: quit

D:\Users\Administrator>
```

Active Directory Domain Services Installation Wizard

Install from Media


Select one of the following options, depending on whether you want to replicate domain data over the network from an existing domain controller or you want to replicate domain data from media created from an existing domain controller (install from media). In either case, the existing domain controller must be in the same domain as the new domain controller.

☒ Replicate data over the network from an existing domain controller

☐ Replicate data from media at the following location

Consult the help to make sure that the media you are using is compatible with the type of domain controller you are installing. Even if you select this option, some data is copied over the network.

Location:

 The media you select must have been created from a writable domain controller, not a read-only domain controller.

[More about install from media](#)

< Back Next > Cancel

Space Usage

***** SPACE DUMP *****						
Name	Type	ObjidFDP	PgnoFDP	PriExt	Owned	Available
C:\Windows\NTDS\ntds.dit	Db	1	1	256-n	7688	98
datatable	Tbl	8	257	226-n	6841	38
<Long Values>	LU	145	598	0-n	853	6
ancestors_index	Idx	148	585	0-n	73	2
deltline_not_recycled_	Idx	132	577	1-s	1	0
DRA_USM_CREATED_index	Idx	141	586	0-n	63	7
DRA_USM_CRITICAL_inde	Idx	134	579	1-s	1	0
DRA_USM_index	Idx	135	588	0-n	57	5
INDEX_000000000	Idx	138	575	0-n	185	14
INDEX_000000003	Idx	170	753	0-n	192	12
INDEX_000000004	Idx	129	574	1-s	1	0
INDEX_000000007	Idx	14	263	1-s	1	0
INDEX_9F8C9373	Idx	271	5865	1-s	1	0
INDEX_F_00000000AD	Idx	73	518	1-s	1	0
INDEX_F_00000000CE	Idx	82	527	1-s	1	0
INDEX_F_81D62047	Idx	273	5883	1-s	1	0
INDEX_F_8331CF33	Idx	222	4679	0-n	57	4
INDEX_F_83E6ADC7	Idx	235	4712	1-s	1	0
INDEX_F_87B0BF31	Idx	224	4681	1-s	1	0
INDEX_F_995291A3	Idx	228	4677	1-s	1	0
INDEX_F_9C63CE18	Idx	255	4941	1-s	1	0
INDEX_F_9DB9D4E4	Idx	274	5884	1-s	1	0
INDEX_F_9DCFAEE6	Idx	226	4683	1-s	1	0
INDEX_F_9E000000	Idx	332	259482	0-n	151	15
INDEX_F_9E0000004	Idx	332	259482	0-n	151	15
LCL_ABVIEW_index000000	Idx	167	584	1-s	1	0
NC_Acc_Type_Name	Idx	138	583	0-n	1977	13
NC_Acc_Type_Sid	Idx	143	588	0-n	3241	4
nc_guid_index	Idx	137	582	0-n	2515	8
PINT_index	Idx	164	563	0-n	2148	12
PhantomIndex22	Idx	131	576	1-s	1	0
processlinks_index	Idx	136	581	1-s	1	0
recycling_index	Idx	133	578	0-n	25	12

Event Properties - Event 700, NTDS ISAM

General
Details

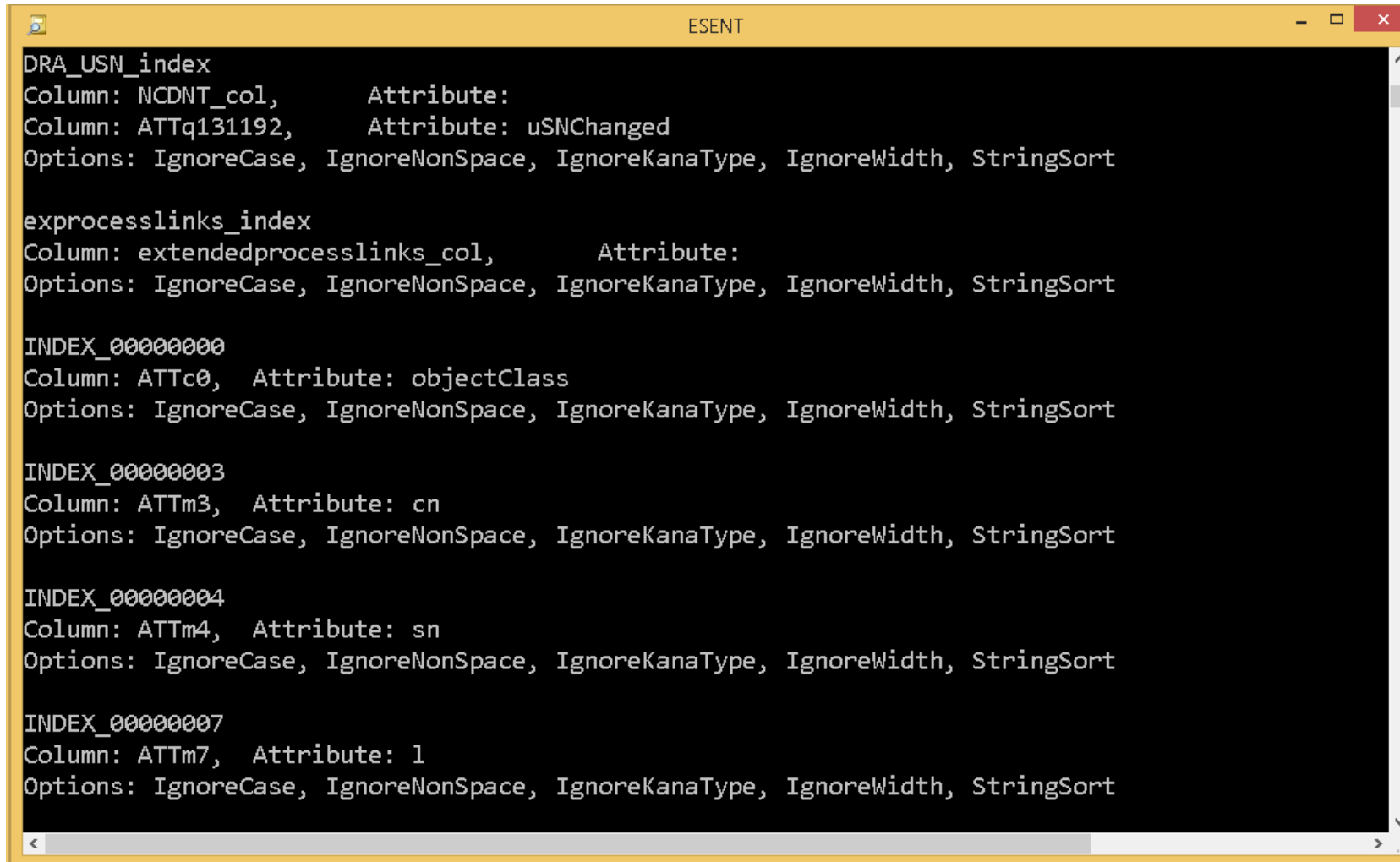
NTDS (520) NTDSA: Online defragmentation is beginning a full pass on database 'C:\Windows\NTDS\ntds.dit'.

Log Name: Directory Service
Source: NTDS ISAM
Event ID: 700
Level: Information
User: N/A
OpCode:
More Information: [Event Log Online Help](#)

Logged: 5/21/2015 2:56:17 AM
Task Category: Online Defragmentation
Keywords: Classic
Computer: LON-DC1.Adatum.com

Copy
Close

Index-Attribute Mapping



```
ESENT
DRA_USN_index
Column: NCDNT_col,      Attribute:
Column: ATTq131192,     Attribute: uSNChanged
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort

exprocesslinks_index
Column: extendedprocesslinks_col,      Attribute:
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort

INDEX_00000000
Column: ATTc0,  Attribute: objectClass
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort

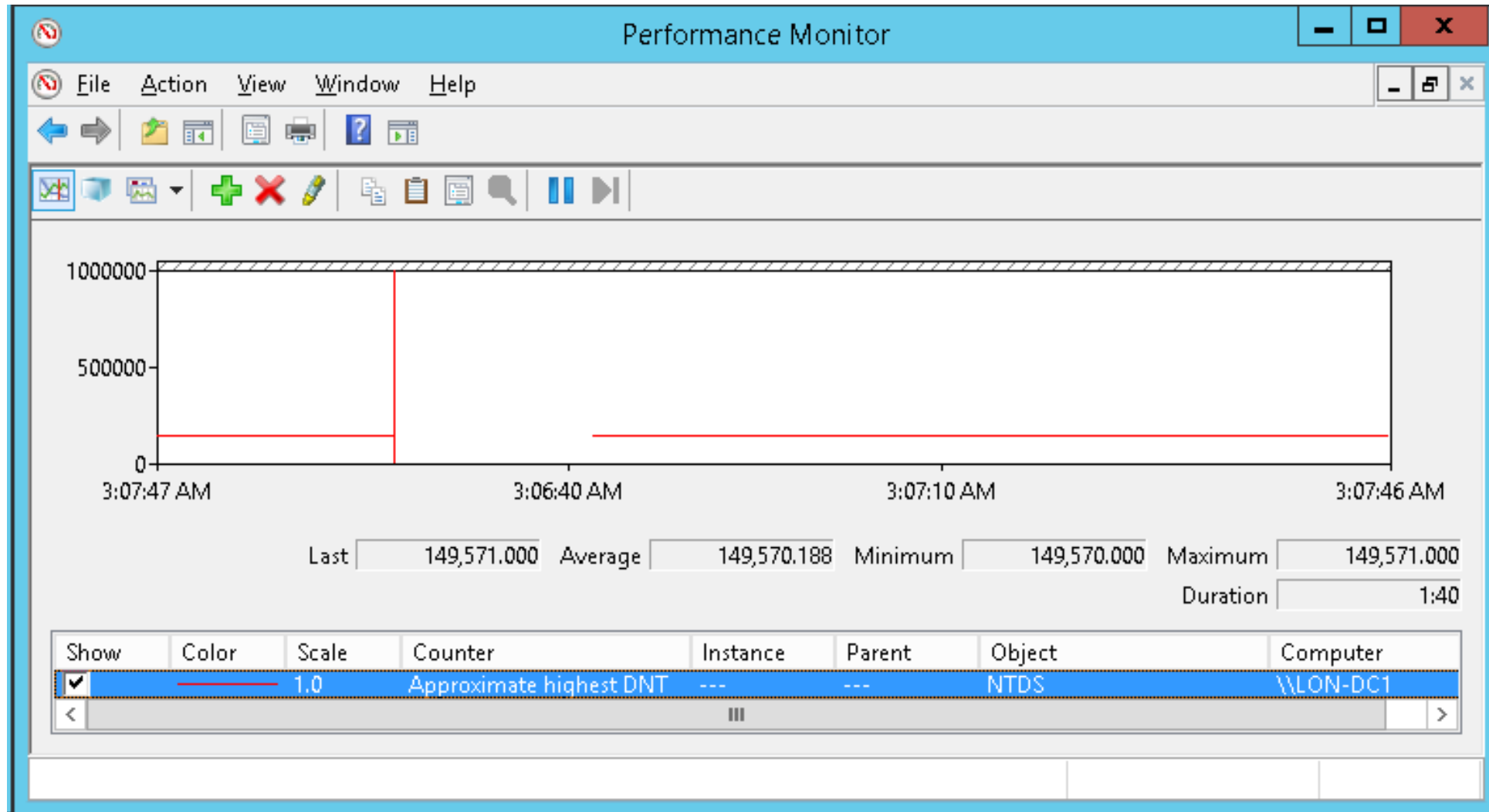
INDEX_00000003
Column: ATTm3,  Attribute: cn
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort

INDEX_00000004
Column: ATTm4,  Attribute: sn
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort

INDEX_00000007
Column: ATTm7,  Attribute: l
Options: IgnoreCase, IgnoreNonSpace, IgnoreKanaType, IgnoreWidth, StringSort
```

DEMO

Highest DNT (2012+)

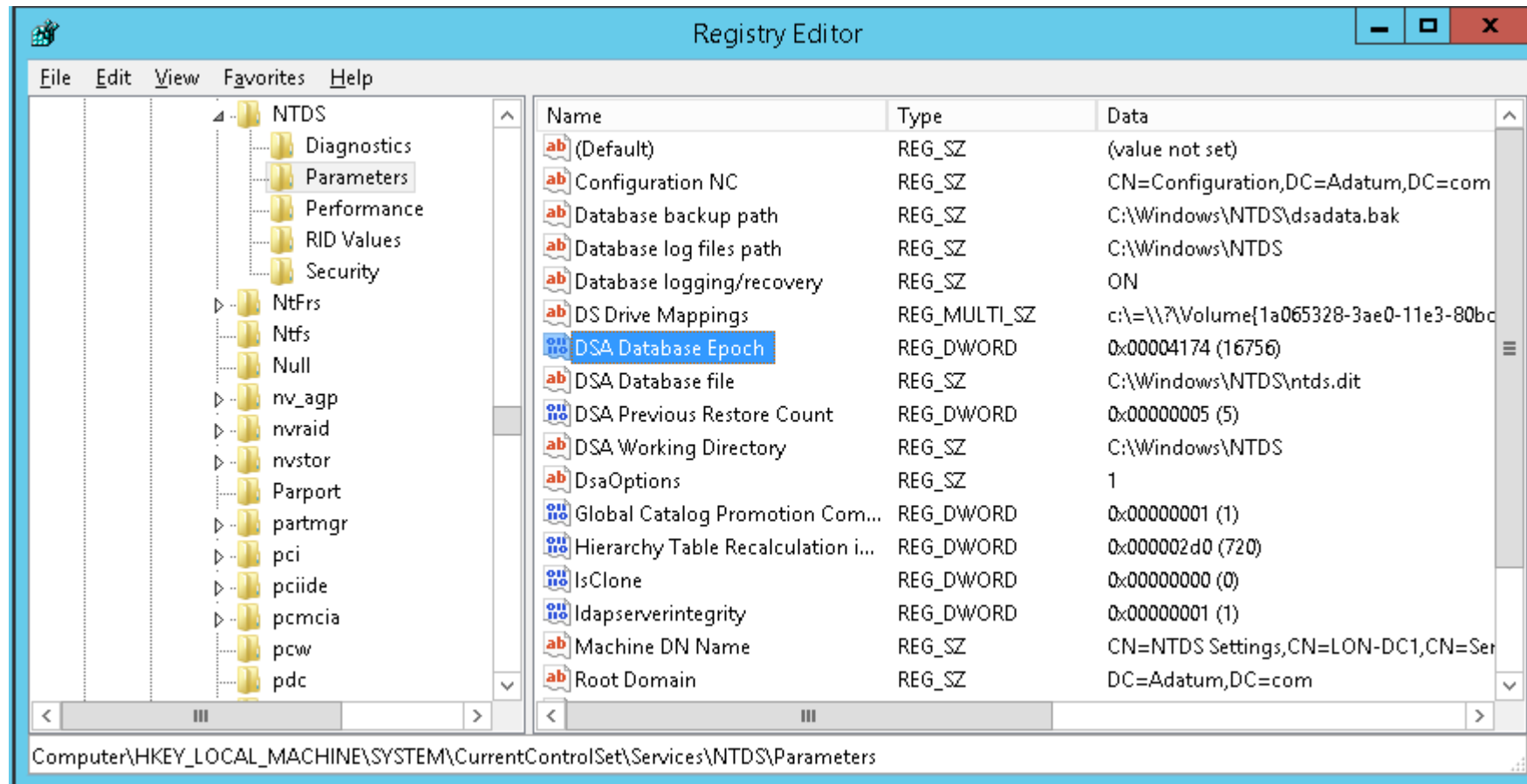


Database Integrity Checks

- Header – DB file status
- Checkpoint – Checkpoint file status
- Checksum – Page checksum test
- Recover – Copy committed transactions from log to DB
- Integrity – Binary level checks
- Semantic Database Analysis – Indexes, Security Descriptors, Links,...

DEMO

Database Epoch



DEMO



Gold partner:



Generální partner:



How Active Directory Database Really Works

Michael Grafnetter
www.dsinternals.com

18. – 21. května 2015

Tech·Ed
DevCon 