# Data Insight Self Paced Lab

# **Objective**:

This lab is designed to introduce the high-level use cases within the Data Insight GUI. The Workspace provides an interactive view of the current environment. The reporting engine offers a variety of report packages designed to provide summary and detail data globally over various time periods.

There are no lab modules offered around the alerting section as this data required ongoing audit activity. This area offers event alerting and anomaly detection capabilities based on statistical deviance from calculated baselines.

# About the environment:

VM Server Name Matrix

Credentials Username: Administrator Password: password Domain: matrix

Once the desktop has loaded, the Data Insight console can be accessed through Internet Explorer, or Chrome. The credentials to log in are the administrator credentials used for VM login. To Log In, Click on the Data Insight Console icon on the desktop or open a browser and navigate to htts://localhost. If login is not working, ensure that cookies are enabled.

Lab Contents

ABOUT THE ENVIRONMENT:	1
DATA INSIGHT USE CASE TEST SCENARIOS	2
DATA OWNERSHIP	2
STALE DATA USE CASES	7
CHARGEBACK ENABLEMENT USE CASES	9
ILM USE CASES	11
DATA FORENSICS USE CASES	13
DATA PROTECTION USE CASES	17

Data Insight Use Case Test Scenarios

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

# Data Ownership

Identify users, notify them, and clean up exposed data

#### Questions:

- Who is the inferred or calculated owner of a file or folder?
- Who else is using the same resources?
- What types of operations are being performed on this resource?
- How confident are we in the ownership calculation?
- Where are the most accesses occurring that impact this calculation?

The main idea of this use case is to be able to illustrate the person who is the most likely data owner based on usage and usage patterns.

#### Navigate to workspace / folders

Select a registered filer and drill down in the tree.

Pick a file or folder of interest. (Must have activity; pick something higher in the tree to increase odds of meaningful access history)

A good target folder for this lab is <u>\\Singularity\DataNTAPCIFS</u>. Click the + sign next to singularity, and the click on the DataNTAPCIFS folder. The overview should load in the main portion of the screen.

Note folder overview. This shows basic data on size, and access information. Also lists files in the parent folder

Workspace	Dirts Settings	
Folder & Users & Groups Filer Hierarchy O DFS Hierarch Search Shares	\\Acmefiler\Acmeshare\Finance	
<b>⊞</b> ∭ 10.209.89.3	📄 Overview 🔓 User Activity 🛱 Folder Activity 🕹 Permissions	Audit Logs
<ul> <li>         · ∃         · ■         · ■         · ■</li></ul>	Details Size: 11.71 MB Created on: 2010-02-07	Files
∃       Finance         ∃       HR         ∃       Legal         ∃       Marketing         ∃       Sales         ∃       Bublin-Ireland	Access Information Last Accessed by: Andy Murray Last Accessed on: 2010-03-10 Last Modified by: Andy Murray Last Modified on: 2010-03-10	

Next click on User Activity

This screen gives you an activity overview with top users, and the inferred data owner. This screen also illustrates if there's a high confidence in the inferred data owner based on the large proportions of accesses by the user.

Also note the balance between reads and writes indicating interactivity with this file.

Workspace Repo	rts Settings
Folder & Users & Groups	\\Acmefiler\Acmeshare\Finance
• Filer Hierarchy O DFS Hierarch	Finance 🛞
Search Shares ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	📄 Overview 🛛 🚨 User Activity 🗔 Folder Activity 🔒 Permissions 🔲 Audit Logs
	Summary Active Users Inactive Users
Acmefiler	
Acmeshare	Time Filter From: 2010-01-20 To: 2010-07-20 Read Write GO
Engineering     Executives	Folder Information
E Finance	Created hu 🖗 Administrators on 2010.02.07
🗄 🫅 HR	
🗄 🚞 Legal	Inferred Data Owner
🗄 🚞 Marketing	Name : SAndy Murray Last Access: 2010-03-10 Access counts: Read: 229   Write: 261   Total: 490
🗄 🚞 Sales	
🗄 🧱 Dublin-Ireland	Graphical View
1 Image: MountainView	
🗄 🧱 OrgFiler	Access data for top 5 users
🗄 🧱 Pune-India	
Singapore-APAC	
SymantecFiler	
⊞ 👹 Tokyo-Japan	Andy Murray, 490 ¬
⊞ <b>∰</b> f11	
∃ 📑 legal	
⊞ ∰ lgl1	
⊞ 😅 newfl1	Ann White, 114 Abey Low, 110
	Shane Rose, 111 Antonio Karosen, 111

Next select Active Users sub tab.

This gives you a larger user list with a quick glance of access proportions in relation to the total count, and by reads and writes.

Workspace Repo	orts Settings					About   Help   Logout
Folder & Users & Groups     Filer Hierarchy O DFS Hierarch     Search Shares     # 10.209.89.3     # 10.209.89.4     # Acmentier	IVAcmefiler/Acmeshare/Finance       Finance       Pinance       Overview       User Activity       Summary       Active Users       Time Filter       From:       2010-01-20	Folder Activity	Permission	ons [ Au	dit Logs	
Engineering	Active Users					
Executives	User Name		Acces	s Count		Read Count Write Count
🗄 🛅 Finance		Read	Write	Other	Total	
HR	S Abey Low	55	55	0	110	
Legal	S Alfred C	39	47	0	86	
B Sales	S Amalia David	41	49	0	90	
🗄 🧱 Dublin-Ireland	Andy Murray	229	261	0	490	
H MountainView	Ann White	60	54	0	114	
🗄 🧱 OrgFiler	Antonio Karoson	55	56	0	111	
Pune-India	Koth But	49	45	0	94	
Singapore-APAC		53	51	0	104	
Symantechiler     Symantechiler		48	53	0	101	
	Pamela Taylor	40	39	0	00	
🗄 🧱 legal	Series Clinton	54	36	0	52	
🗄 🎆 lgl1	Patrick Moncada	47	39	0	86	
🗄 🧱 newfl1	Peter Wortmann	50	46	0	96	
	Shane Rose	56	55	0	111	
	S Tracy Williams	64	46	0	110	

Next click on Folder Activity, then select by subfolders and files.

This screen gives you a breakdown by subfolder. You can get a sense of what data is dispersed in this directory, and how the accesses are spread across.

Workspace Repo	⊢ ⊂ <i>ς</i> orts Settings				
<b>Folder</b> SUsers SGroups	\\Acmefiler\Acmeshare\Finance				
• Filer Hierarchy O DFS Hierarch					
Search Charge	Finance 🙁				
∃ ■ 10.209.89.3	📄 Overview 🔒 User Activity 🛅 Folder Activity	y 👵 Permissi	ons 📃 Audit	Logs	
10.209.89.4	Pu Time - Ru Cubfolders & Elles - Leasting Cubfolders		_		
Acmefiler	by time by subfolders & Files Inactive Subfolders				
Acmeshare	Time Filter From: 2010-01-20 📴 To: 2010-07-	20 🖸 GO			
🗉 🚞 Engineering	Folder Name: Finance				
Executives					
🗄 🚞 Finance	Iotal Access Count:	(	J   1/95) <b>1/95</b>		
🗉 🚞 HR	Read:	(0   900) <b>900</b>			
🖽 🚞 Legal	Write:	(0   895) <b>895</b>			
🗄 🚞 Marketing	Other [Create, Delete, Rename]: (0   0) 0				
🗄 🚞 Sales					
🗄 🧱 Dublin-Ireland	Folder Access Count     SubFolder Access Count				
HountainView					
🗄 🧱 OrgFiler	Sub Folder and File Activity				
🗄 🚟 Pune-India	File/Folder Name		Acce	ss Count	
Singapore-APAC		Read	Write	Other	Total
SymantecFiler	CLAIMS\$	0	0	0	0
🗄 🧱 Tokyo-Japan	EXPENSES	0	0	0	0
🛨 🧱 fl1		0	0	0	0
± 🎆 legal	ORDERS(PROC)	0	0	0	0
🛨 🧱 lgl1	PAYROLL	0	0	0	0
🗄 🚟 newfl1	Quarter1	243	223	0	466
	Quarter2	226	212	0	438
	Quarter3	207	227	0	434
	Quarter4	224	233	0	457

Now that we have gotten more data about the owner, we can go back to the user activity screen and right click on the Data Owner's name.

We are given the option of getting an overview, global activity, global permissions, and raw access history from the audit logs.

Finance ×			
📄 Overview 🤱	User Activity	Gilder Activity	Permissions
Summary Active	Users   Inactive User	s	
Time Filter	From: 2010-01-20	To: 2010-07-20	🖪 🗹 Read 🗹 W
Folder Information			
Created by: 🚨 A	dministrators on 20	010-02-07	Last Modified t
Inferred Data Owne	r		
Name : 🚨 Andy	Overview	*ccess: 2010-03-10	Access counts: R
Graphical View	Activity		
	Permissions		
	Audit Logs	a for top 5 users	

Clicking on overview will give you details on the Data Owner including security groups, and any custom AD attributes that have been configured to be gathered.

This info is useful in determining some details about any such as dept, job function, etc.

& And	dy Murray 🙁	Finance					
Ov	erview	Activity	👵 Permissi	ons	Audit Logs		
							]
	Login Nam	e: Andy Murray(	@tulip.matrixad	.local			
	Display Na	me: Andy Murra	Y				
	First Name	: Andy					
	Last Name	: Murray					
	510: 5-1-5	-21-617441397	7-4198358099-3	2716562547	-1130		
Membe	sid: <b>5-1-</b>	-21-61/44139/	7-4198358099-3	2716562547	-1130	Attributes	
Member Member	r of ministrator	s@tulip.matrix	r-4198358099-:	2716562547	-1130	Attributes	
Member Adr Doi	ministrator	s@tulip.matrix ns@tulip.matri	ad.local	2716562547	-1130	Attributes	
Member Pada Dor Dor	ministrator main Admi main Users	s@tulip.matrix ns@tulip.matri ;@tulip.matrix	xad.local ixad.local ad.local	2716562547	-1130	Attributes	
Member Adr Doi Doi Go fus	ministrator main Admi main Users er@tulip.m	s@tulip.matrix ns@tulip.matri @tulip.matrix atrixad.local	ad.local ixad.local ixad.local ad.local	2716562547	-1130	Attributes	
Member State Dor State State State Manual Member Manual Member Manual Member Manual Member Member Member Member Member Member Member Manual Member Me	r of main Admi main Users er@tulip.m egal@tulip.	s@tulip.matrix ns@tulip.matrix @tulip.matrix atrixad.local matrixad.local	ad.local ixad.local ixad.local ad.local	2716562547	-1130	Attributes	
Member Market Ma	r of ministrator main Admi main Users er@tulip.m egal@tulip. itrix@tulip. ma@tulip.m	s@tulip.matrix ns@tulip.matrix @tulip.matrix atrixad.local matrixad.local matrixad.local	ad.local ixad.local ixad.local ad.local	2716562547	-1130	Attributes	
Member Adr Dol Dol Dol G G G G G G G G G G G G G G G G G G G	r of ministrator main Admi main Users er@tulip.m egal@tulip.m a@tulip.m ers@tulip.m	s@tulip.matrix ns@tulip.matrix @tulip.matrix atrixad.local matrixad.local matrixad.local atrixad.local atrixad.local	xad.local ixad.local ad.local ad.local	2716562547	-1130	Attributes	

You can also click on the Activity tab to get a view of global activity; as a time series, or by folder.





S Andy Murray E Finance										
📄 Overview 🔲 Activity 🔱 Permissions 🔲 Audit Logs										
By Time By Folders										
Time Filter From: 2010-01-20  To: 2010-07-20  GO										
Folders		Acce	ss Count							
	READ	WRITE	OTHER	TOTAL						
E Diagonal Acmeshare										
Engineering	287	283	0	570						
	51	55	0	106						
Command Central Storage	75	55	0	130						
Symantec Data Loss Prevention	47	46	0	93						
E Cluster Server	56	51	0	107						
🗄 🦳 Veritas File System	58	76	0	134						
E Finance	229	261	0	490						
🗄 🛅 HR	323	342	0	665						
🗄 🛅 Legal	395	352	0	747						
🗄 📃 legal1										
🗄 📃 legal2										
🗄 😓 legal3										

#### **Stale Data Use Cases**

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

#### Stale Data

Evaluate age of data and understand potential areas for remediation. Improve storage utilization through file management.

Questions

- How old are all the files or folders owned by a certain user or group?
- How much can be saved with stale file remediation techniques?

The main idea of this use case is to try to get an overview of the age of your data, to identify stale files and folders for remediation.

Navigate to reports / Inactivity Reports Select "Inactive Data by Owner" report Choose Create Report Here you can choose the output of the report, when it's run, and what areas of the NAS environment it looks at. To ensure data in the report, select an entire NAS device and set the "Inactive Time Period" to "1 Month" and "Limit Number of Records" to 25

Filer Hierarchy			Selected resources
Search Shares	9		singularity
🖄 🎒 Enterprise	2		
± ﷺ singularity			
😐 📟 superluminal.hrocclab.local			
		<	
		>>	
		<<	
Filter filers	Q		
🚺 🖣 Page 1 of 1 🕨 🕅 🧬			
nactive Time Period			
Show files which are inactive for more th	ian		
1 month 💌			
imit Number of Records			
Select number of records to be displayed	d in the details section	for e	ach selected path
25 👻			

test

Select "Save and Run" to see the new report listed. After successful completion, open the report in the preferred format (CSV, HTML, PDF)

1	Report: Inactive Data by Owner							
	Use this report to get a summary of space used by files or folders, so							
	Sample Outputs: MTML							
List of R	eports							
🖓 Creat	te Report 📀 Refresh 🛛 📃 Auto Refre	sh (10 seconds re	efresh interval)					
Report Na	ame	Last Successfu	Last Run Status					

The top area of the report calls out all owners of files considered stale based on your report settings. The number of files as well as what % of all files owned by the user are considered stale.

🟩 🔁 😫

IN PROGRESS

User	User Account	Size (MB)	•	% of Size	File Count	BU Name	Custodian
Administrators	Administrators	9273	31	7.87	2393		
Total		9273	31		2393		

The remainder of the report calls out individual files, locations, and dates of modification and access.

User	Data Owner Policy	File Server	Share Name	File (Path)	Size (MB)	Last Modified	Last Accessed				
Administrators (Administrators)	Administrators (Administrators)										
	Parent Owner	singularity	AppleBackup	\\singularity\AppleBackup\Data Insight Use Case Test Scenarios.docx	1.90	Oct 25, 2010 12:54 AM	Nov 12, 2010 6:13 PM				
	Parent Owner	singularity	DataNTAPCIFS	\\singularity\DataNTAPCIFS\vms\DataInsightx64\ DataInsightx64.vmem	1024.00	Oct 26, 2010 2:23 PM	Nov 12, 2010 12: 08 PM				
	Parent Owner	singularity	DataNTAPCIFS	\\singularity\DataNTAPCIFS\vms\DataInsightx64\ DataInsightx64.vmss	19.71	Oct 26, 2010 2:31 PM	Nov 12, 2010 12: 42 PM				
	Parent Owner	singularity	SoftwareNTAPCIFS	\\singularity\SoftwareNTAPCIFS\Windows ISOs\ SW_DVD5_Windows_Svr_DC_EE_SE_Web_2008R -bit_English_X15-59754.ISO	2857.97	Feb 1, 2010 11:27 PM	Apr 11, 2010 2:13 AM				

# **Chargeback Enablement Use Cases**

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

#### Enable Chargeback

Evaluated size of files owned by particular users and groups. Improve storage utilization through accountability

Questions

- What users and groups are using the most storage for unstructured data?
- How much could each user or group pay for access to that storage?

The main idea of this use case is to try to get an overview of the sizes of your unstructured data files, and assign ownership for accountability and chargeback

Navigate to reports / Utilization Reports Select "Storage by file group and owner" report Choose Create Report Here you can choose the output of the report, when it's run, and what areas of the NAS environment it looks at. To ensure data in the report, select an entire NAS device and "Specify duration" to the length of time DataInsight has been running.

"Limit Number of Records" to 25

Filer Hierarchy      DFS Hierarch	chy			Selected resources	
Search Shares		Q		📟 singularity	
Enterprise		~			
🗄 🚟 singularity					
😟 🚟 superluminal.hrocclab.local			> < *		
Filter filers		2			
14 4   Dana 1 of 1   b   1 🔊					
Time Filter					
Specify Duration	Specify date r	ange			
Time Duration:	Last:		D	AYS 👻	
Limit Number of Records					
Select number of records to be di	splayed in the deta	ils section fo	or ea	ach selected pat	h

Select "Save and Run" to see the new report listed. After successful completion, open the report in the preferred format (CSV, HTML, PDF)



The report can be broken down by user, filetype, and any Active Directory attributes like Business Unit:

User	User Account	File Group Type	Space Used (MB)	File Count	BU Name	Custodian
John Dodds	john_dodds@ hrocclab.local	All Files	108488.35	937	SAMG	
Administrator s	Administrator s	All Files	7734.18	2300		
Ryan Jancaitis	ryan_jancaiti s@hrocclab.l ocal	All Files	0.43	3	SAMG	
Creator Owner	Creator Owner	All Files	0.01	1		
John D'Alto	john_dalto@h rocclab.local	All Files	0.01	3	SAMG	
Tom Harwood	tom_harwood @hrocclab.lo cal	All Files	0.01	2	SAMG	

#### File usage by user and type of file:

User	Туре	Data Owner Policy	File Server	File (Path)	Size (MB)	Access Count	
John Dodds (john_dodds@hrocclab. local)							
	VMWare Server Files	Read+Write Count	singularity	\\singularity\DataNTAPCIFS\vms\Enforcedemo_V11\ Enforcedemo_V11-Snapshot1.vmem	3096.00	28	
	VMWare Server Files	Read+Write Count	singularity	\\singularity\DataNTAPCIFS\vms\Enforcedemo_V11\ Enforcedemo_V11-Snapshot2.vmsn	135.78	2	
	VMWare Server Files	Read+Write Count	singularity	\\singularity\DataNTAPCIFS\vms\Enforcedemo_V11\ Enforcedemo_V11-Snapshot1.vmsn	134.35	2	
	VMWare Server Files	Read+Write Count	singularity	\\singularity\DataNTAPCIFS\vms\Enforcedemo_V11\ Enforcedemo_V11.vmx	0.01	1	
	VMWare Server Files	Read+Write Count	singularity	\\singularity\DataNTAPCIFS\vms\Netapp_Filer (v11)\ Netapp_Filer (v11).vmx	0.01	3	

Exporting and manipulating this data through spreadsheets allows complete flexibility in chargeback reports.

#### **ILM Use Cases**

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

#### ILM: Data Aging

Evaluated age of files owned by particular users and groups. Improve storage utilization through accountability

Questions

- What users and groups are using the most storage for unstructured data?
- Are the proper users and groups keeping the right files for extended periods of time?

The main idea of this use case is to try to get an overview of the age of your unstructured data files, and assign ownership for remediation.

Navigate to reports / Inactivity Reports

Select "Data Aging" report

Choose Create Report

Here you can choose the output of the report, when it's run, and what areas of the NAS environment it looks at.

To ensure data in the report, select an entire NAS device and "Limit Number of Records" to 25

Select the files and folders by dragging them from left pane to the right pane. Double click on a folder

Filer Hierarchy      O DFS Hierarchy	Selected resources
Search Shares	📟 singularity
Z Enterprise	
🕀 🚟 singularity	
superluminal.hrocclab.local	
Filter filers	
14 4 Dana 1 nf 1 b bil 2	
Limit Number of Records	
Select number of records to be displayed in the details section for 25	each selected path

Select "Save and Run" to see the new report listed. After successful completion, open the report in the preferred format (CSV, HTML, PDF)

Report: **Data Aging** Use this report to get a summary of space used by files or folders v

Sample Outputs: MITML

List of Reports			
中 Create Report 📀 Refresh	Auto Refres	h (10 seconds re	efresh interval)
Report Name		Last Successfu	Last Run Status
Sample Data Aging		🟩 🔁 鸖	IN PROGRESS

This report is broken down into aging "buckets" of last access to quickly identify count and size of all files.



This is broken down further into NAS device, share, and eventually file.

#### Overview of aging per NAS device.

Age	File Server	Size (MB)	File Count
0-3 Months			
	singularity	3714.10	2327
	superluminal.hrocclab.local	1538.70	145
6-9 Months			
	singularity	2989.17	2
Older than 12 Months			
	singularity	0.01	17
	superluminal.hrocclab.local	0.00	54

# Overview of aging per NAS Share and device

Age	File Server	Share Name	Size (MB)	File Count
0-3 Months				
	singularity	SoftwareNTAPCIFS	3710.71	2134
	singularity	DataNTAPCIFS	3.39	193
	superluminal.hrocclab.local	SuperluminalShare	1538.70	145
6-9 Months				
	singularity	SoftwareNTAPCIES	2989.17	2
Older than 12 Months				
	singularity	HOME	0.01	1
	singularity	DataNTAPCIES	0.00	16
	superluminal.hrocclab.local	SuperluminalShare	0.00	54

# Overview of aging per share and file

Age	Filer Name	Share Name	File (Path)	Space Used (MB) Last Accessed
Older than 12 Months				
	singularity	DataNTAPCIFS	\\singularity\DataNTAPCIFS\DILoad\ORDERS(PROC)\2007\Feb\ order8_20.txt	0.00 Jan 1, 1970 12:00 AM
	singularity	DataNTAPCIFS	\\singularity\DataNTAPCIFS\DILoad\CLAIMS\$\2008\ClaimsJan2_17. txt	0.00 Jan 1, 1970 12:00 AM
	singularity	DataNTAPCIFS	\\singularity\DataNTAPCIFS\DILoad\CLAIMS\$\2008\ClaimsJan2_18. txt	0.00 Jan 1, 1970 12:00 AM

#### **Data Forensics Use Cases**

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

#### Data Forensics Investigate and solve data breaches; monitor sensitive data usage

Questions

- Who as been touching sensitive files?
- How did this person get access to a file?
- Who wrote to a file and potential was responsible for the inclusion of sensitive information?
- What has a person been up to lately?
- What time an ip has a person of interest been using to get to a file?

The main idea of this use case is to try to get a root cause for the introduction of sensitive data, or the scope of a potential data leak.

Navigate to workspace / folders

Select a registered filer and drill down in the tree.

Pick a file or folder of interest. (Must have activity; pick something higher in the tree to increase odds of meaningful access history)

You can continue to use the same <u>\\Singularity\DataNTAPCIFS</u> share that was used for the previous Data Ownership lab module.

Overview shows the last people to access and modify the target file.

Folder 🖁 Users 🖓 Groups	\\Acmefiler\Acmeshare\Legal\Patent\Patent-1802929329.pdf
Filer Hierarchy     O DFS Hierarch	Patent-18029 🗵
Search Shares	📄 Overview 🔚 User Activity 🔚 File Activity 🐍 Permissions 🔲 Audit Logs
⊞ 🧱 10.209.89.4 ⊒ 🧱 Acmefiler	Details
🖃 딇 Acmeshare	Size: 0 bytes
🗄 🚞 Engineering	Created on: 2009-07-31
Executives	
🗄 🚞 Finance	
🗄 🚞 HR	Access Information
🖃 🚞 Legal	Last Accessed by: 🕹 Pamela Taylor
H 🚞 2008	Last Accessed on: 2010-03-10
🗄 🚞 2009	Last Modified by: 🖏 Ann White
🖃 🚞 IDF	Last Modified on: 2010-03-09
🗆 🦳 Patent	
Marketing	
🗄 🚞 Sales	

Click on user activity to see the top users of this file as well as the inferred data owner. The inferred data owner would be the primary contact for remediation, or the best person to notify if there's a suspected issue, or incident created on this file.

You can use this screen to also potentially identify any users that have a suspiciously large amount of file accesses, or people that possibly should be using this resource at a high level.



Click on active users to get more detail on usage, as well as an overview of the file's most active writers.

Patent-18029					
📄 Overview 🛛 🔓 User Activity 💼	File Activity	Permissions	🔳 Audit L	ogs	
Summary Active Users Inactive Users					
Time Filter From: 2010-01-20	To: 2010-07-20	GO			
Active Users					
User Name		Access	Count		Read Count Write Count
	Read	Write	Other	Total	
岛 Abey Low	7	2	0	9	
Salfred C	8	5	0	13	
🔓 Amalia David	6	5	0	11	
🔓 Andy Murray	21	22	0	43	
🚨 Ann White	4	6	0	10	
🚨 Antonio Karosen	4	4	0	8	
S Archie Andrews	3	3	0	6	
🔓 Keith Burt	8	6	0	14	
🔓 Nichol Habel	2	4	0	6	
🔓 Pamela Taylor	4	7	0	11	
Paris Clinton	3	3	0	6	
Patrick Moncada	6	4	0	10	
🔓 Peter Wortmann	7	4	0	11	
🔓 Shane Rose	7	4	0	11	
🔓 Tracy Williams	4	3	0	7	

At this point, we have a good idea of people that have been using this file; we want to know who's touched it recently. If the data breach was in the last 24 hours we can modify the Time filer of the above screen to see who's written or read this file.

Next we are interested in the raw activities that have happened on this file. We may have a person or time of interest, click on audit lots to see the raw access history and choose the appropriate time frame. We can also filter this list by user, path, ip, or type of access. If I wanted to see all writes in a certain time window by a user, this is possible with the filters. We are presented with a time series access heat map as well as the raw events that can pinpoint the suspicious activity.

Patent-18	029 ×																											
Overview	/ 🔓 U	ser Activ	ity			File	e Acti	vity	,	8	P	Perm	issi	ons			Au	ıdit	Log	s								
Filtor	From: 2010	0-02-01				ОТО	: 201	0-0	7-20	1		E	•															60
riter	User: Ente	r user@d	omai	n		Path	:							IP:							\cce	ess /	All Ac	ces	s	~		30
Access Patter	rn Map																											8
			Feb	-10				Mar	-10			Apr-	10			Мау	/-10				Jun	-10			Jul-	10		0
			01	07	14	21	28	07	14	21	28	04	11	18	25	02	09	16	23	30	06	13	20	27	04	11	18	
_		r																										
Archie A	ndrews	w																										
		0 r								_																		_
Andy Mu	irrav	w																										
		o																										
		r																										Ŧ
Page	ellof1 ▶		,																							Di	splayin	g 1 - 15 of 15
User Name			File	Name	e				Path					Access 1 File 1P				Co			Start Time							
🔓 Pamela T	Taylor		Þ	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	lf			REA	D	pdf	10.	209	.89.18	3	1	2010-03-
Salfred C			Ta r	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	lf			REA	D	pdf	10.	209	.89.16	6	1	2010-03-
Salfred C			Þ	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	lf			REA	D	pdf	10.	209	.89.11		1	2010-03-
Sandy Mu	Irray		Þ	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	lf			REA	D	pdf	10.	209	.89.4		1	2010-03-
S Ann Whi	ite		Þ	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	If			WRIT	ΓE	pdf	10.	209	.89.7		1	2010-03-
B Patrick N	Moncada		Þ	Paten	t-18	0292	9329.p	odf	\Le	gal\P	aten	t\Pate	ent-1	8029	2932	29.pd	lf			REA	D	pdf	10.	209	.89.10	)	1	2010-03-
0																					$\supset$							)4 +

You can select permissions and evaluate the raw permissions at the share and file level to determine if the ACL is valid. You can also start here to see where the suspicious user got access to this file. You can right click to see memberships.

It's possible for an invalid explicit ACE to be applied to a file or folder, or for a user to be erroneously assigned to an AD group.

Legal Patent-1802925 🙁											
📄 Overview 🛛 🔓 User Activity 💼 Folder Activity	&	Permi	ssions		Audit Logs						
● Effective Rights ○ File System Access Control List ○ Share	e level	permi	ssions								
User/UserGroup	Permission Advanced permission										
	FULL	READ	WRITE	MODIFY	READ & EXEC	LIST	SPECIAL				
B gLegal@tulin_matrixad.local		~	~	×	×	~	×				
Admir Apermissions cad.local	1	× .	× .	×	×	1	×				
Group Members											

#### **Data Protection Use Cases**

Listing of main Data Insight Use Cases, and methods to validate data and show functionality.

**Data Protection** 

Evaluate access and understand potential access breaches and evaluate ACL changes. Improve security though tighter security.

Questions

- How did a person or group inherit access to a folder or file
- At what point does inheritance break and the ACL tree change?
- How many have access, but may not need it based on inactivity?

The main idea of this use case is to try to get a root cause for the introduction of sensitive data, or the scope of a potential data leak.

Navigate to workspace / folders

Select a registered filer and drill down in the tree.

Pick a file or folder of interest. (Must have activity; pick something higher in the tree to increase odds of meaningful access history)

You can continue to use the same <u>\\Singularity\DataNTAPCIFS</u> share that was used for the previous lab module.

Overview shows the last people to access and modify the target file.

C	Legal	
	Overview 🔓 User Activity 🗟 Folder Activity 😓 Permissions 目	Audit Logs
	Details	Files
	Size: 3.08 MB	
	Created on: 2010-02-07	
	Access Information	
	Last Accessed by: 🖧 Pamela Taylor	
	Last Accessed on: 2010-03-10	
	Last Modified by: 岛 Amalia David	
	Last Modified on: 2010-03-10	

Next Click on Permissions. This gives us an effective permissions view that includes folder and share level ACL calculations.

Legal R Patent-1802925 R										
🔋 Overview 📲 User Activity 🔚 Folder Activity 🔒 Permissions 🔲 Audit Logs										
● Effective Rights ○ File System Access Control List ○ Share level permissions										
User/UserGroup				Perm	ission			Advanced permissions		
User/UserGroup	FULL	READ	WRITE	Perm	iission READ & EXEC	LIST	SPECIAL	Advanced permissions		
User/UserGroup	FULL	READ	WRITE	Perm MODIFY	iission READ & EXEC	LIST	SPECIAL	Advanced permissions		

For a raw ACE list (ntfs style permissions) with inheritance, click on radio button next to File System Access Control List. Note the inheritance data. No inheritance means a direct ACE on that Object. If you are using a share such as <u>\\Singularity\DataNTAPCIFS</u>, there should be no inheritance as this is the root of the share. To see inheritance, navigate to a sub folder such as DILoad.

📄 Overview 🛛 🔓 User Activ	vity		Folde	r Activity	/ 🐣 Pe	rmis	sions	Audit Logs		
O Effective Rights 💿 File System Access Control List 🛛 Share level permissions										
User/UserGroup		Permission						Inherited From	Applies To	
	FULL	READ	WRITE	MODIFY	READ & EXEC	LIST	SPECIAL			
gLegal@tulip.matrixad.loc			<b>N</b>	<b>%</b>	<b>F</b>				This folder, Subfolders, files	
Administrator@tulip.matri:	<b>.</b>	Ē	<b>S</b>	1	Ŧ			<b>₽</b> 1	This folder, Subfolders, files	

Next evaluate the permissions granted at the share level. Effective access is calculated by evaluating NTFS style ACL's and masking it with the restrictions at the share point.

ivity 🛅	Folder Activity	Permissions	Audit Logs							
○ Effective Rights ○ File System Access Control List ③ Share level permissions										
User/UserGroup Permission Inherited From										
FULL READ	WRITE MODIFY REA	D&EXEC LIST SPECIAL								
<b>S</b>			lisingularity.hrocclab.local/Software	This folder						
	ivity stem Access FULL READ	ivity 🕞 Folder Activity stem Access Control List  Sha Permission FULL READ WRITE MODIFY REA	ivity Folder Activity Permissions stem Access Control List Share level permissions Permission FULL READ WRITE MODIFY READ & EXEC LIST SPECIAL	ivity Folder Activity Permissions Audit Logs stem Access Control List Share level permissions Permission FULL READ WRITE MODIFY READ & EXEC LIST SPECIAL						

Next we can attempt to make recommendations on tightening up the access list by seeing who has not been using their access to this folder. Click on User Activity, and then select inactive users.

In a real world environment, there is likely to be many users that aren't using the permissions granted to a share. Larger numbers of inactive users may indicate an overly permissive share.

S Administrator@ 🖲 🔁 Acmeshare 💌	🛅 Legal 🛞								
📄 Overview 🔓 User Activity	Gilder Activity	Permissions	Audit Logs						
Summary   Active Users   Inactive Use	ers								
Time Filter From: 2010-01-21	To: 2010-07-21	GO							
User									
Administrator@tulip.matrixad.local									

We can then determine how a user got access to this folder by right clicking on the user and selecting permissions.

🔱 Administrator@ 🗵	Acmeshare X Legal X
📄 Overview 🛔	User Activity 🕞 Folder Activity 🐍 Permissions 📃 Audit Logs
Summary Active	Users Inactive Users
Time Filter	From: 2010-01-21 To: 2010-07-21 GO
User	
S Administrator@	atulin matrixed local
	Overview
	Activity
	a Permissions
	Audit Logs

Once on the user's global permissions screen, we can scroll to the file and share in question. This view will show direct ACLs as well as permissions that have been inherited by virtue of group membership.

Instances such as the Everyone group can be a potentially useful red flag.

It's also possible that the permissions are valid, but there are people that are erroneously in groups that have valid access. This would pinpoint the error in membership.

8	各 Administrator 🛞 🔂 Acmeshare 🛞 🔂 Legal											
	Overview 🔲 A	ctivity	8	Perm	nissions	Audit	Logs					
С	Effective Permissions											
Ac	Access Control List											
	Path			Perm	nissions	ons Inherited From			Advanced permissions			
		FULL	READ	WRITE	MODIFY	READ & EXEC	LIST	SPECIAL				
±	IN10.209.89.3\Financi	a										
Ŧ	Ref 10.209.89.4\share1											
Ξ		e										
	IVAcmefiler/Acmesh	E.S.		<b>N</b>	1	<b>I</b>				<b></b>		
	<b>-</b> 1		Ē	<b>S</b>	1	Ē				<b></b>		
	Engineering		E			ED.			Domain Users@tulip	.m 🛃		
	Engineering\anu	<b>S</b>	E	<b>N</b>	1	<b>I</b>			🚭 Everyone	<b></b>		
	Executives\Querter			<b>N</b>	1	<b>I</b>				<b></b>		
	Finance\PAYROLL					Ē.			🚭 Everyone	<b></b>		
	HR\OpenReqs					<b>I</b>			🚭 Everyone	<b></b>		
	Legal/IDF		=	<b>\$</b>	<b>1</b>	•			😵 Everyone	<u>a</u>		
	Legal/Patent		E	<b>N</b>	1	Ð			😽 Everyone	<b></b>		
	Sales\2009		=			<b>I</b>			Domain Users@tulip	.m 🛃		
4												

If there is a break in ACE inheritance, you will see a lock next to the folder icon in the tree view, and a popup will appear warning you that the permissions structure has changed.



Identifying unique control points can also be a useful tool in evaluating permissions, or finding locations where high-level users have broken standards and change permissions.