ArcSight

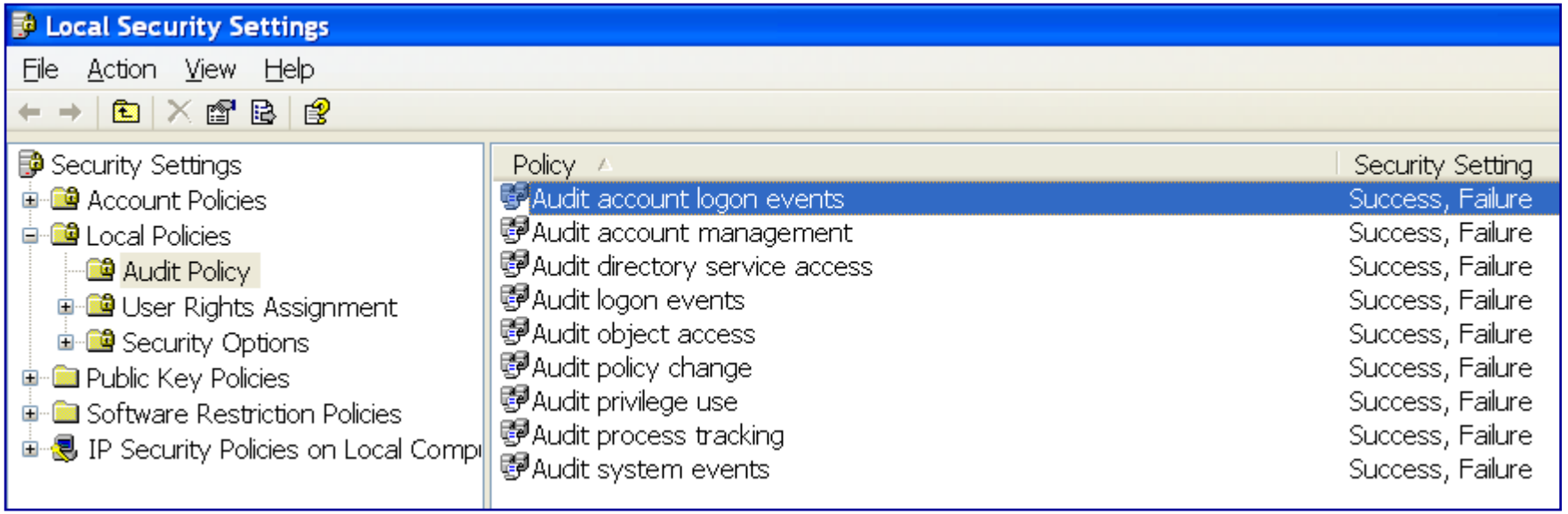
Monitoring and Analyzing Windows 2003 and XP Event Logs

Doron A. Keller, CISSP
Sr. Solutions Engineer
September 2008

Outline

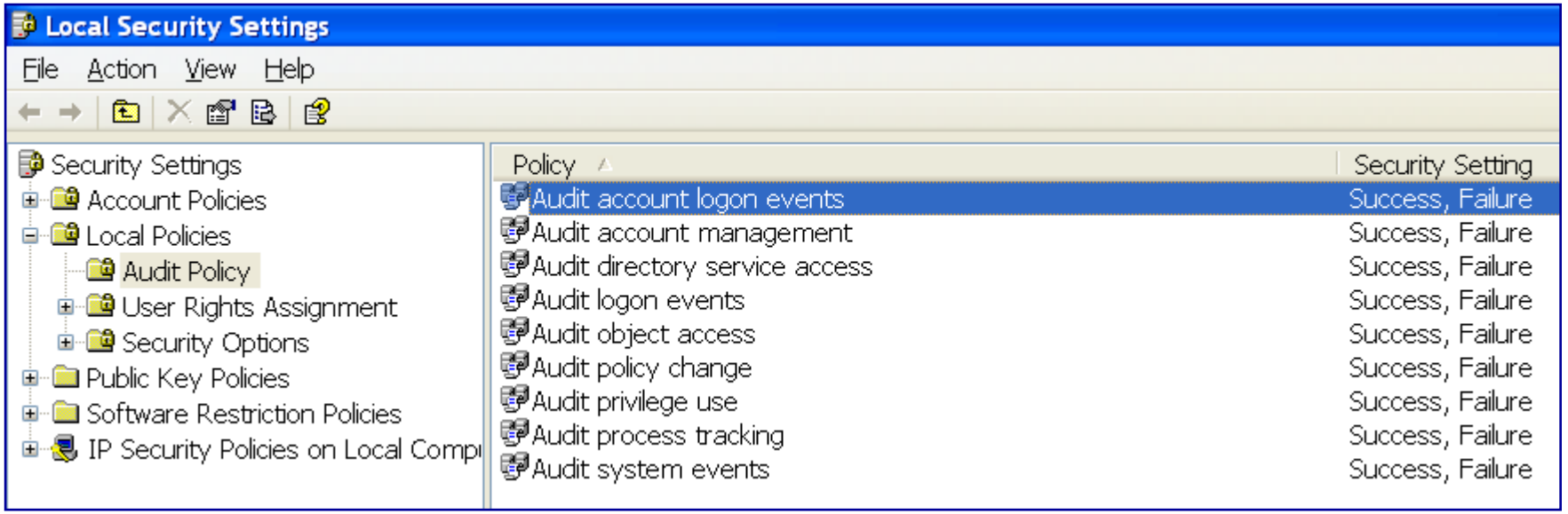
- Setting Windows 2K3 Audit
- Authentication Events
- Logon/Logoff
- File Access
- Account Management
- Directory Service Access
- Process Tracking
- Summary

Setting Windows Audit

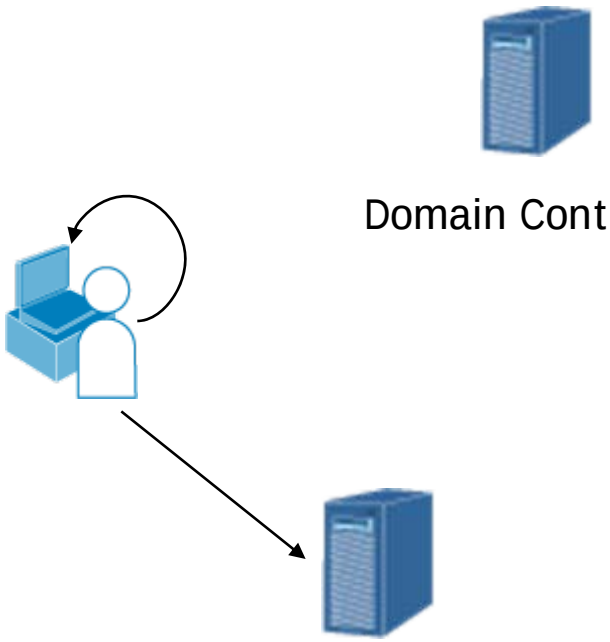


Authentication

Audit Account Logon Events



Kerberos Login Process



Events

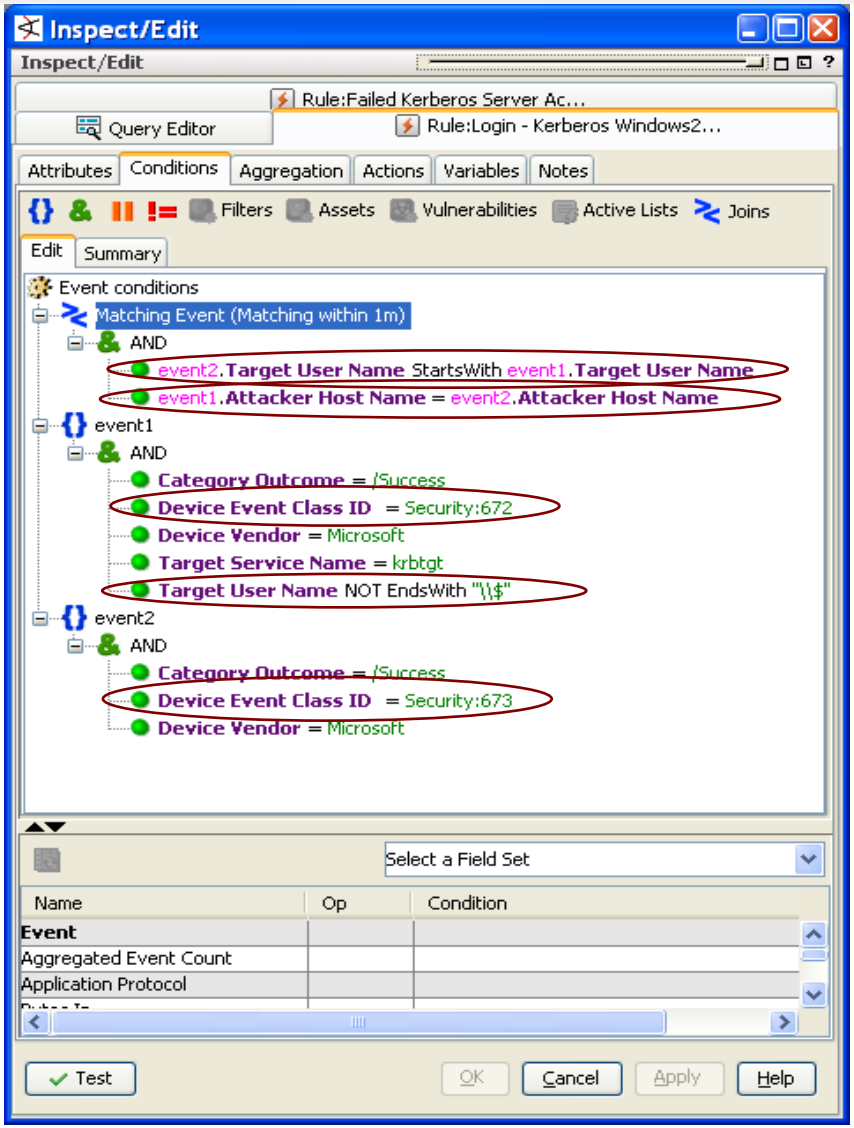
Event ID 672: Authentication Ticket Request

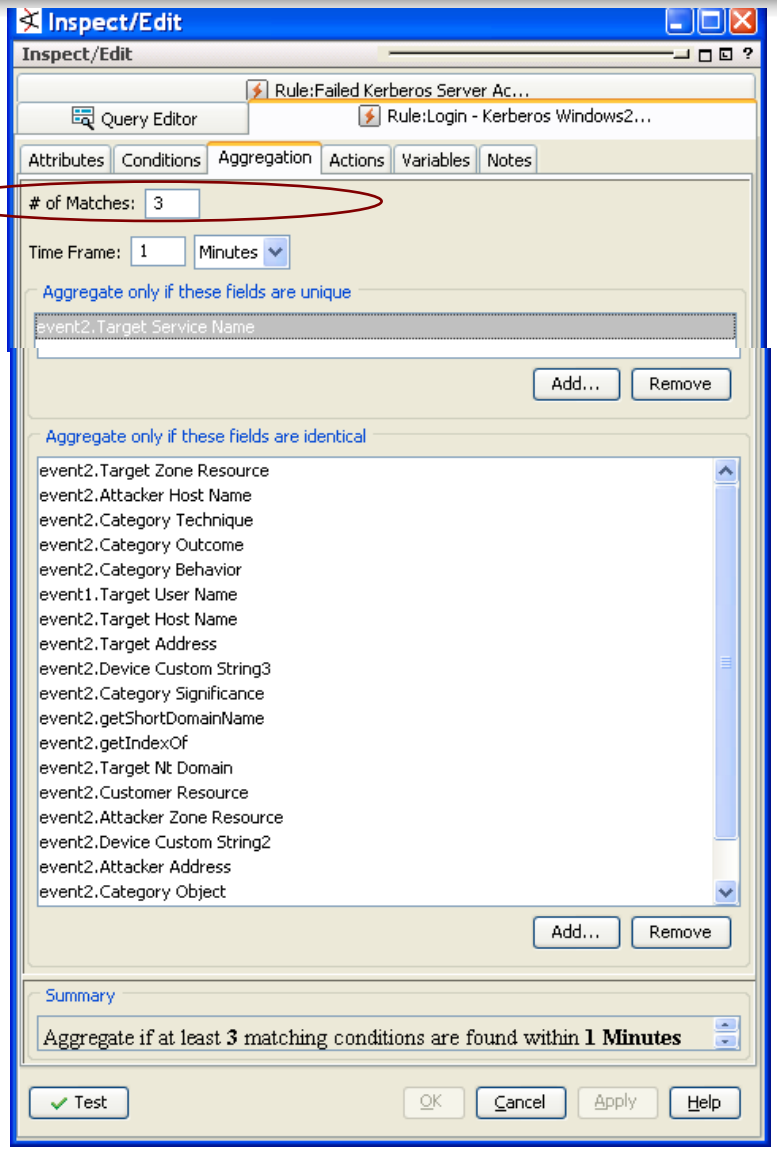
- Event Type: Success Audit
- Date: 8/4/2008
- Time: 5:53:44 PM
- Computer: HOST1
- User Name: palmoni
- Supplied Realm Name: TESTDOMAIN
- Client Address: 192.168.43.11

Event ID 673: Service Ticket Request

- Event Type: Success Audit
- Date: 8/4/2008
- Time: 5:53:44 PM
- Computer: HOST1
- User Name: palmoni@TESTDOMAIN.LOCAL
- User Domain: TESTDOMAIN.LOCAL
- Client Address: 192.168.43.11
- Service Name: HOST1$

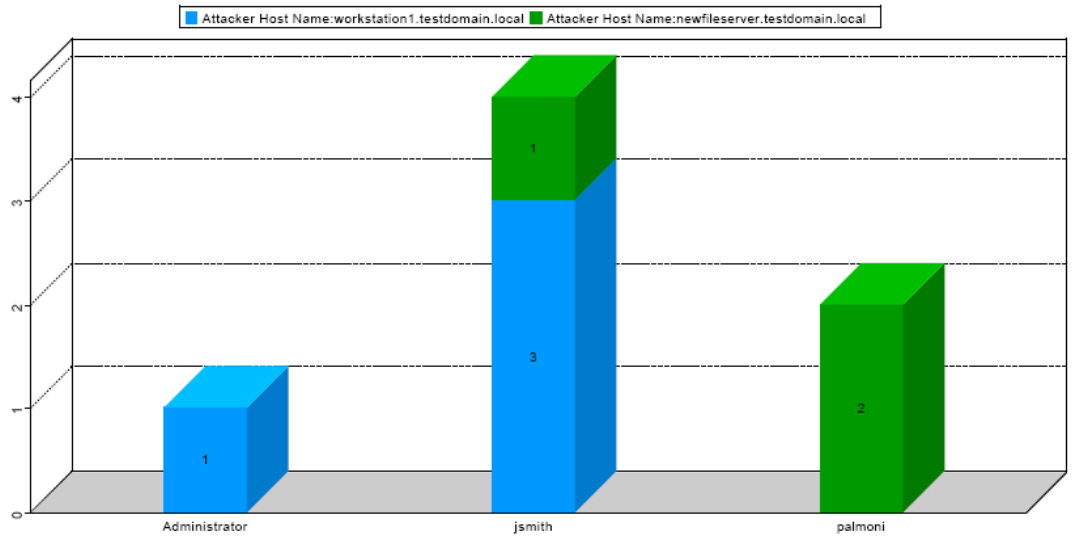
Kerberos Login Rule





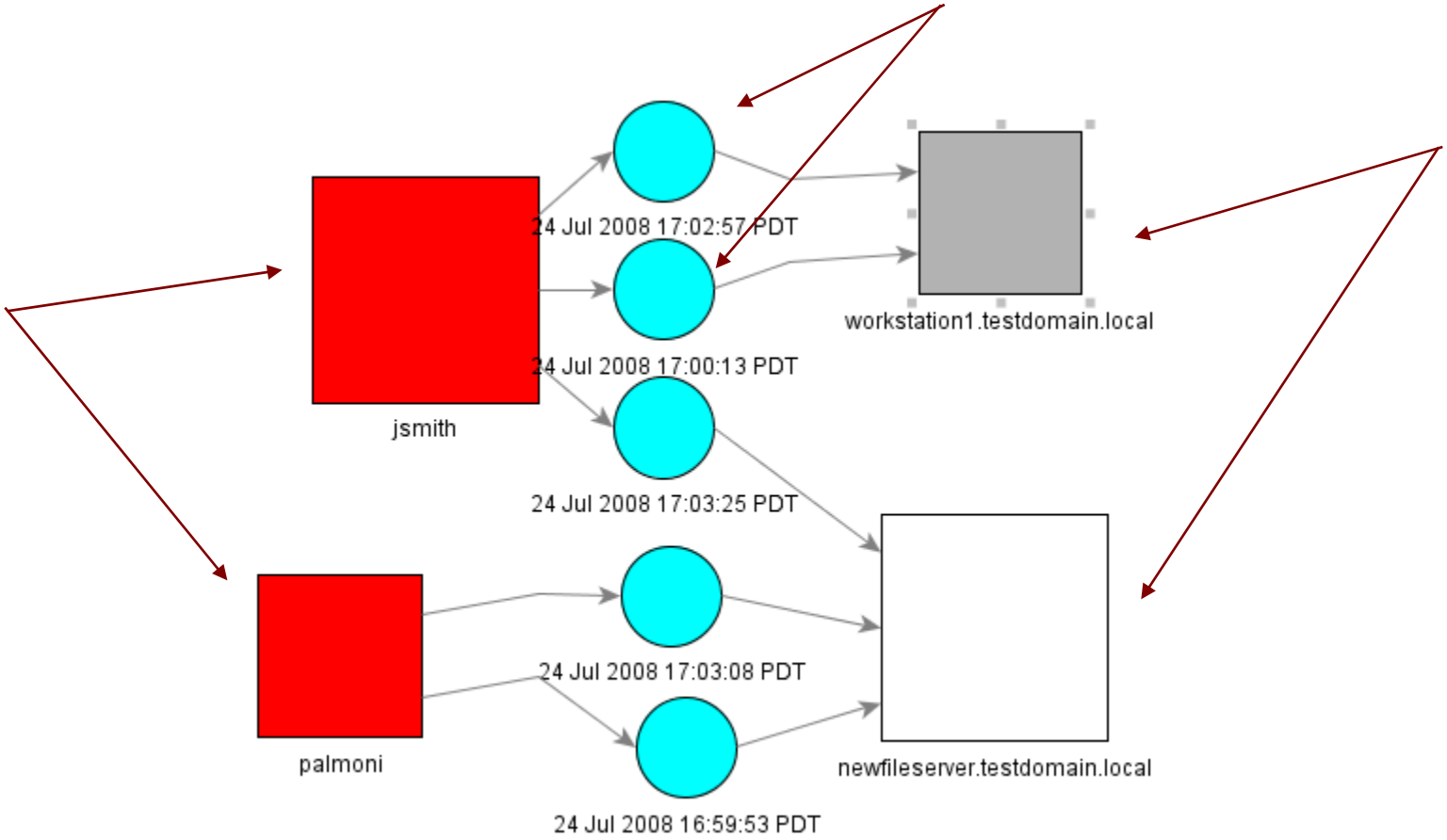
Login Reports

Windows - Kerbreos Logins



Target User Name	Attacker Host Name	End Time
Administrator	workstation1.testdomain.local	Jul 25 2008 15:19:55
jsmith	newfileserver.testdomain.local	Jul 24 2008 17:03:25
	workstation1.testdomain.local	Jul 24 2008 17:00:13
		Jul 24 2008 17:02:57
		Jul 25 2008 15:20:39
palmoni	newfileserver.testdomain.local	Jul 24 2008 16:59:53
		Jul 24 2008 17:03:08

Kerberos Logins - Dashboard



Login Failure Events

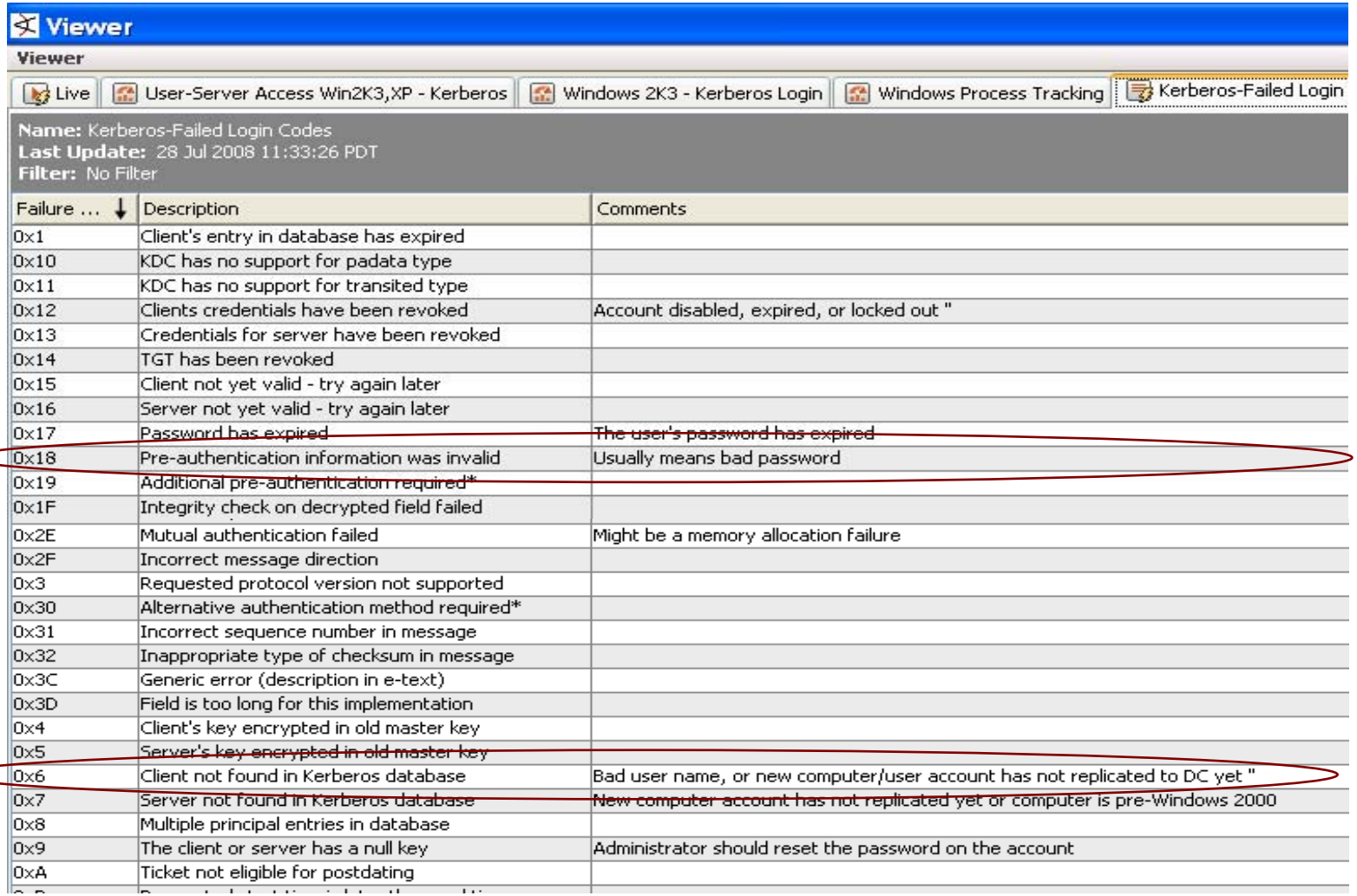
Event ID 672: Authentication Ticket Request

- Event Type: Failure Audit
- Date: 7/28/2008
- Time: 2:18:43 PM
- User Name: hacker
- Supplied Realm Name: TESTDOMAIN
- Client Address: 192.168.43.10
- Result Code: 0x6

Event ID 675: Pre-Authentication Failed

- Event Type: Failure Audit
- Date: 7/28/2008
- Time: 2:18:33 PM
- User Name: jsmith
- User ID: TESTDOMAIN\jsmith
- Client Address: 192.168.43.11
- Failure Code: 0x18

Kerberos Failure Codes



Viewer

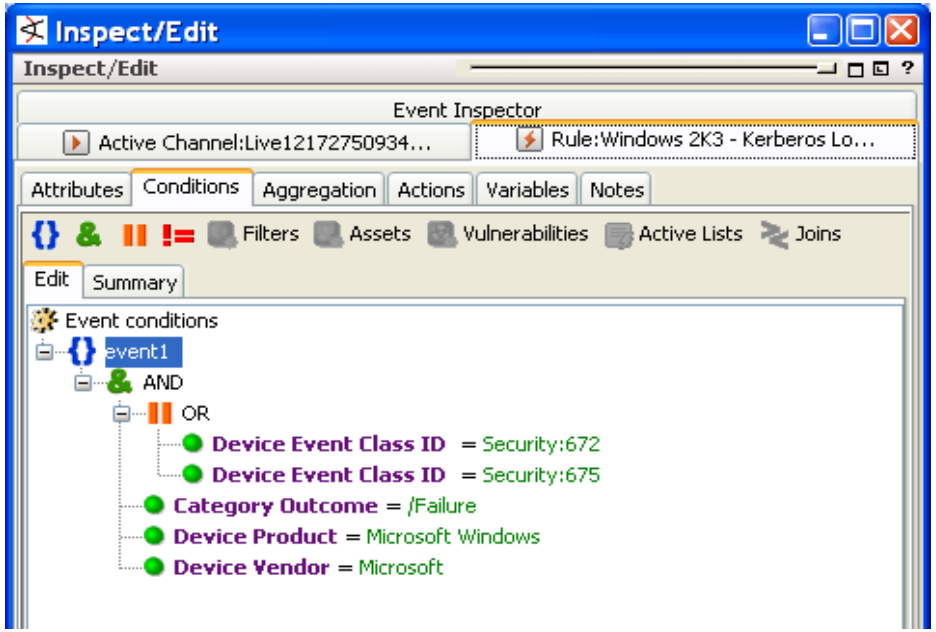
Viewer

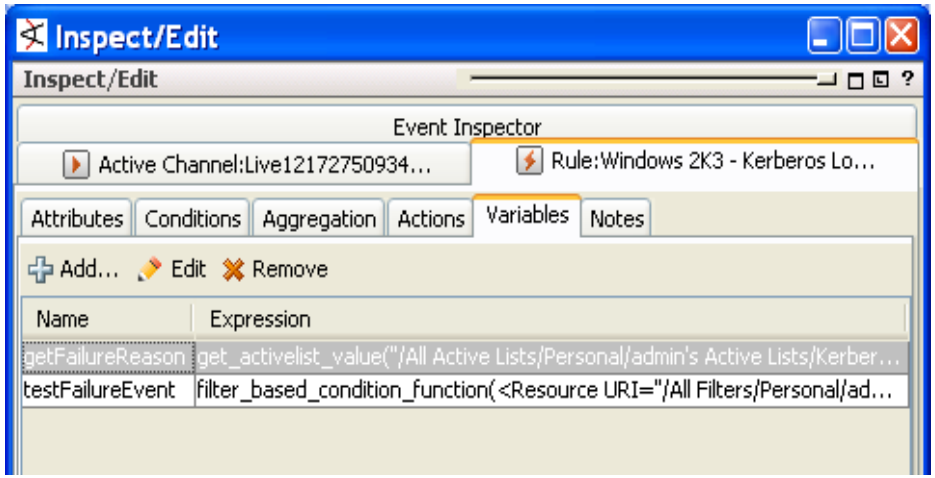
Live | User-Server Access Win2K3,XP - Kerberos | Windows 2K3 - Kerberos Login | Windows Process Tracking | Kerberos-Failed Login

Name: Kerberos-Failed Login Codes
Last Update: 28 Jul 2008 11:33:26 PDT
Filter: No Filter

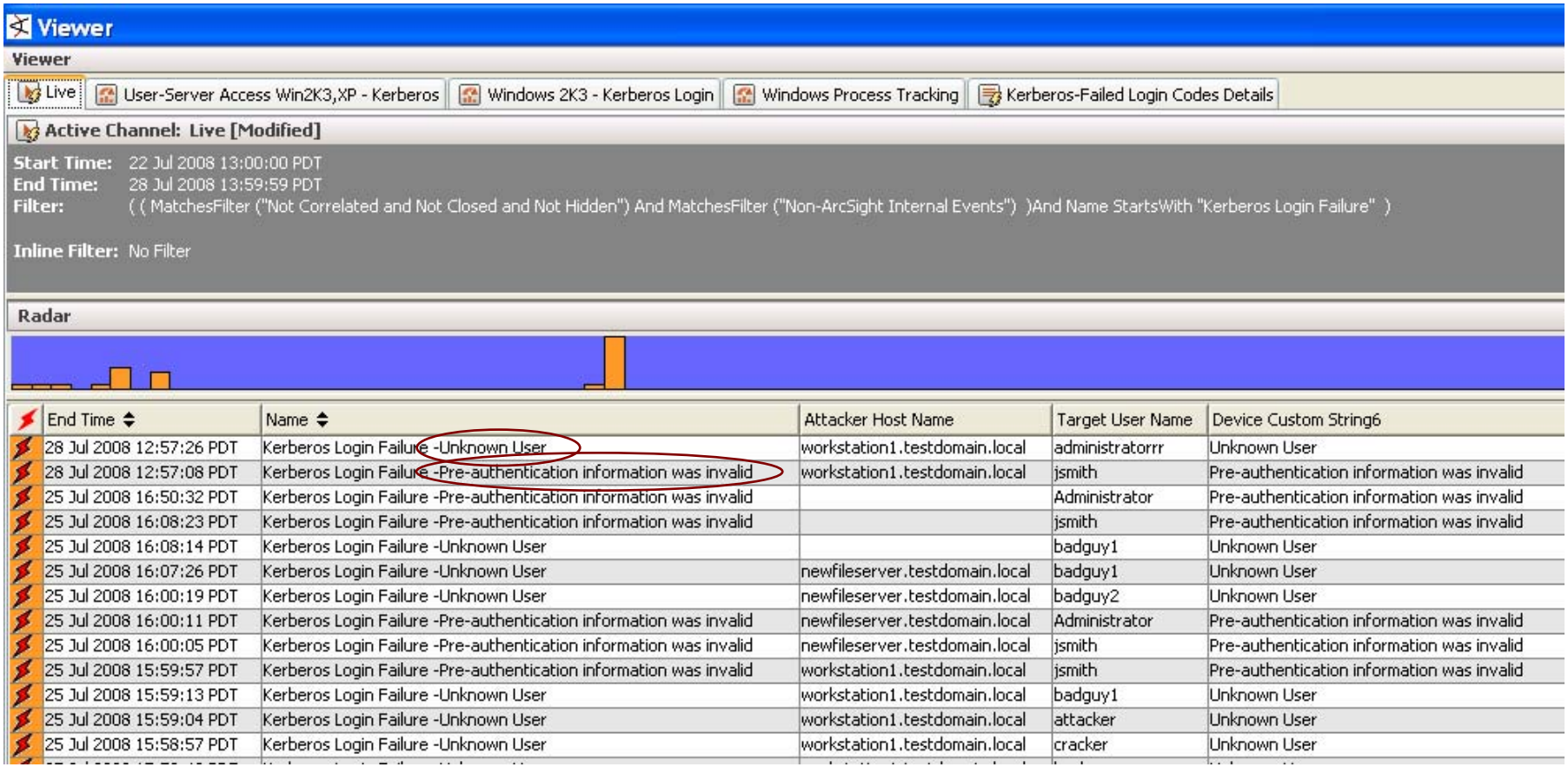
Failure ...	Description	Comments
0x1	Client's entry in database has expired	
0x10	KDC has no support for padata type	
0x11	KDC has no support for transited type	
0x12	Clients credentials have been revoked	Account disabled, expired, or locked out "
0x13	Credentials for server have been revoked	
0x14	TGT has been revoked	
0x15	Client not yet valid - try again later	
0x16	Server not yet valid - try again later	
0x17	Password has expired	The user's password has expired
0x18	Pre-authentication information was invalid	Usually means bad password
0x19	Additional pre-authentication required*	
0x1F	Integrity check on decrypted field failed	
0x2E	Mutual authentication failed	Might be a memory allocation failure
0x2F	Incorrect message direction	
0x3	Requested protocol version not supported	
0x30	Alternative authentication method required*	
0x31	Incorrect sequence number in message	
0x32	Inappropriate type of checksum in message	
0x3C	Generic error (description in e-text)	
0x3D	Field is too long for this implementation	
0x4	Client's key encrypted in old master key	
0x5	Server's key encrypted in old master key	
0x6	Client not found in Kerberos database	Bad user name, or new computer/user account has not replicated to DC yet "
0x7	Server not found in Kerberos database	New computer account has not replicated yet or computer is pre-Windows 2000
0x8	Multiple principal entries in database	
0x9	The client or server has a null key	Administrator should reset the password on the account
0xA	Ticket not eligible for postdating	

Kerberos Failed Logins - Rule





Failed Login Active Channel



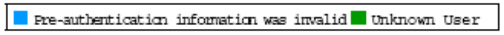
End Time	Name	Attacker Host Name	Target User Name	Device Custom String6
28 Jul 2008 12:57:26 PDT	Kerberos Login Failure -Unknown User	workstation1.testdomain.local	administratorrr	Unknown User
28 Jul 2008 12:57:08 PDT	Kerberos Login Failure -Pre-authentication information was invalid	workstation1.testdomain.local	jsmith	Pre-authentication information was invalid
25 Jul 2008 16:50:32 PDT	Kerberos Login Failure -Pre-authentication information was invalid		Administrator	Pre-authentication information was invalid
25 Jul 2008 16:08:23 PDT	Kerberos Login Failure -Pre-authentication information was invalid		jsmith	Pre-authentication information was invalid
25 Jul 2008 16:08:14 PDT	Kerberos Login Failure -Unknown User		badguy1	Unknown User
25 Jul 2008 16:07:26 PDT	Kerberos Login Failure -Unknown User	newfileserver.testdomain.local	badguy1	Unknown User
25 Jul 2008 16:00:19 PDT	Kerberos Login Failure -Unknown User	newfileserver.testdomain.local	badguy2	Unknown User
25 Jul 2008 16:00:11 PDT	Kerberos Login Failure -Pre-authentication information was invalid	newfileserver.testdomain.local	Administrator	Pre-authentication information was invalid
25 Jul 2008 16:00:05 PDT	Kerberos Login Failure -Pre-authentication information was invalid	newfileserver.testdomain.local	jsmith	Pre-authentication information was invalid
25 Jul 2008 15:59:57 PDT	Kerberos Login Failure -Pre-authentication information was invalid	workstation1.testdomain.local	jsmith	Pre-authentication information was invalid
25 Jul 2008 15:59:13 PDT	Kerberos Login Failure -Unknown User	workstation1.testdomain.local	badguy1	Unknown User
25 Jul 2008 15:59:04 PDT	Kerberos Login Failure -Unknown User	workstation1.testdomain.local	attacker	Unknown User
25 Jul 2008 15:58:57 PDT	Kerberos Login Failure -Unknown User	workstation1.testdomain.local	cracker	Unknown User

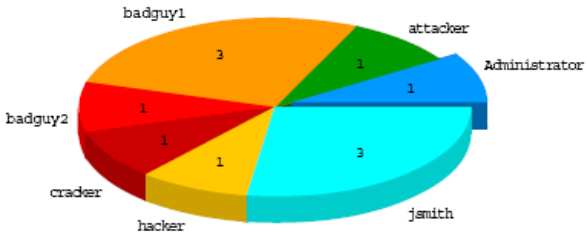
Kerberos Failed Logins - Reports

Windows 2K3 - Kerberos Login Failed

Failed Logins - Hosts per User

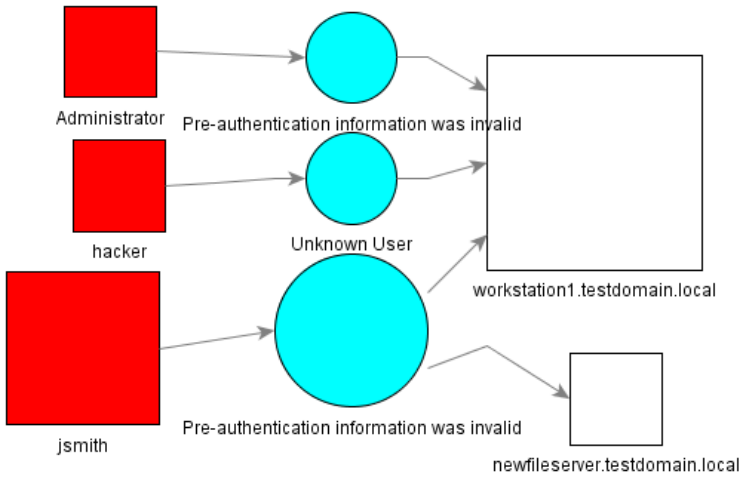
Reasons of Login Failures

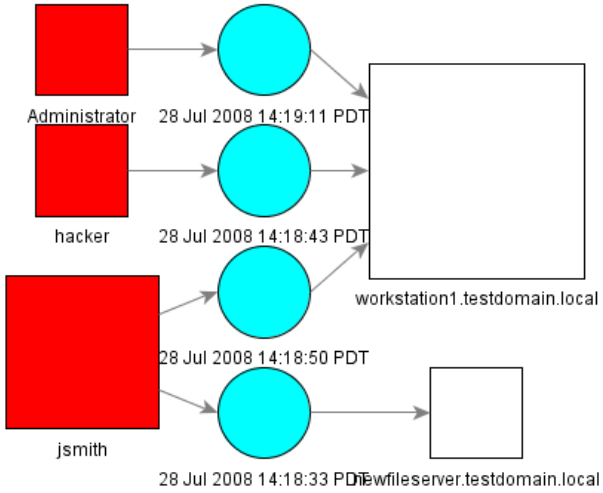




User Name	Failure Reason	Host Name	End Time
Administrator	Pre-authentication information was invalid	newfileserver.testdomain.local	Jul 25 2008 16:00:11
attacker	Unknown User	workstation1.testdomain.local	Jul 25 2008 15:59:04
badguy1	Unknown User	workstation1.testdomain.local	Jul 25 2008 15:59:13
		host1.testdomain.local	Jul 25 2008 16:08:14
		newfileserver.testdomain.local	Jul 25 2008 16:07:26
badguy2	Unknown User	newfileserver.testdomain.local	Jul 25 2008 16:00:19
cracker	Unknown User	workstation1.testdomain.local	Jul 25 2008 15:58:57
hacker	Unknown User	workstation1.testdomain.local	Jul 25 2008 15:58:49
jsmith	Pre-authentication information was invalid	workstation1.testdomain.local	Jul 25 2008 15:59:57
		host1.testdomain.local	Jul 25 2008 16:08:23
		newfileserver.testdomain.local	Jul 25 2008 16:00:05

Kerberos Failed Logins – Data Monitors





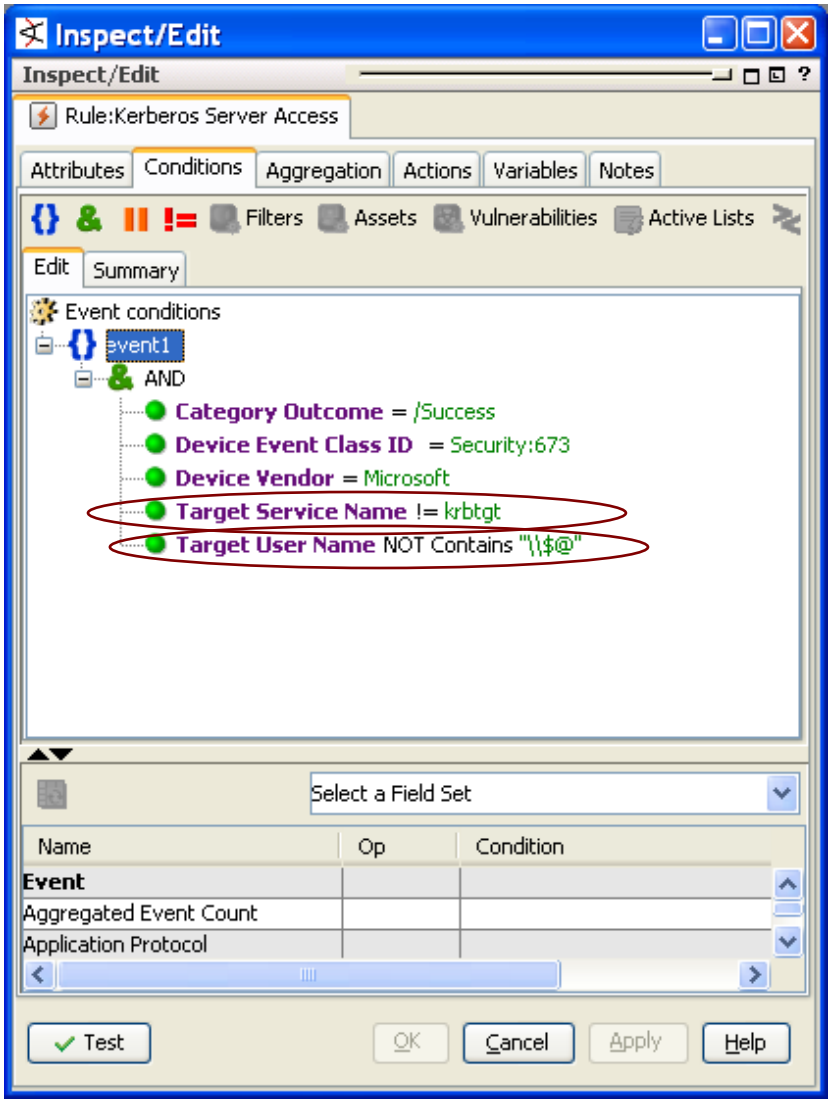
Server Access - Event ID 673

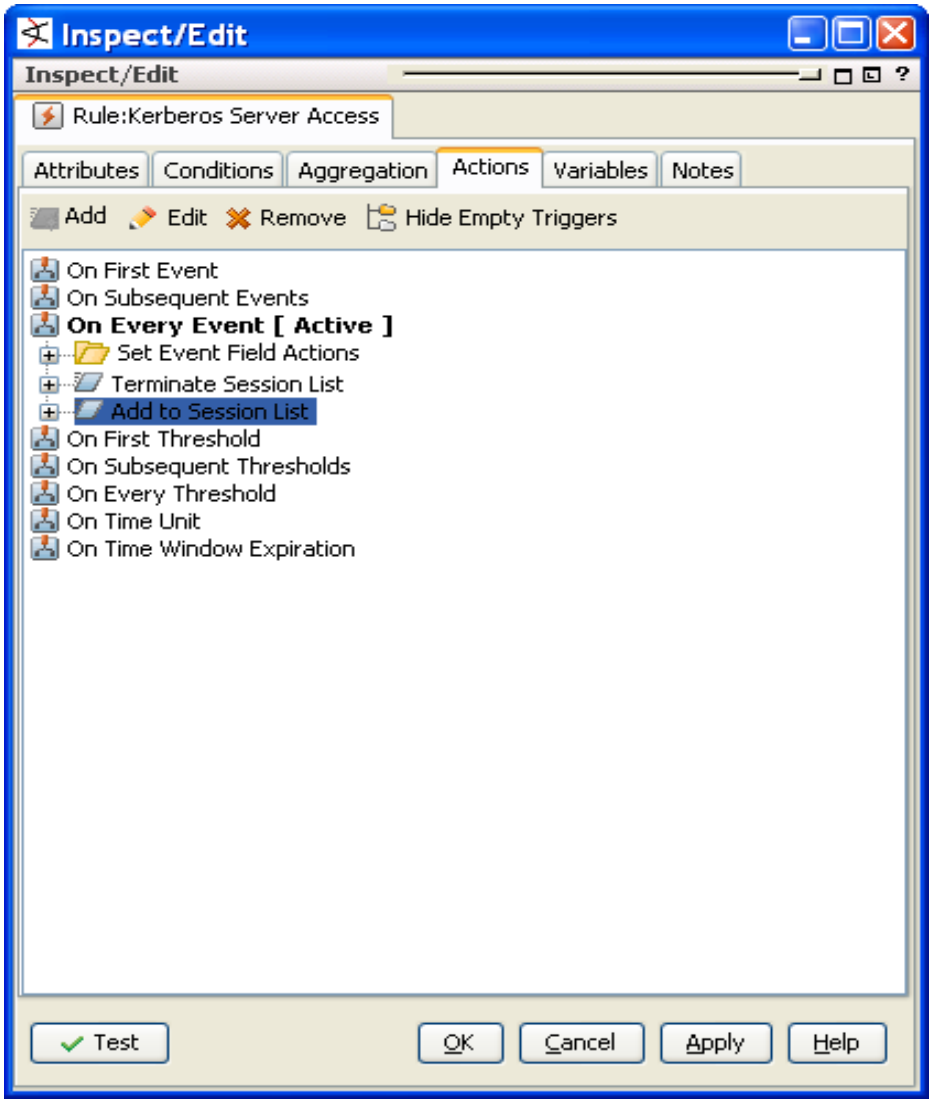
Event ID 673: Service Ticket Request

- Event Type: Success Audit
- Date: 8/4/2008
- Time: 5:53:44 PM
- Computer: HOST1
- User Name: palmoni@TESTDOMAIN.LOCAL
- Service Name: NEWFILESERVER$
- Client Address: 192.168.43.11
- Computer: HOST1

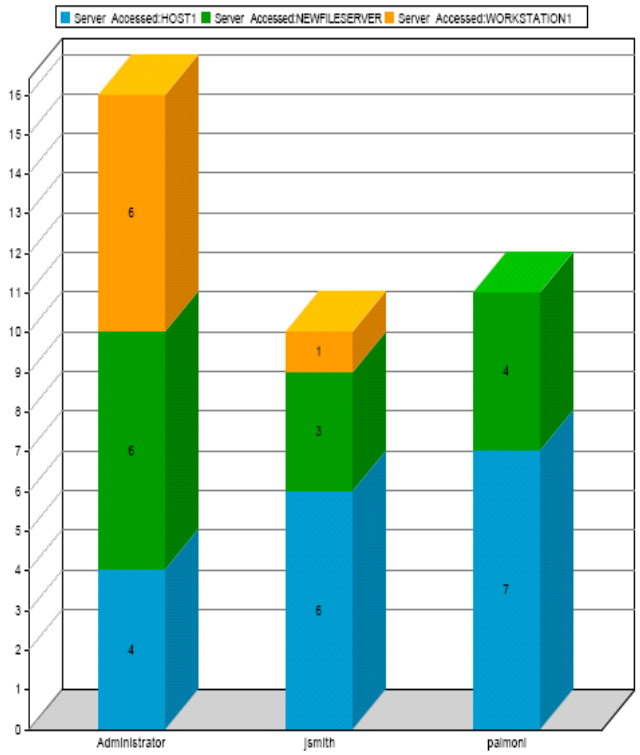
MS Field	ESM Field	Logger Report Field
User Name	Destination User Name	events.arc_ destinationUserName
Service Name	Destination Service Name	events.arc_ destinationService Name
Client Address	Source Address	events.arc_ sourceAddress
Computer	Destination Host Name	events.arc_ destinationHostName

Server Access - Rule



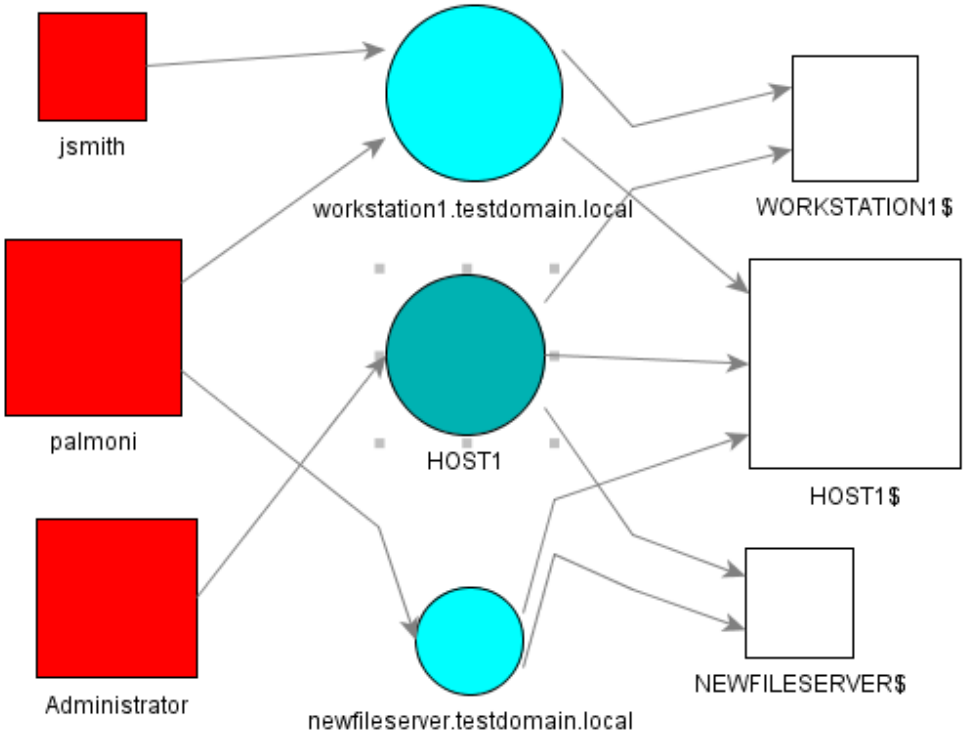


Server Access - Reports

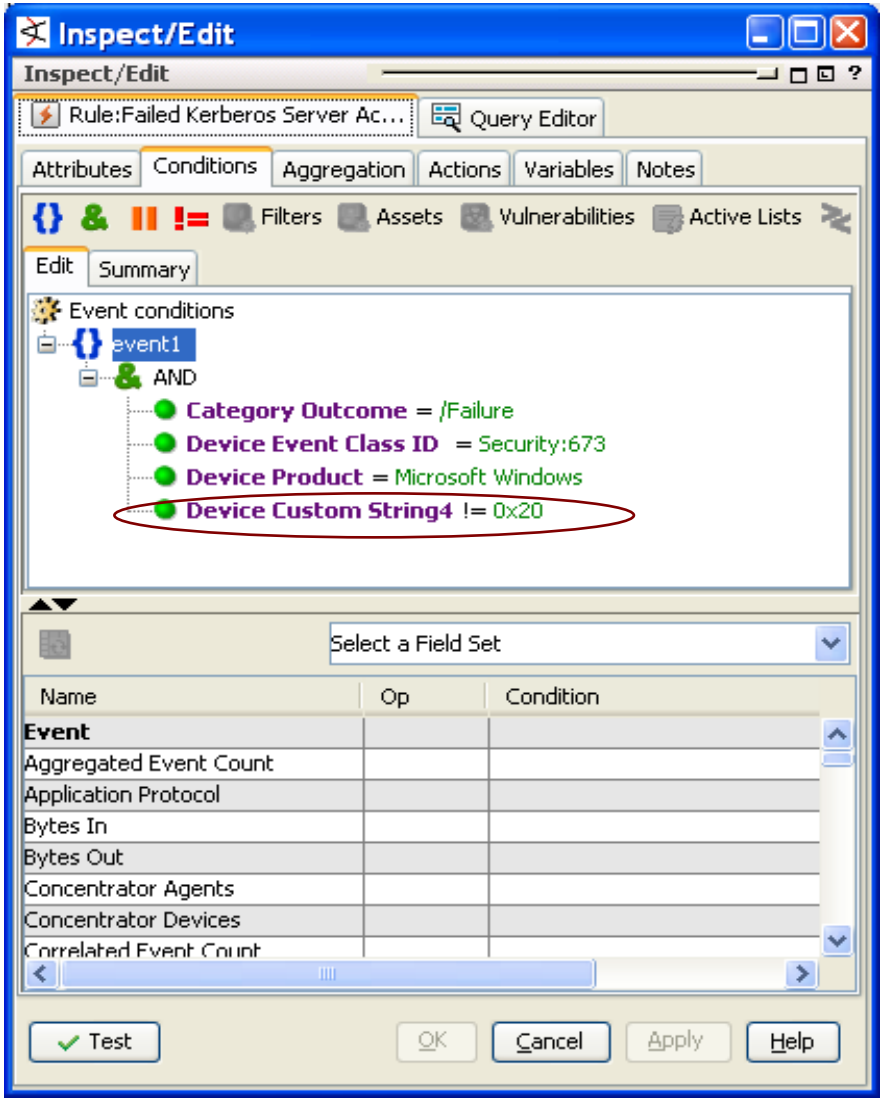


User Name	Host Name	Server Accessed
Administrator	host1.testdomain.local	HOST1
		WORKSTATION1
		NEWFILESERVER
	newfileserver.testdomain.local	NEWFILESERVER
		HOST1
	workstation1.testdomain.local	HOST1
		WORKSTATION1
jsmith	workstation1.testdomain.local	NEWFILESERVER
		HOST1
		WORKSTATION1
palmoni	newfileserver.testdomain.local	NEWFILESERVER
		HOST1
	workstation1.testdomain.local	WORKSTATION1
		HOST1

Data Monitors

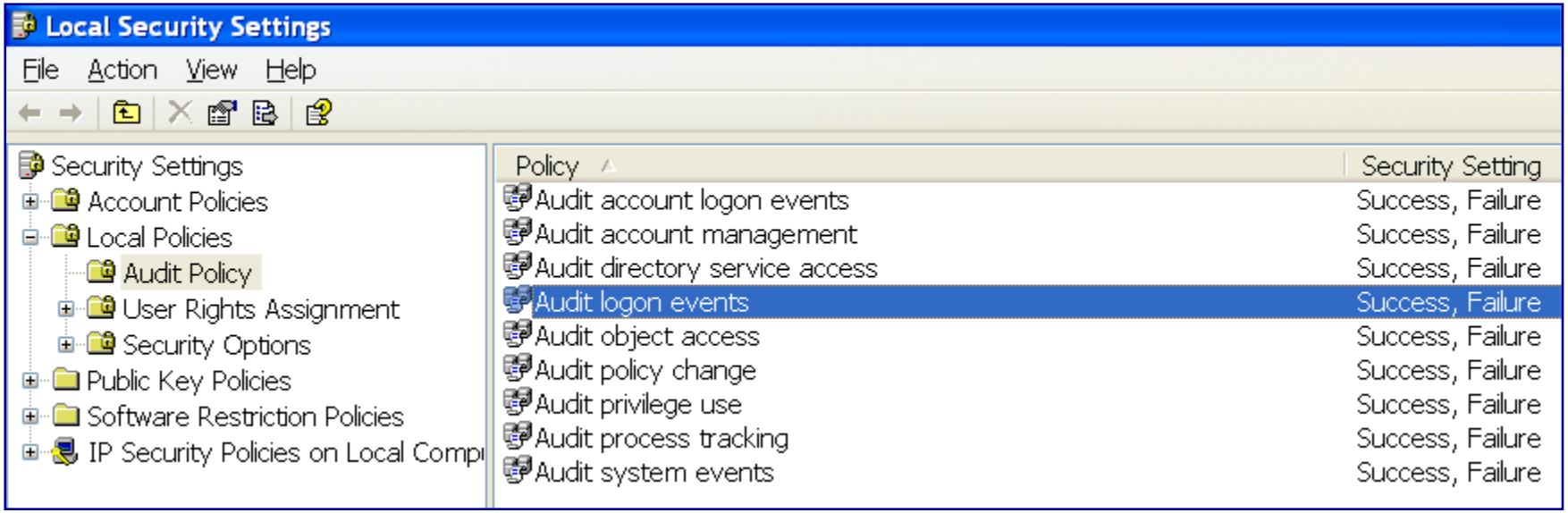


Failed Access Attempt

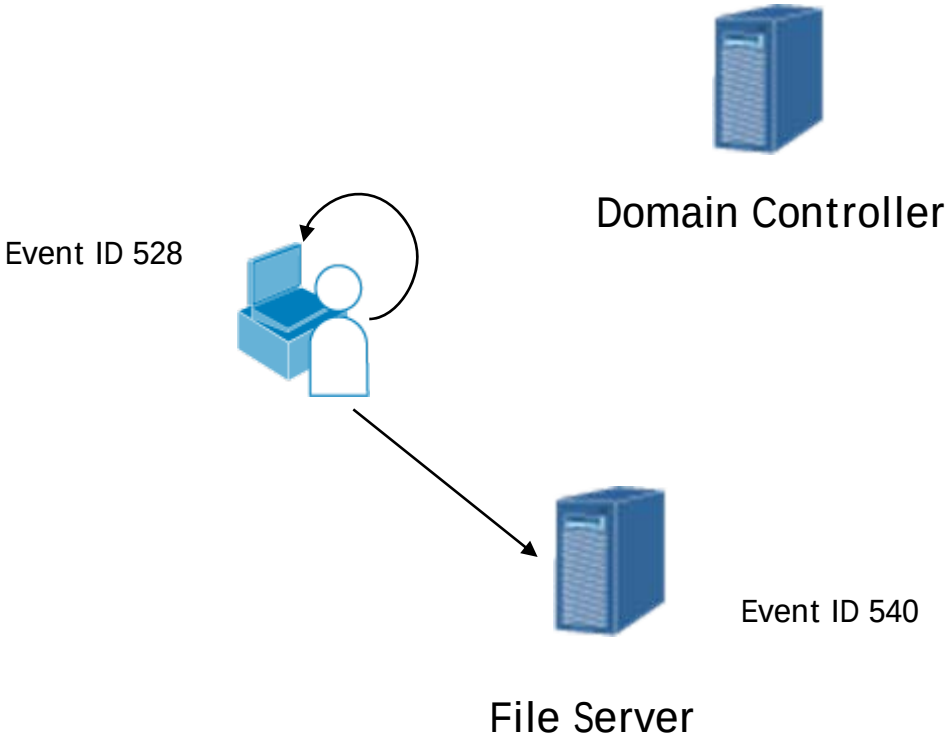


Logon/Logoff

Audit Logon Events



Authentication
Kerberos Login Process



Logon Event

Event ID 528: Successful Logon

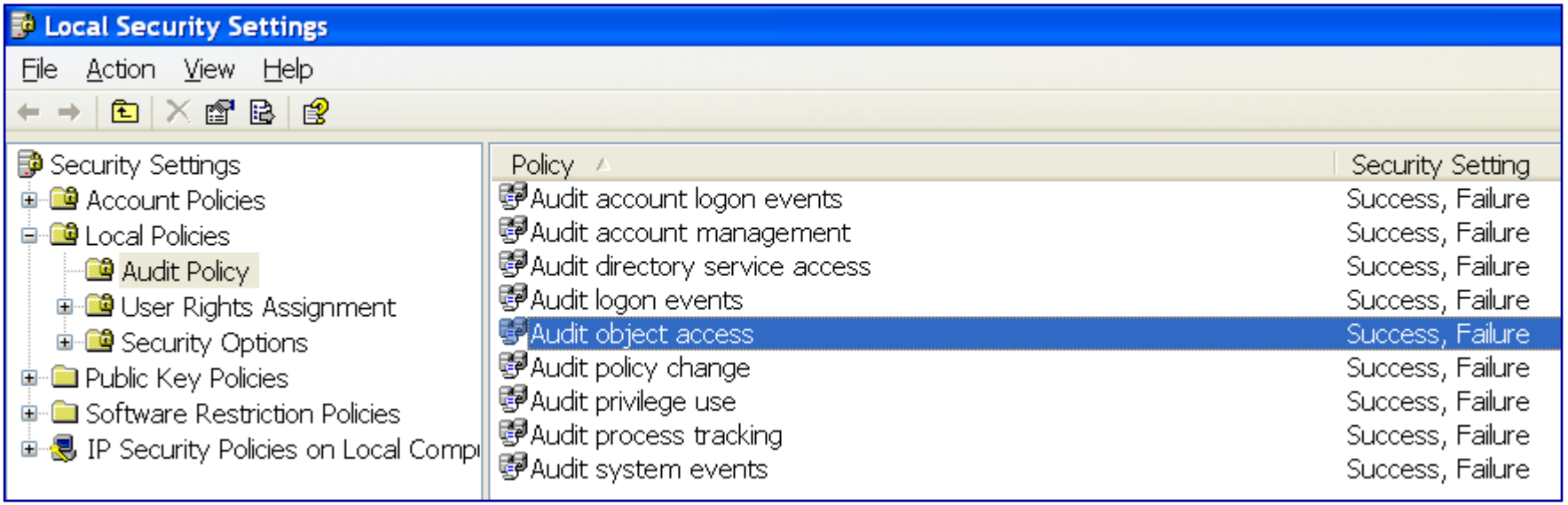
- Date: 7/31/2008
- Time: 4:46:41 PM
- User Name: Administrator
- Domain: HOST1
- Logon ID: (0x0,0x1DFAD)
- Logon Type: 2
- Workstation Name: HOST1
- Source Network Address: 127.0.0.1

Event ID 540: Successful Network Logon

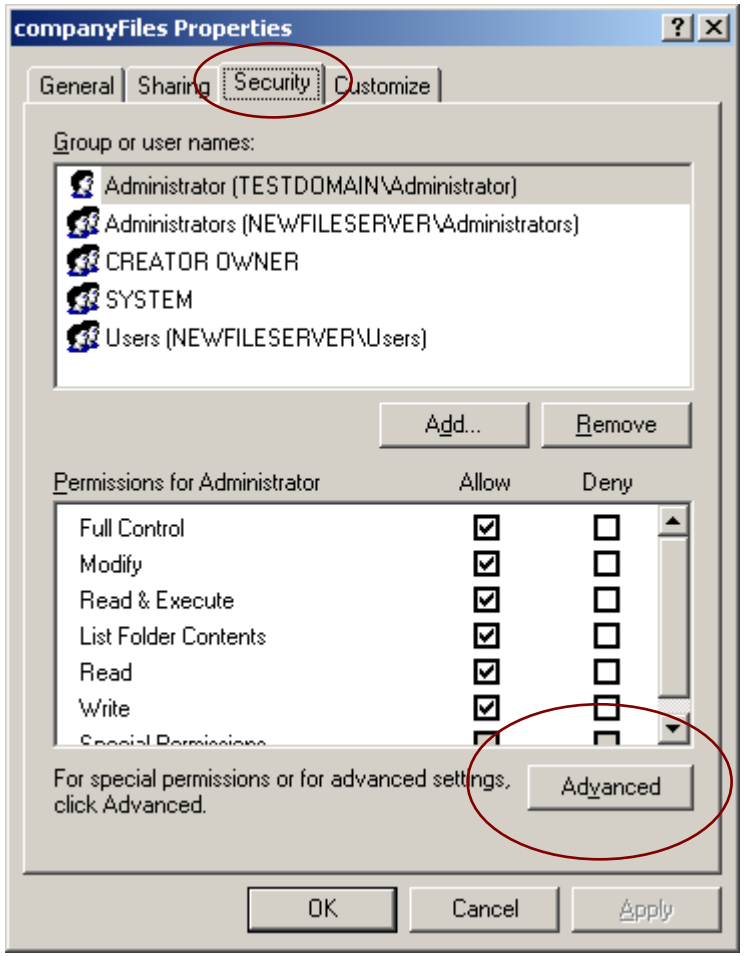
- Date: 8/7/2008
- Time: 2:47:04 PM
- User Name: jsmith
- Domain: TESTDOMAIN
- Logon ID: (0x0,0x18AD9DC)
- Logon Type: 3
- Source Network Address: 192.168.43.10

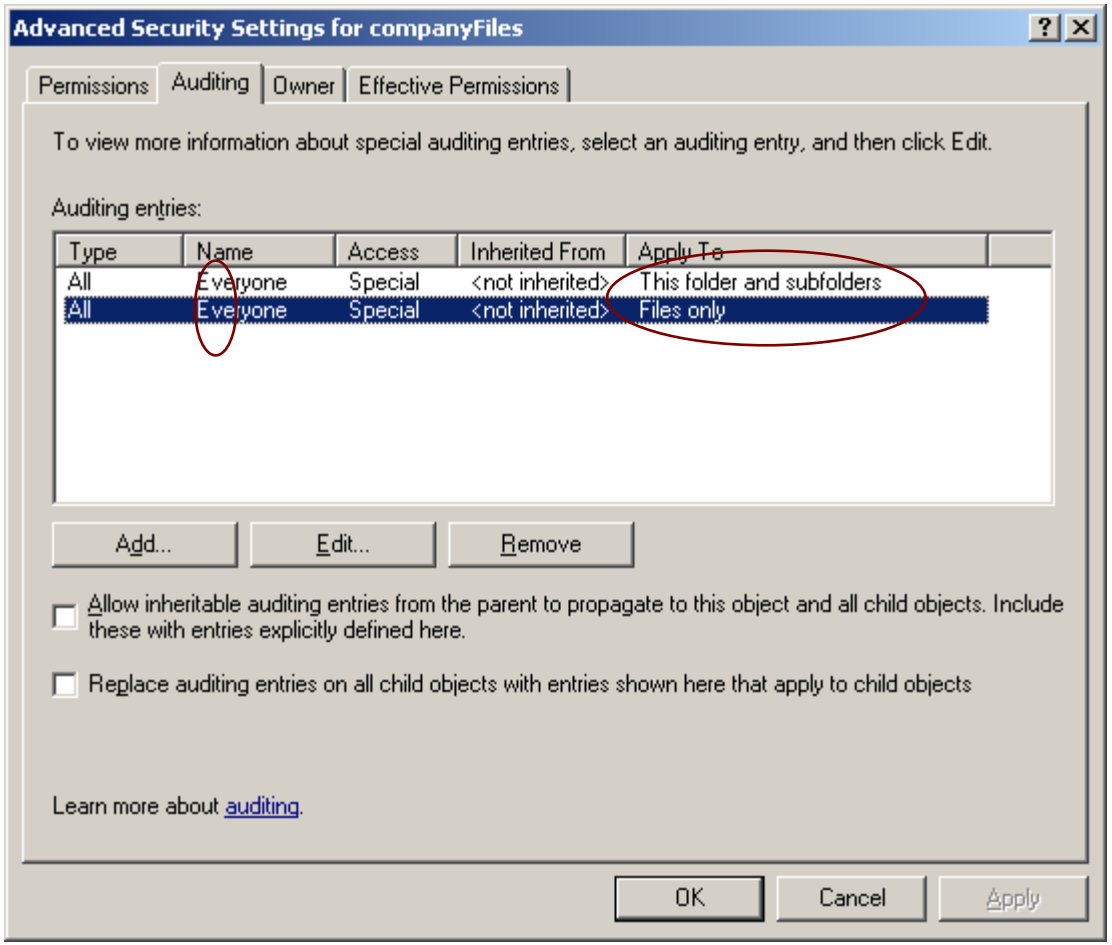
File Access

Audit Object Access

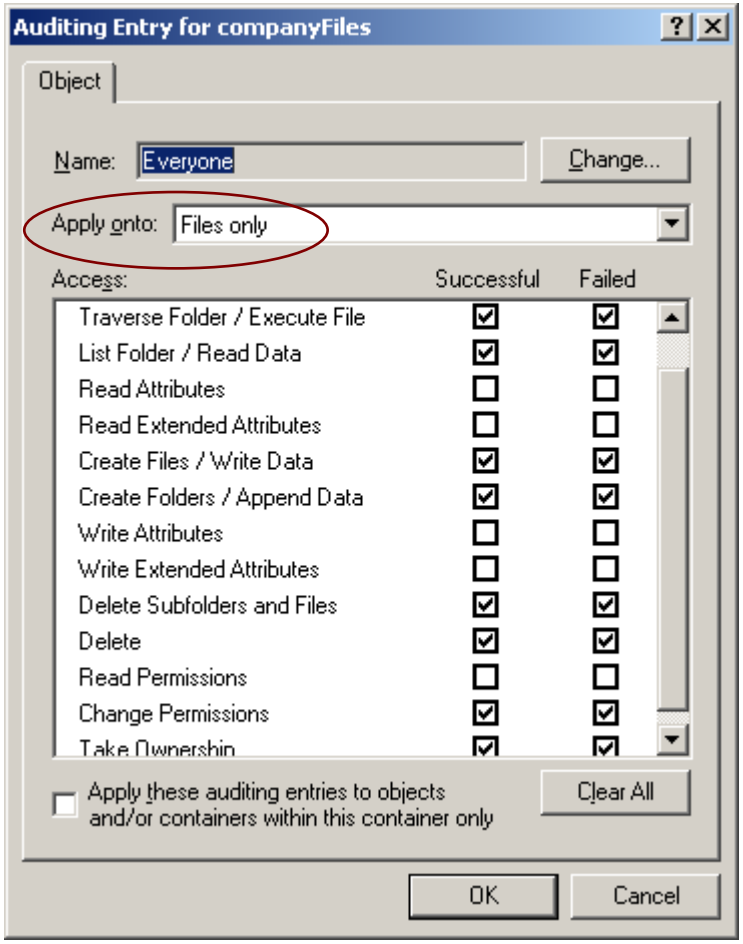


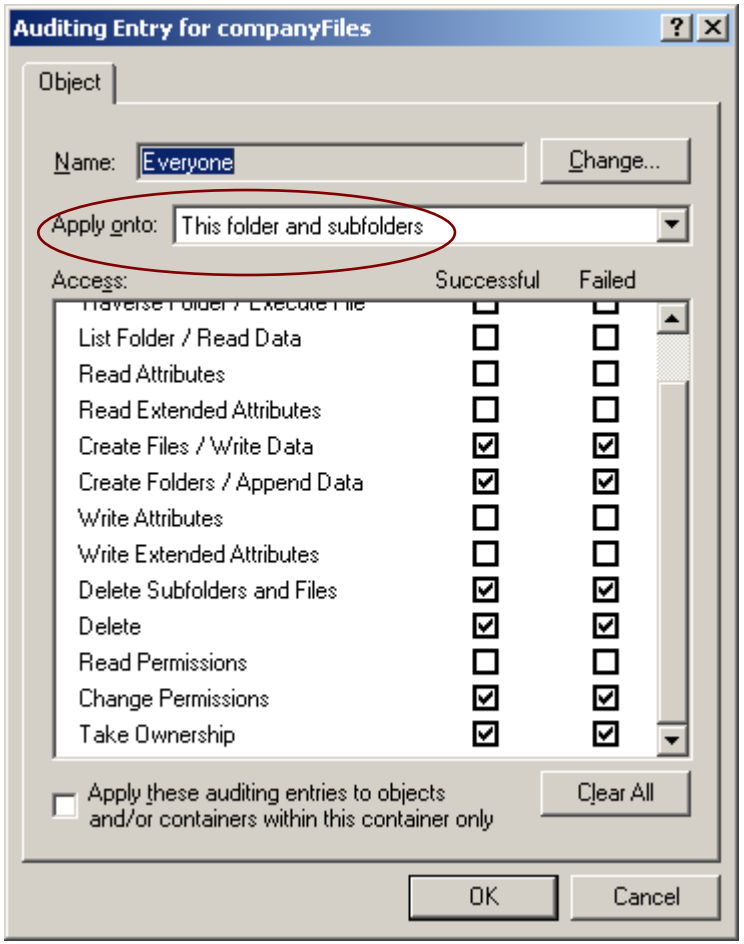
Enabling File Audit



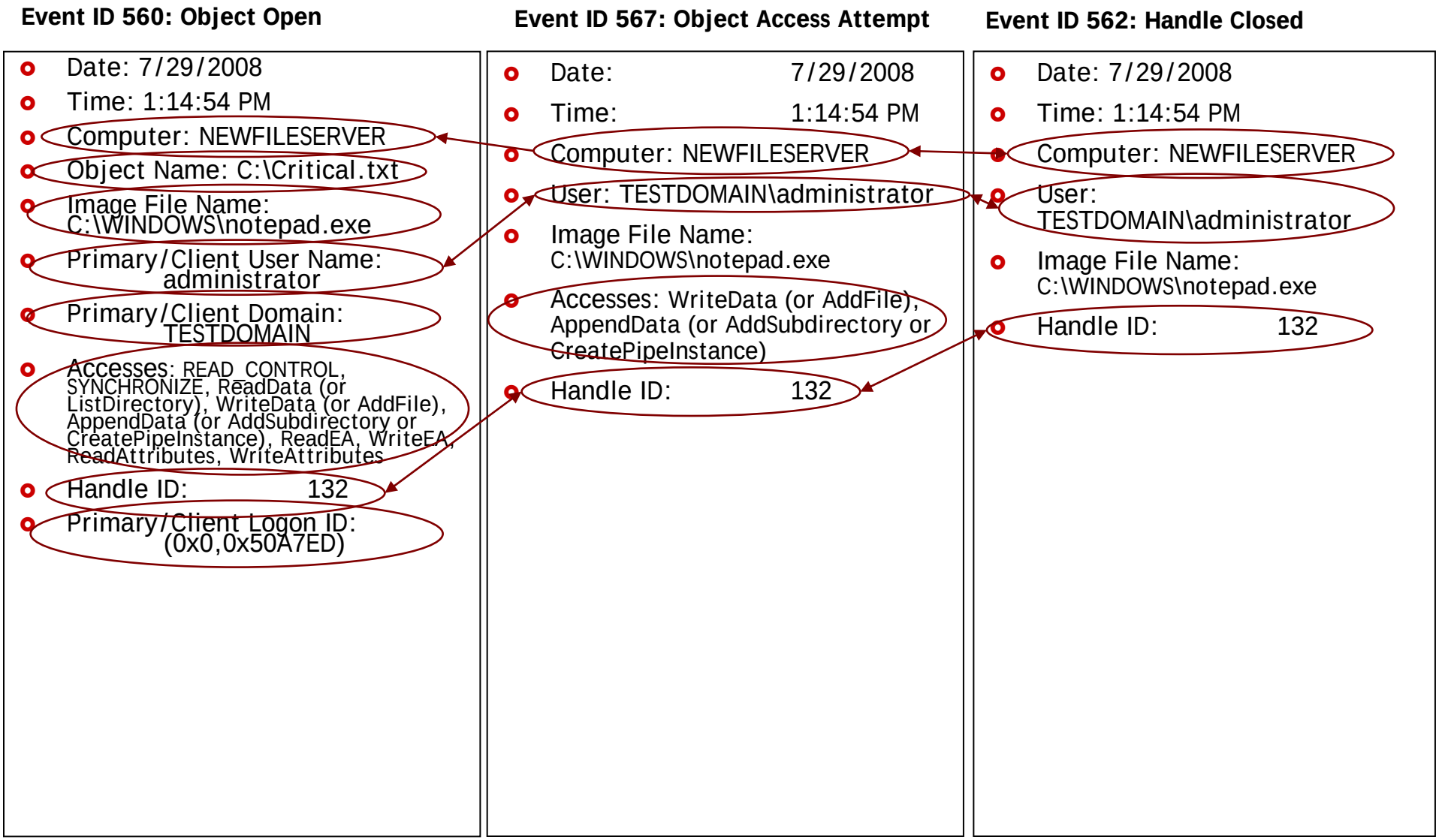


Enabling File Audit

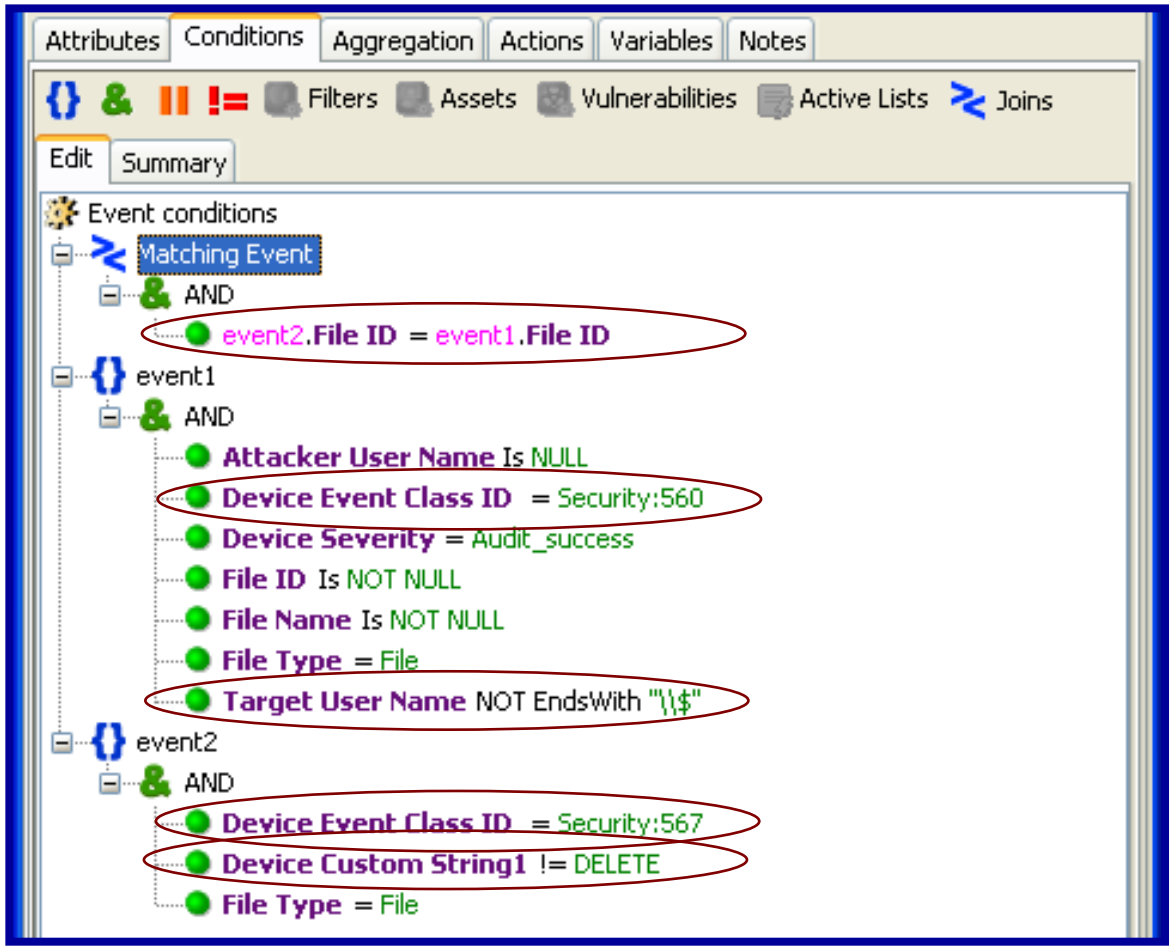




Audit Events



Rule



File Deletion Audit Events

Event ID 564: Object Deleted

- Date: 7/29/2008
- Time: 1:14:54 PM
- User: TESTDOMAIN\administrator
- Computer: NEWFILESERVER
- Handle ID: 400
- Image File Name: C:\WINDOWS\system32\notepad.exe

Failed Access Events

Event ID 560: Failed Object Access

- Event Type: Failure Audit
- Event Category: Object Access
- Event ID: 560
- Date: 7/29/2008
- Time: 3:37:57 PM
- Computer: NEWFILESERVER
- Object Name: C:\companyFiles\Critical Files\credit card numbers.txt
- Handle ID: -
- Client User Name: jsmith
- Client Domain: TESTDOMAIN
- Client Logon ID: (0x0,0x6D0F03)
- Accesses: READ_CONTROL ReadData (or ListDirectory) ReadEA ReadAttributes

Dashboard

Last 25 Deleted Files

Last 25 Deleted Files

attackerUserHostDomain4	File Name	targetUserHostDomain4	End Time
jsmith/Remote Host/TESTDOMAIN	C:\companyFiles\Critical Files\Salaries.txt	NEWFILESERVER$/NEWFILESERVER/TESTDOMAIN	29 Jul 2008 15:25:25 PDT
administrator/NEWFILESERVER/TESTDOMAIN	C:\companyFiles\Critical Files\test.txt	administrator/NEWFILESERVER/TESTDOMAIN	29 Jul 2008 15:24:11 PDT
administrator/NEWFILESERVER/TESTDOMAIN	C:\companyFiles\Critical Files\Copy of Salaries.txt	administrator/NEWFILESERVER/TESTDOMAIN	29 Jul 2008 15:24:03 PDT

Last 25 Failed File Deletions

Last 25 Failed File Deletions

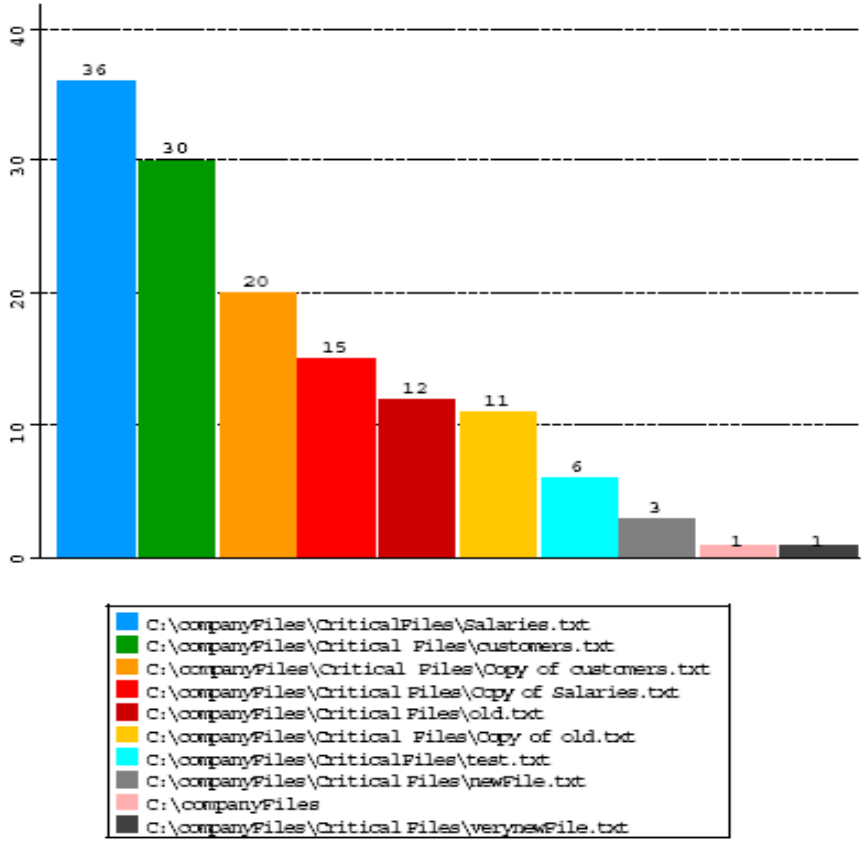
attackerUserHostDomain4	File Name	targetUserHostDomain4	End Time
jsmith/Remote Host/TESTDOMAIN	C:\companyFiles\Critical Files\credit card numbers.txt	NEWFILESERVER$/NEWFILESERVER/TESTDOMAIN	29 Jul 2008 15:25:05 PDT

Reports

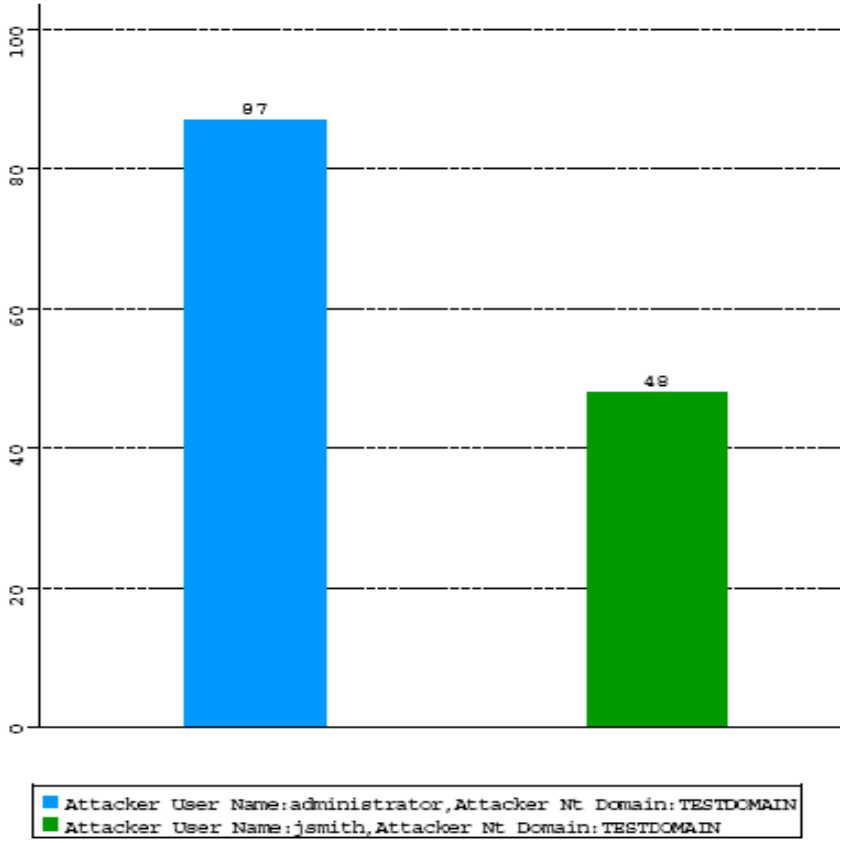
Successful File Access per User

FISMA - NIST § SI- 1 - System and Information Integrity Policy and Procedures

Top 10 Accessed Files

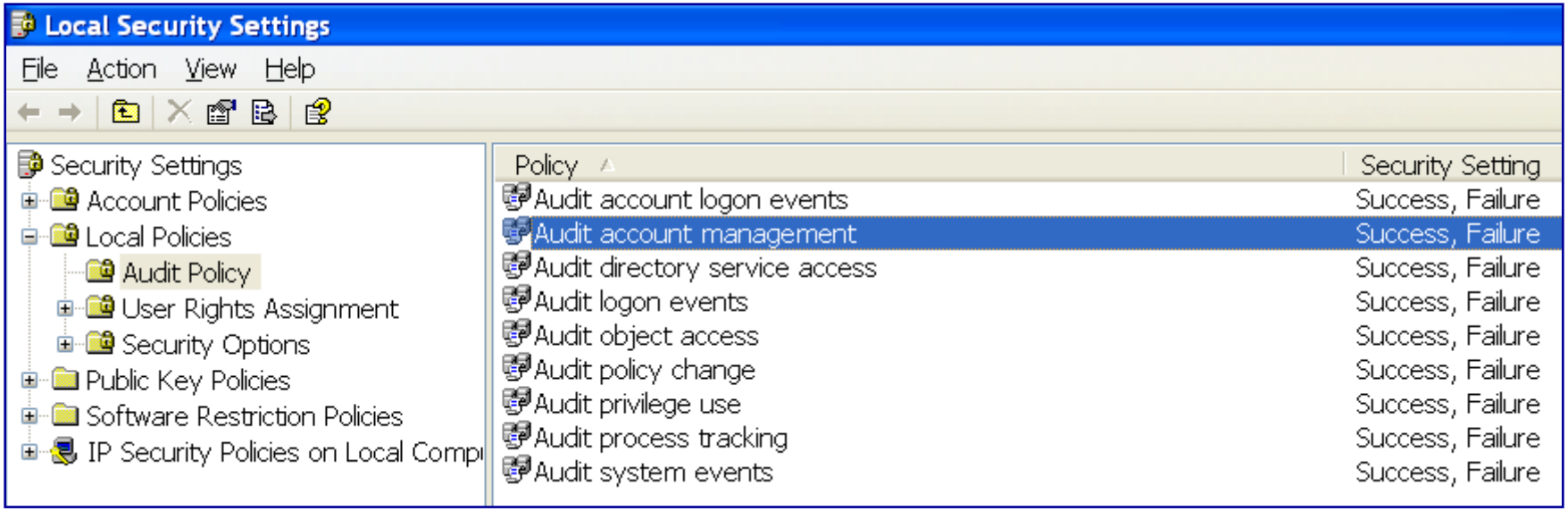


Users Accessing Files



Account Management

Audit Account Management



Events Map

			Created	Changed	Deleted	Member	
						Added	Removed
User			624	642	630	N/A	
Computer			645	646	647		
Groups	Security	Local	635	641	638	636	637
		Global	631	639	634	632	633
		Universal	658	659	662	660	661
	Distribution	Local	648	649	652	650	651
		Global	653	654	657	655	656
		Universal	663	664	667	665	666

* Credits: The Windows Server 2003 Security Log Revealed by Randy F. Smith

Reports

User Account Management

User	Operation	Details	by Whom	on Host	When
emustermann	User Account Created		Administrator	HOST1	Jul 30 2008 13:35:49
	User Account Changed	Password Last Set=7/30/2008 1:35:51 PM	Administrator	HOST1	Jul 30 2008 13:35:51
	User Account Changed	Old UAC Value=0x15|New UAC Value=0x11|User Account Control='Password Not Required' - Disabled	Administrator	HOST1	Jul 30 2008 13:35:51
	User Account Changed	Old UAC Value=0x11|New UAC Value=0x10|User Account Control=Account Enabled	Administrator	HOST1	Jul 30 2008 13:35:51
palmoni	User Account Changed	Password Last Set=7/30/2008 2:26:47 PM	Administrator	HOST1	Jul 30 2008 14:26:48

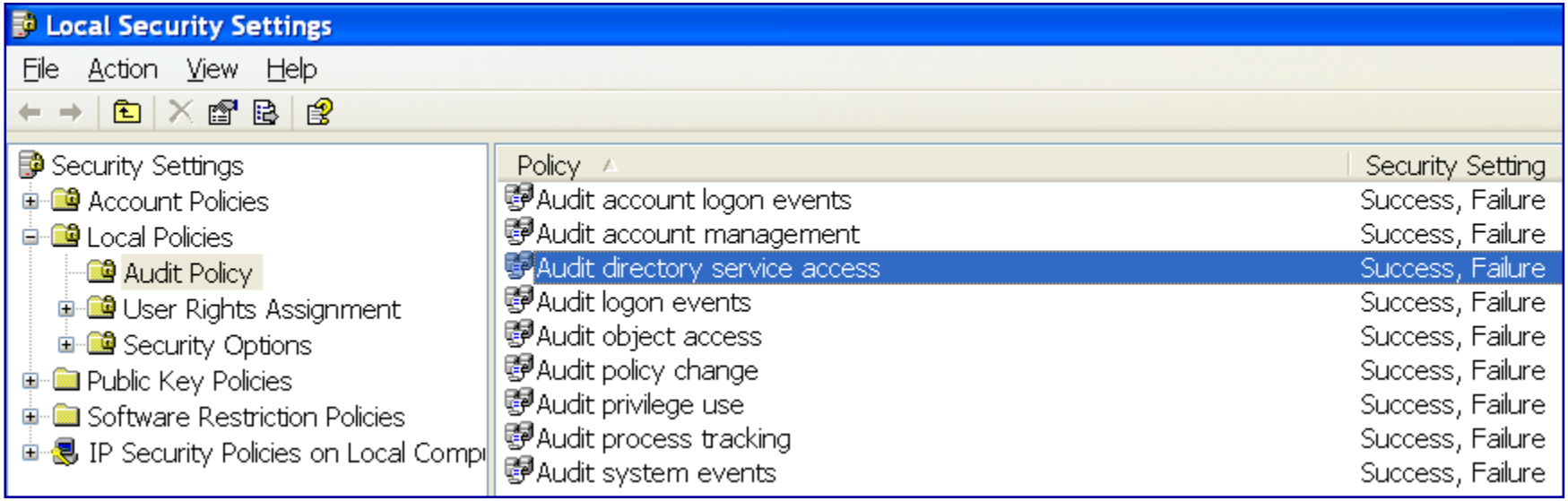
Group Account Management

Group	Operation	Subject	by Whom	on Host	When
Domain Admins	Security Enabled Global Group Member Added	cn=Erika Mustermann,OU=Server,OU=Development,DC=testDomain,DC=local	Administrator	HOST1	Jul 30 2008 13:51:02
Managers	Security Disabled Global Group Created		Administrator	HOST1	Jul 30 2008 14:05:58
	Security Disabled Global Group Member Added	TESTDOMAIN\palmoni	Administrator	HOST1	Jul 30 2008 14:06:24
Remote Desktop Users	Security Enabled Local Group Member Added	TESTDOMAIN\palmoni	Administrator	HOST1	Jul 30 2008 13:51:51
Solution	Security Enabled Global Group Member Added	cn=Erika Mustermann,OU=Server,OU=Development,DC=testDomain,DC=local	Administrator	HOST1	Jul 30 2008 13:52:20
	Security Enabled Global Group Member Added	cn=myServer,OU=Server,OU=Development,DC=testDomain,DC=local	Administrator	HOST1	Jul 30 2008 15:09:03
	Security Enabled Global Group Member Removed	TESTDOMAIN\emustermann	Administrator	HOST1	Jul 30 2008 15:15:43

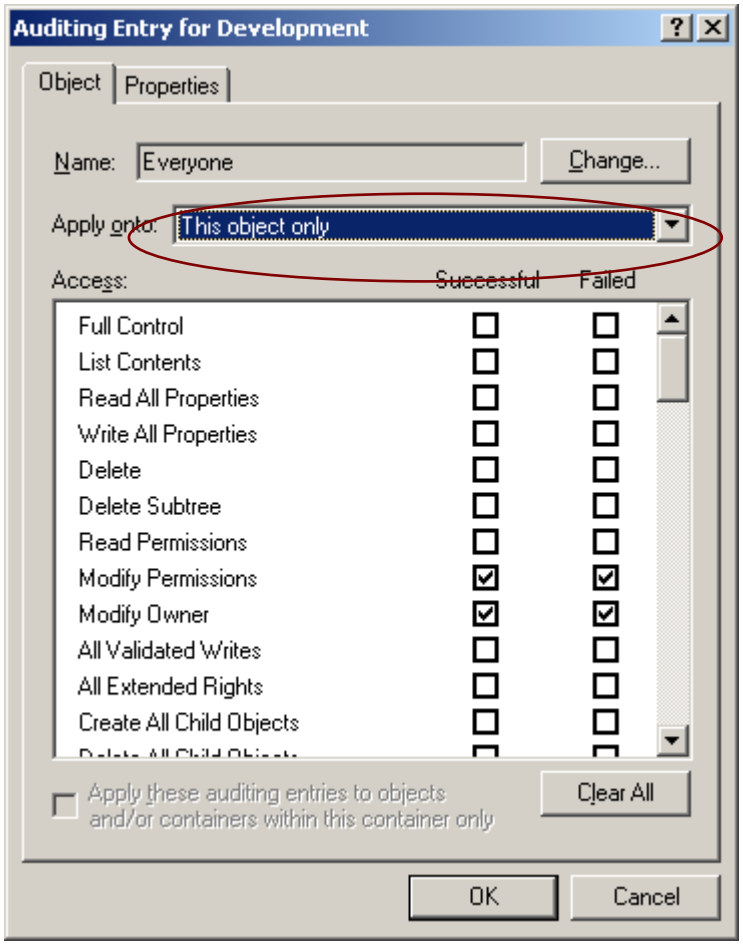
ArcSight™

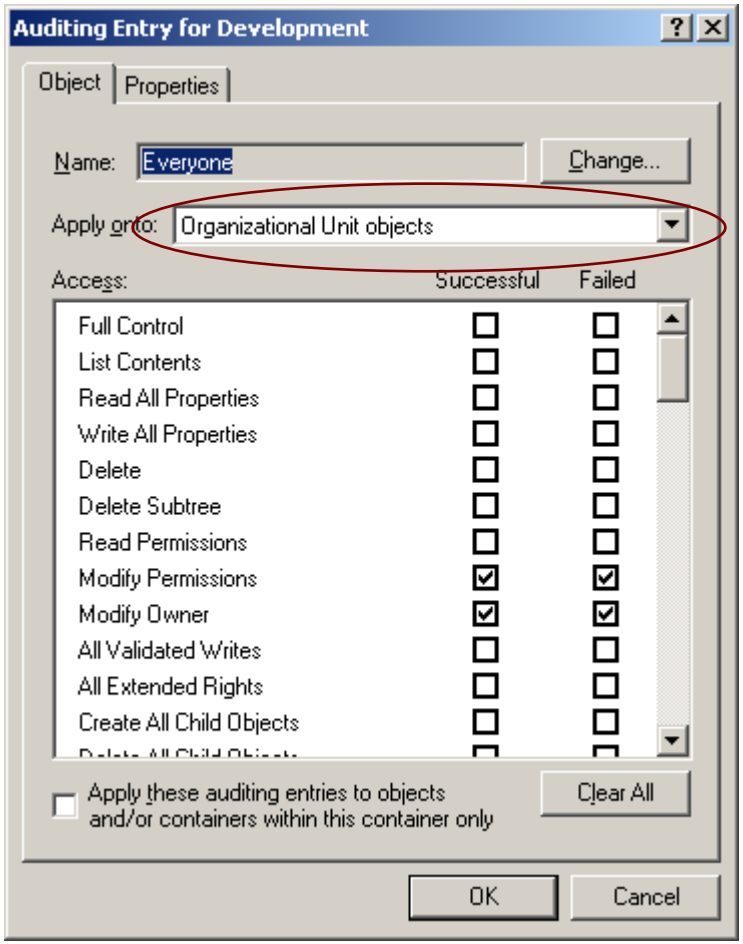
Directory Service Access

Audit Directory Service Access



Audit Configuration





Events

Event ID 565: Object Open

- Date: 6/26/2008
- Time: 12:59:17 PM
- Object Name: CN=Builtin,DC=testDomain,DC=local
- Handle ID: 52241736
- Process Name: C:\WINDOWS\system32\lsass.exe
- Primary User Name: HOST1$
- Primary Domain: TESTDOMAIN
- Primary Logon ID: (0x0,0x3E7)
- Client User Name: Administrator
- Client Domain: TESTDOMAIN
- Client Logon ID: (0x0,0x231F7)
- Accesses: DELETE READ_CONTROL WRITE_DAC WRITE_OWNER ReadPasswordParameters WritePasswordParameters ReadOtherParameters WriteOtherParameters CreateUser CreateGlobalGroup CreateLocalGroup GetLocalGroupMembership ListAccounts
- Properties:Domain Password & Lockout Policies lockOutObservationWindow lockoutDuration…

Event ID 566: Object Access

- Date: 7/31/2008
- Time: 5:13:25 PM
- User: TESTDOMAIN\Administrator
- Computer: HOST1
- Object Server: DS
- Object Type: organizationalUnit
- Object Name: OU=Domain Controllers,DC=testDomain,DC=local
- Primary User Name: HOST1$
- Primary Domain: TESTDOMAIN
- Primary Logon ID: (0x0,0x3E7)
- Client Logon ID: (0x0,0x1DFAD)
- Accesses: WRITE_DAC
- Properties:

  WRITE_DAC

  organizationalUnit

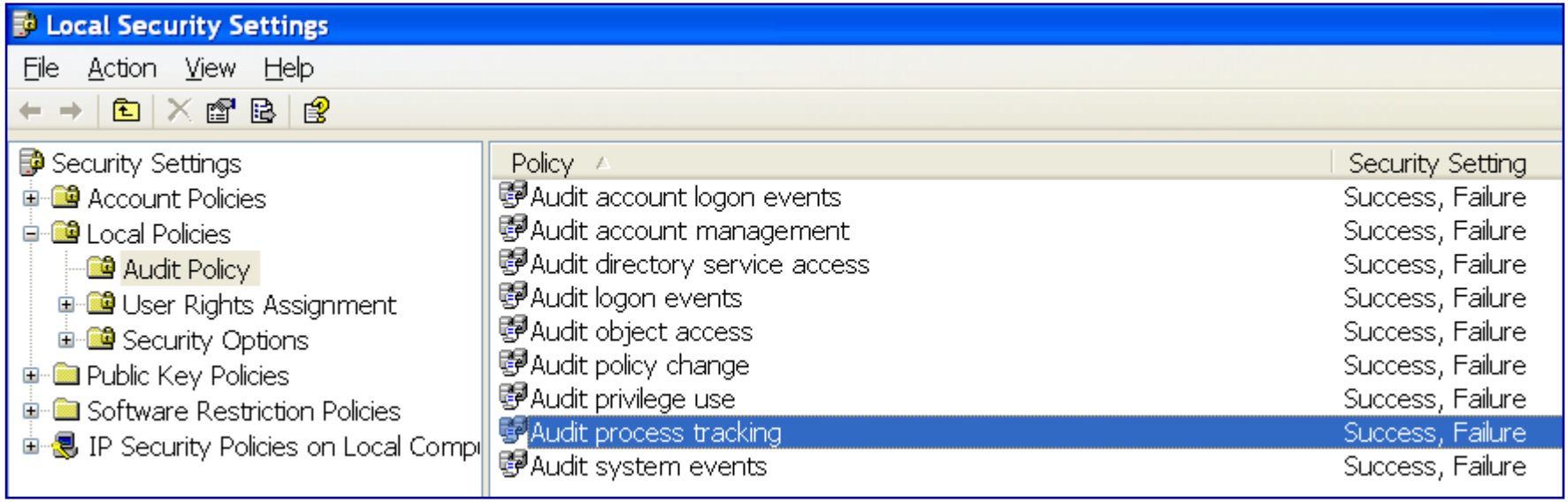
Report

Directory Object Access

User	Object Type	AD Object	Access	DC	When
Administrator	organizationalUnit	OU=Development,DC=testDomain,DC=local	WRITE_DAC	HOST1	Jul 31 2008 16:58:27
	organizationalUnit	OU=Domain Controllers,DC=testDomain,DC=local	WRITE_DAC	HOST1	Jul 31 2008 17:13:25
	group	CN=Managers,OU=Development,DC=testDomain,DC=local	Write Property	HOST1	Jul 31 2008 17:19:37
	groupPolicyContainer	CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=testDomain,DC=local	WRITE_DAC	HOST1	Aug 01 2008 10:32:09
	groupPolicyContainer	CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=testDomain,DC=local	WRITE_DAC	HOST1	Aug 01 2008 10:33:20
	groupPolicyContainer	CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=testDomain,DC=local	Write Property	HOST1	Aug 01 2008 10:37:58
	groupPolicyContainer	CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=testDomain,DC=local	Write Property	HOST1	Aug 01 2008 10:38:18

Process Tracking

Audit Process Tracking



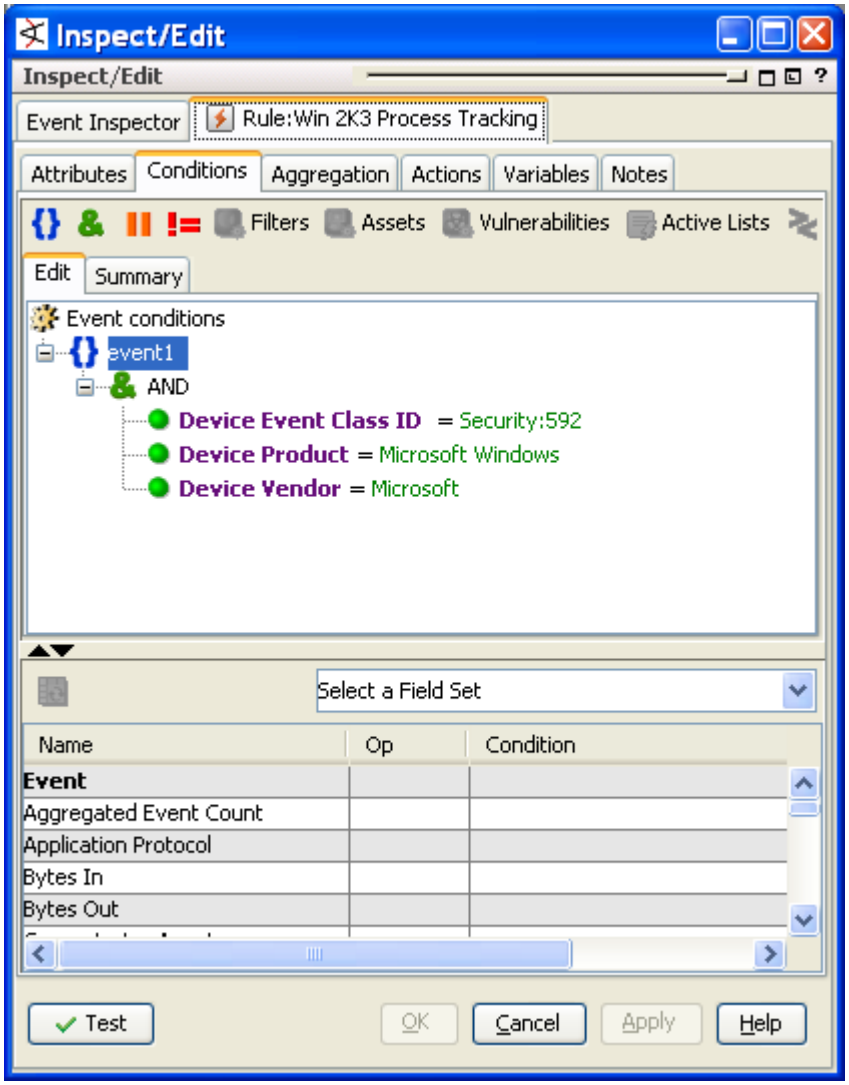
Event ID 592 – New Process Creation

Event ID 592: A new process has been created

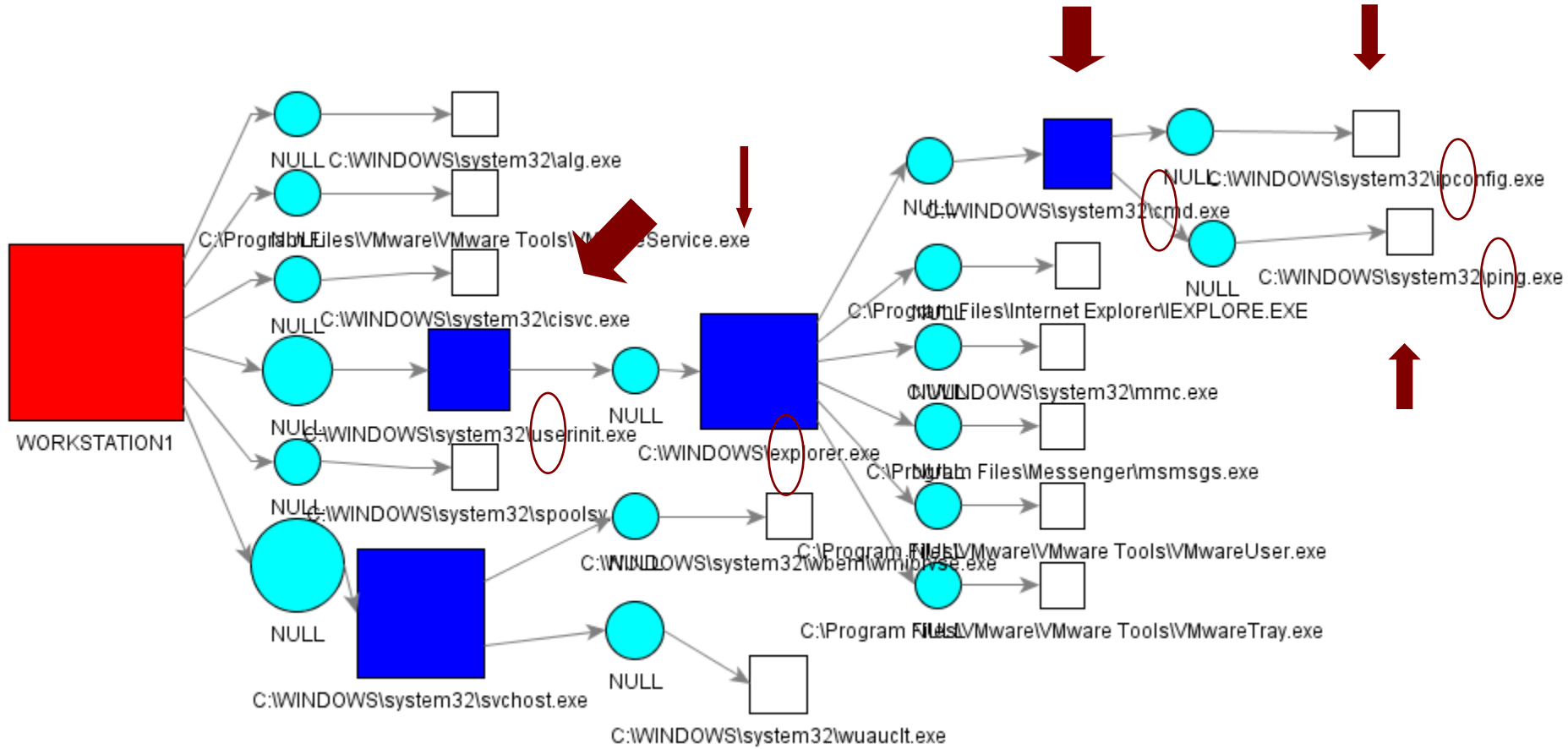
- Date: 8/7/2008
- Time: 5:56:17 PM
- Computer: NEWFILESERVER
- New Process ID: 1444
- Image File Name: C:\WINDOWS\system32\ping.exe
- Creator Process ID: 2088
- User Name: palmoni
- Domain: TESTDOMAIN
- Logon ID: (0x0,0x177293F)

Process ID	Process Name
2088	cmd.exe
1444	ping.exe

Rule Definition



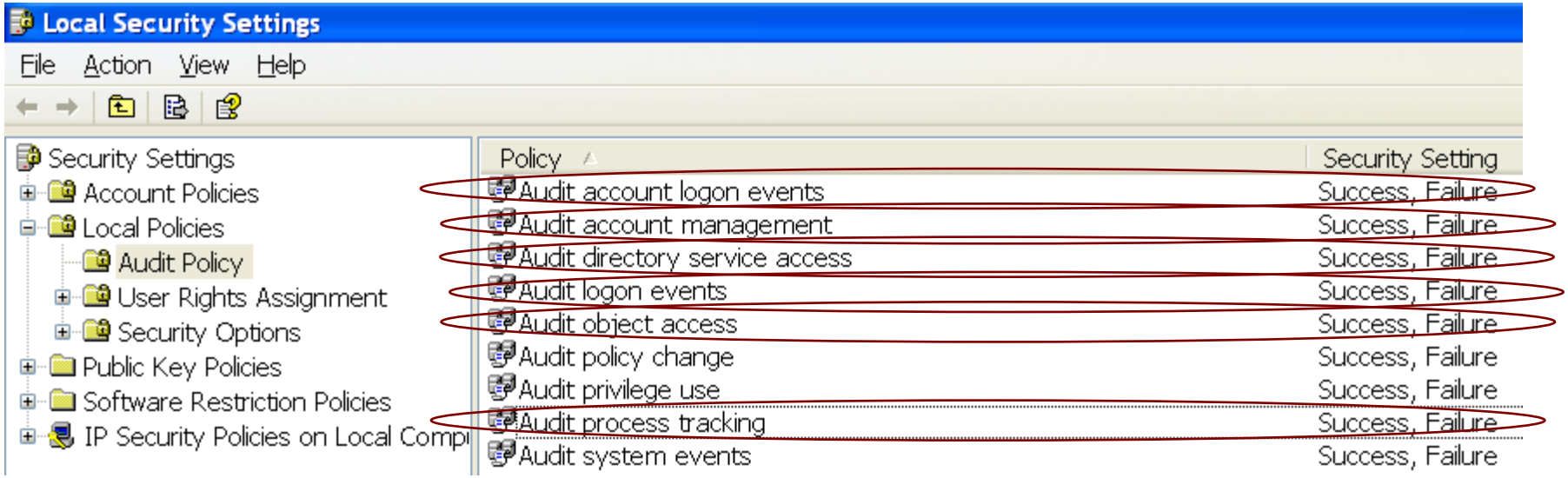
Process View Data Monitor



ArcSight™

Summary

Summary



Useful Resources

- www.ultimatewindowssecurity.com
- http://blogs.msdn.com/ericfitz/
- https://forum.arcsight.com/showthread.php?t=754&highlight=windows

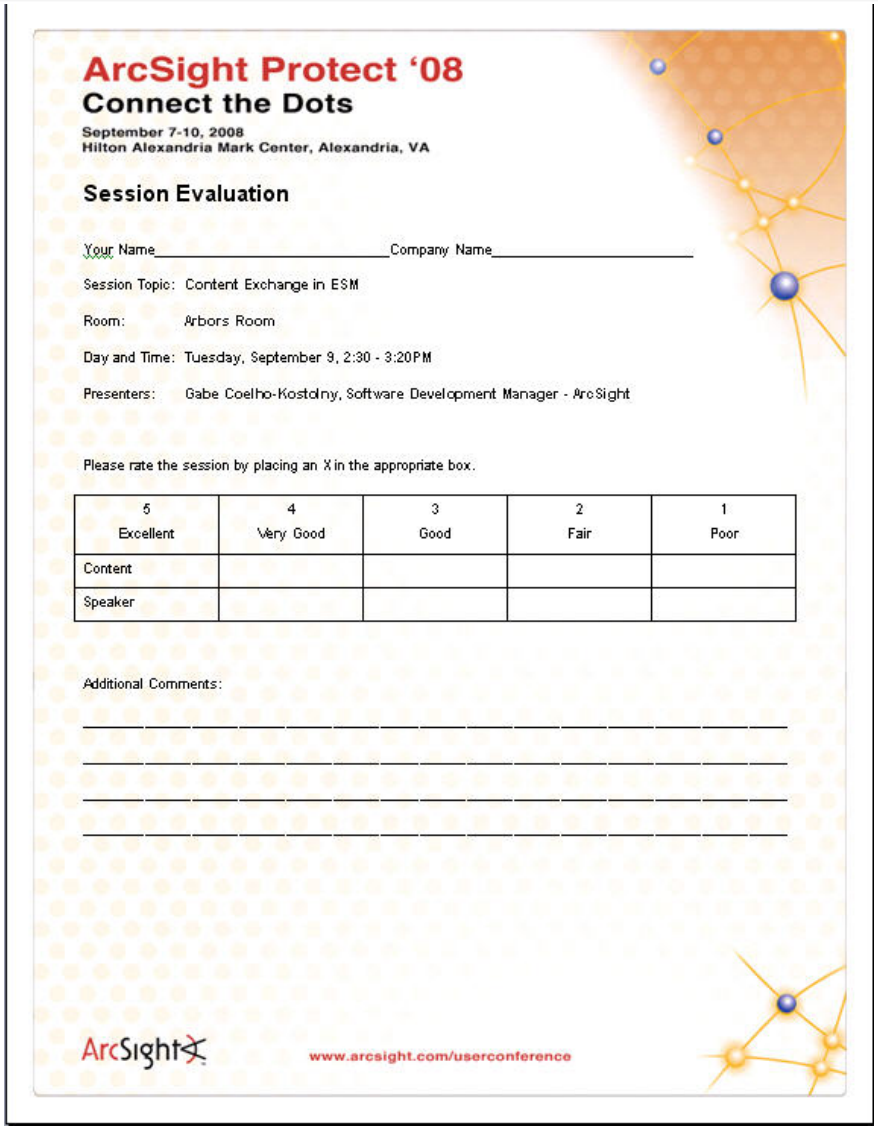
ArcSight™

For More Information

- **ArcSight Inc.**: www.arcsight.com
- **Webcasts**: www.arcsight.com/news_webinars.htm
- **Collateral**: www.arcsight.com/whitepapers.htm

Session Evaluation

Please take a moment
to fill out our
session evaluation



ArcSight Protect '08
Connect the Dots

September 7-10, 2008
Hilton Alexandria Mark Center, Alexandria, VA

Session Evaluation

Your Name_____Company Name_____

Session Topic: Content Exchange in ESM

Room: Arbors Room

Day and Time: Tuesday, September 9, 2:30 - 3:20PM

Presenters: Gabe Coelho-Kostolny, Software Development Manager - ArcSight

Please rate the session by placing an X in the appropriate box.

	5 Excellent	4 Very Good	3 Good	2 Fair	1 Poor
Content					
Speaker					

Additional Comments:

_____

_____

_____

_____

ArcSight www.arcsight.com/userconference