

General Daily WMI Statistics

mercredi septembre 7, 2005

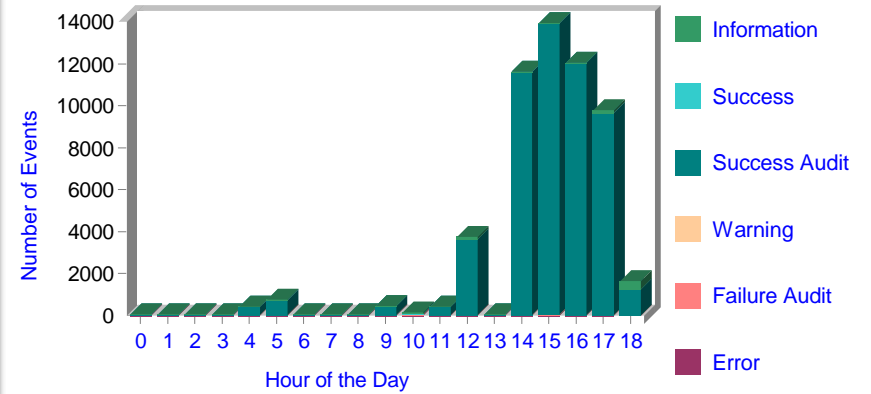
Log Activity for the Top 5 Users

User	Events
dataset\pascal	33 883
dataset\didier	17 735
autorite nt\system	3 346
dataset\administrateur	194
	158

Event Types of the Day

Event Type	Events
Success Audit	54 005
Information	728
Error	626
Failure Audit	82
Warning	35
Success	13

WMI Filtered Traffic - Hourly Activity



Top 5 Failed Logons by User

User	Event Name	Events
kiwi\pierre	Logon Failure: Reason: Unknown user name or bad	19

Top 5 Successful Logons and Logoffs by User

User	Event Name	Events
dataset\administrateur	User Logoff.	94
dataset\administrateur	Successful Network Logon.	92
autorite nt\anonymous logon	User Logoff.	83
dataset\luc	User Logoff.	4
dataset\luc	Successful Network Logon.	4

Number of Security Events by Category

Unused message ID	1 376
System Event	51
Logon/Logoff	323
Object Access	52 015
Privilege Use	147
Detailed Tracking	1 501
Policy Change	1
Account Management	3
Directory Service Access	3
Account Logon	50

Other WMI Statistics

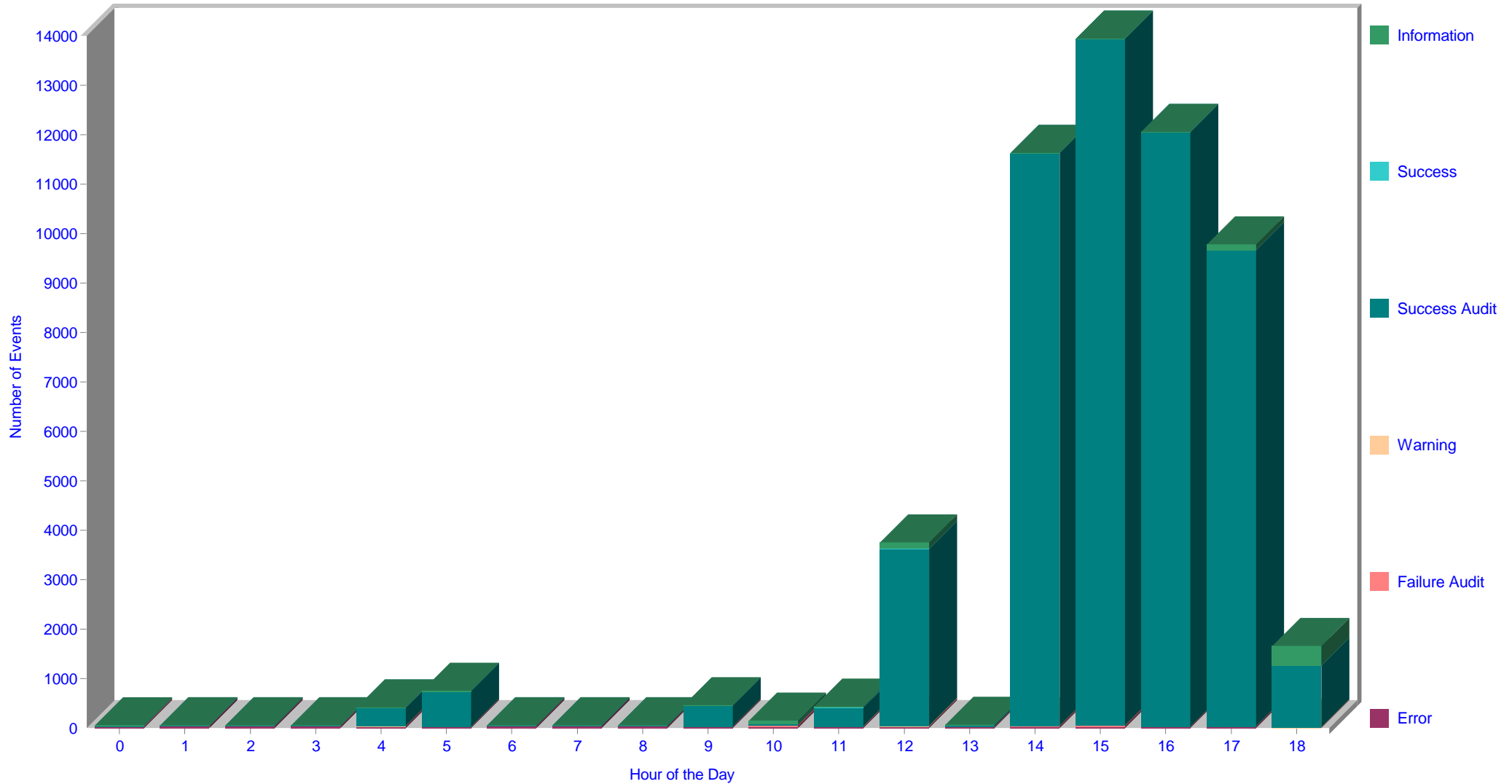
1 Security Log(s) have been cleared by 1 User(s) on 1 Computer(s).
 12 Services have been started or stopped 31 times by 3 User(s) on 2 Computer(s).
 The user: dataset\pascal has accessed 1332 files or directories 16771 times on 1 Computer(s).
 The file or directory: E:\mydev32\NetReport\NetReport\Setup\NRWZConfig has been accessed 3739 times by 1 User(s) on 1 Computer(s).

Log File Activity

Log File	Events
Security	54 092
Application	703
System	702



Event Types by Hour of the Day





Log Activity by Hour - Data

mercredi septembre 7, 2005



Hour		Error	Failure Audit	Warning	Success Audit	Success	Information	Total Events	Events %
00:00		33		1	16		3	53	0,10%
01:00		40			13		2	55	0,10%
02:00		40		2	17		2	61	0,11%
03:00		40		1	15			56	0,10%
04:00		42		2	371	1		416	0,75%
05:00		32		1	712	2	6	753	1,36%
06:00		40		1	15			56	0,10%
07:00		41			15			56	0,10%
08:00		36		1	17			54	0,10%
09:00		30			427		2	459	0,83%
10:00		30	33	1	34		56	154	0,28%
11:00		30		6	381	3	16	436	0,79%
12:00		33		10	3 584	5	127	3 759	6,78%
13:00		30		1	28		6	65	0,12%
14:00		30	13	1	11 587		3	11 634	21,00%
15:00		30	30	1	13 883		2	13 946	25,17%
16:00		28			12 030		2	12 060	21,76%
17:00		28	6	4	9 603	1	112	9 754	17,60%
18:00		13		2	1 208	1	362	1 586	2,86%
Total for mercredi septembre 7, 2005		626	82	35	53 956	13	701	55 413	100,00%



Cleared Security Log Audit Events

mercredi septembre 7, 2005



Date and Time	Computer Name	User
07/09/2005 11:22:28	127.0.0.1	dataset\didier
Total Number of Events for the Above List:		1



Log Activity for the Top 30 Active Users

mercredi septembre 7, 2005







User	Error	Failure Audit	Warning	Success Audit	Success	Information	Total Events	Events %
dataset\pascal				33 866			33 866	61,11%
dataset\didier				17 702		14	17 716	31,97%
autorite nt\system	619	49	16	2 095		548	3 327	6,00%
dataset\administrateur				194			194	0,35%
	7		19		13	118	157	0,28%
autorite nt\anonymous logon				83			83	0,15%
dataset\luc		33		12		1	46	0,08%
dataset\vero						23	23	0,04%
skipper\iusr_test1				5			5	0,01%
skipper__vmware_user__				2			2	0,00%
Total for the above User list:	626	82	35	53 959	13	704	55 419	100,00%
Total for all Users:	626	82	35	54 030	13	741	55 527	100,00%



Top 30 Successful Logons and Logoffs

mercredi septembre 7, 2005



User	Computer Name	Event ID	Event Name	Logon Type	Logon Type Description	Events
 						
dataset\administrateur	patate	538	User Logoff.	3	Network logon	94
dataset\administrateur	patate	540	Successful Network Logon.	3	Network logon	92
autorite n\anonymous logon	patate	538	User Logoff.	3	Network logon	79
autorite n\anonymous logon	127.0.0.1	538	User Logoff.	3	Network logon	4
dataset\luc	127.0.0.1	538	User Logoff.	3	Network logon	4
dataset\luc	127.0.0.1	540	Successful Network Logon.	3	Network logon	4
dataset\pascal	patate	528	Successful Logon.	4	Batch logon	2
dataset\pascal	patate	538	User Logoff.	4	Batch logon	2
skipper\iusr_test1	127.0.0.1	540	Successful Network Logon.	3	Network logon	2
dataset\didier	127.0.0.1	528	Successful Logon.	2	Console logon	1
dataset\didier	127.0.0.1	528	Successful Logon.	5	Service logon	1
dataset\didier	127.0.0.1	538	User Logoff.	5	Service logon	1
dataset\pascal	patate	528	Successful Logon.	7	Unlock Workstation	1
dataset\pascal	patate	538	User Logoff.	7	Unlock Workstation	1
skipper_vmware_user__	127.0.0.1	528	Successful Logon.	2	Console logon	1
skipper\iusr_test1	127.0.0.1	538	User Logoff.	3	Network logon	1

Total Successful Logons and Logoffs for the Above User List:





290



Top 30 Failed Logons

mercredi septembre 7, 2005



User	Computer Name	Event ID	Event Name	Logon Type	Logon Type Description	Number of Events	Events %
 							
kiwi\pierre	127.0.0.1	529	Logon Failure: Reason: Unknown user name or bad password	3	Network logon	18	94,74%
kiwi\pierre	patate	529	Logon Failure: Reason: Unknown user name or bad password	3	Network logon	1	5,26%
Total Number of Failed Events for the Above User List:						19	100,00%



All Stopped and Started Services by User

mercredi septembre 7, 2005



Date and Time	User	Computer Name	Service Name	Status
07/09/2005 10:01:04	autorite nt\system	bouzigues	service de transfert intelligent en arrière-plan	Démarrer
07/09/2005 10:01:05	datasetluc	bouzigues	gestionnaire de connexions d'accès distant	Démarrer
07/09/2005 10:01:06	autorite nt\system	bouzigues	service com de gravage de cd imapi	Démarrer
07/09/2005 10:01:07	autorite nt\system	bouzigues	connexions réseau	Démarrer
07/09/2005 10:01:09	autorite nt\system	bouzigues	service de découvertes sssdp	Démarrer
07/09/2005 10:01:15	autorite nt\system	bouzigues	nla (network location awareness)	Démarrer
07/09/2005 11:02:45	autorite nt\system	bouzigues	application système com+	Démarrer
07/09/2005 11:02:45	autorite nt\system	bouzigues	distributed transaction coordinator	Démarrer
07/09/2005 18:08:05	datasetvero	carambole	netreport xml remote configuration service	Arrêter
07/09/2005 18:08:07	datasetvero	carambole	netreport filter engine	Arrêter
07/09/2005 18:08:27	datasetvero	carambole	netreport radius agent	Arrêter
07/09/2005 18:08:30	datasetvero	carambole	netreport performance counters manager	Arrêter
07/09/2005 18:08:44	datasetvero	carambole	netreport performance counters manager	Démarrer
07/09/2005 18:08:46	datasetvero	carambole	netreport xml remote configuration service	Démarrer
07/09/2005 18:08:48	datasetvero	carambole	netreport filter engine	Démarrer
07/09/2005 18:08:52	datasetvero	carambole	netreport radius agent	Démarrer
07/09/2005 18:12:38	datasetvero	carambole	netreport xml remote configuration service	Arrêter
07/09/2005 18:12:40	datasetvero	carambole	netreport filter engine	Arrêter
07/09/2005 18:13:01	datasetvero	carambole	netreport radius agent	Arrêter
07/09/2005 18:13:03	datasetvero	carambole	netreport performance counters manager	Arrêter
07/09/2005 18:13:21	datasetvero	carambole	netreport performance counters manager	Démarrer
07/09/2005 18:13:23	datasetvero	carambole	netreport xml remote configuration service	Démarrer
07/09/2005 18:13:25	datasetvero	carambole	netreport filter engine	Démarrer
07/09/2005 18:13:29	datasetvero	carambole	netreport radius agent	Démarrer
07/09/2005 18:17:39	datasetvero	carambole	netreport xml remote configuration service	Arrêter
07/09/2005 18:17:41	datasetvero	carambole	netreport filter engine	Arrêter



All Stopped and Started Services by User

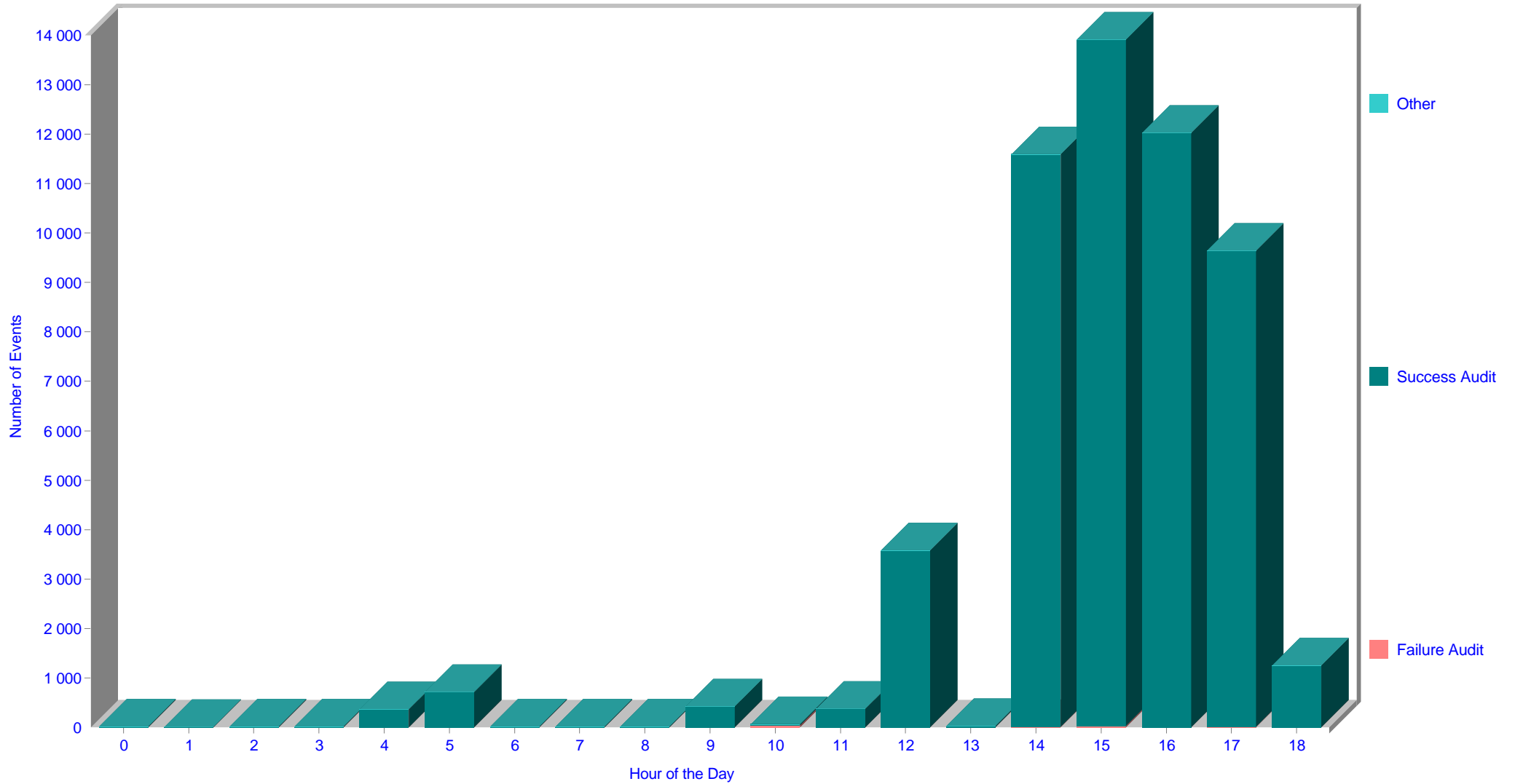
mercredi septembre 7, 2005



Date and Time	User	Computer Name	Service Name	Status
07/09/2005 18:18:01	datasetvero	carambole	netreport radius agent	Arrêter
07/09/2005 18:18:04	datasetvero	carambole	netreport performance counters manager	Arrêter
07/09/2005 18:19:10	datasetvero	carambole	netreport performance counters manager	Démarrer
07/09/2005 18:19:12	datasetvero	carambole	netreport xml remote configuration service	Démarrer
07/09/2005 18:19:14	datasetvero	carambole	netreport filter engine	Démarrer
Total Number of Events for the Above List:		31		



Security Log Activity by Hour of the Day





Security Log Activity for the Top 30 Active Users

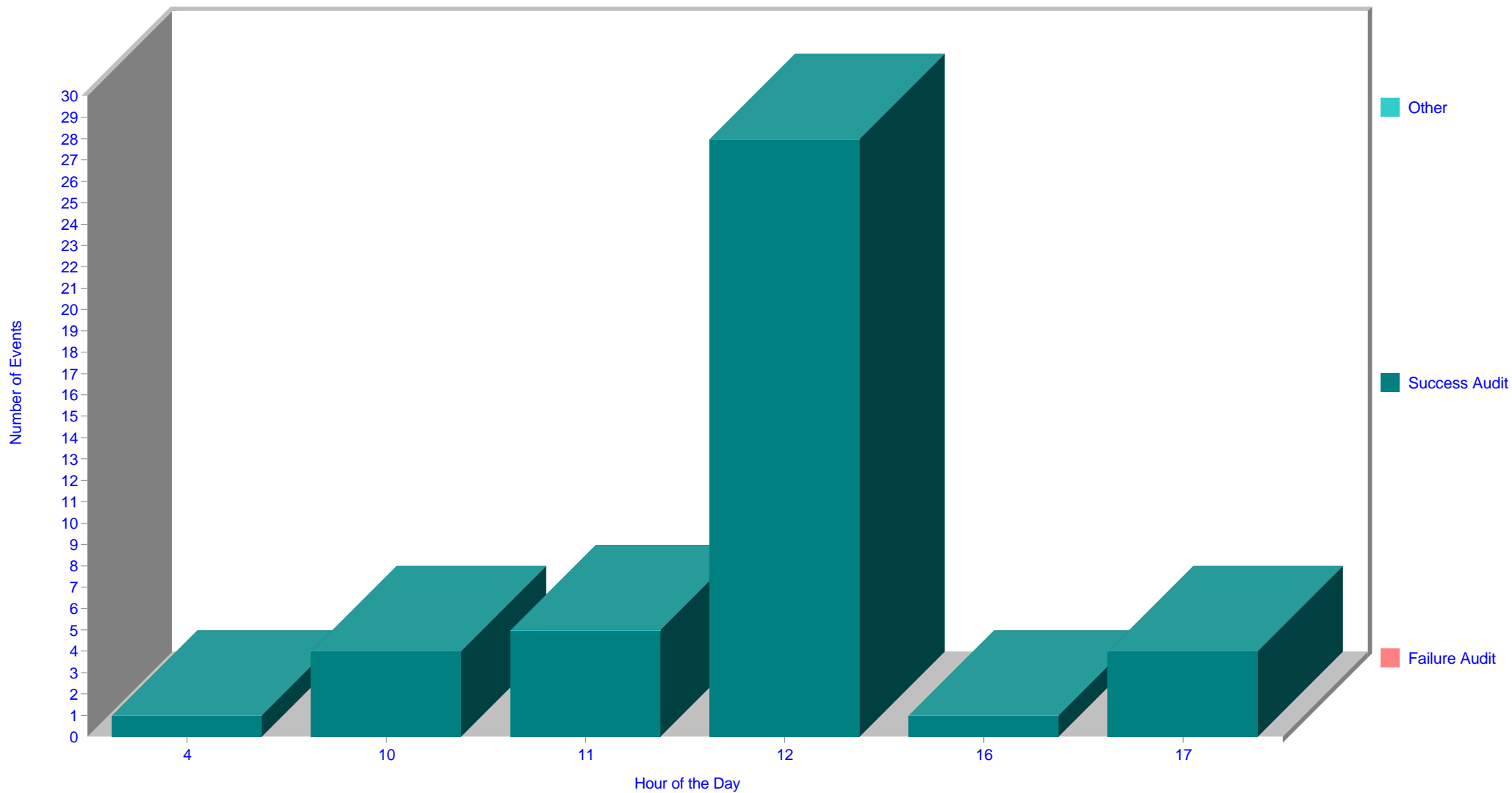
mercredi septembre 7, 2005



User	Failure Audit	Failure Audit %	Success Audit	Success Audit %	Other	Other %	Total Events	Total Events %
dataset\pascal			33 871	62,76%			33 871	62,66%
dataset\didier			17 709	32,81%			17 709	32,76%
autorite nt\system	49	59,76%	2 095	3,88%			2 144	3,97%
dataset\administrateur			194	0,36%			194	0,36%
autorite nt\anonymous logon			83	0,15%			83	0,15%
dataset\luc	33	40,24%	12	0,02%			45	0,08%
skipper\iusr_test1			5	0,01%			5	0,01%
skipper__vmware_user__			2	0,00%			2	0,00%
Total for mercredi 7 septembre 2005	82	100,00%	53 971	100,00%			54 053	100,00%



Security System Event Activity by Hour of the Day





Security System Event Activity for the Top 30 Active Users

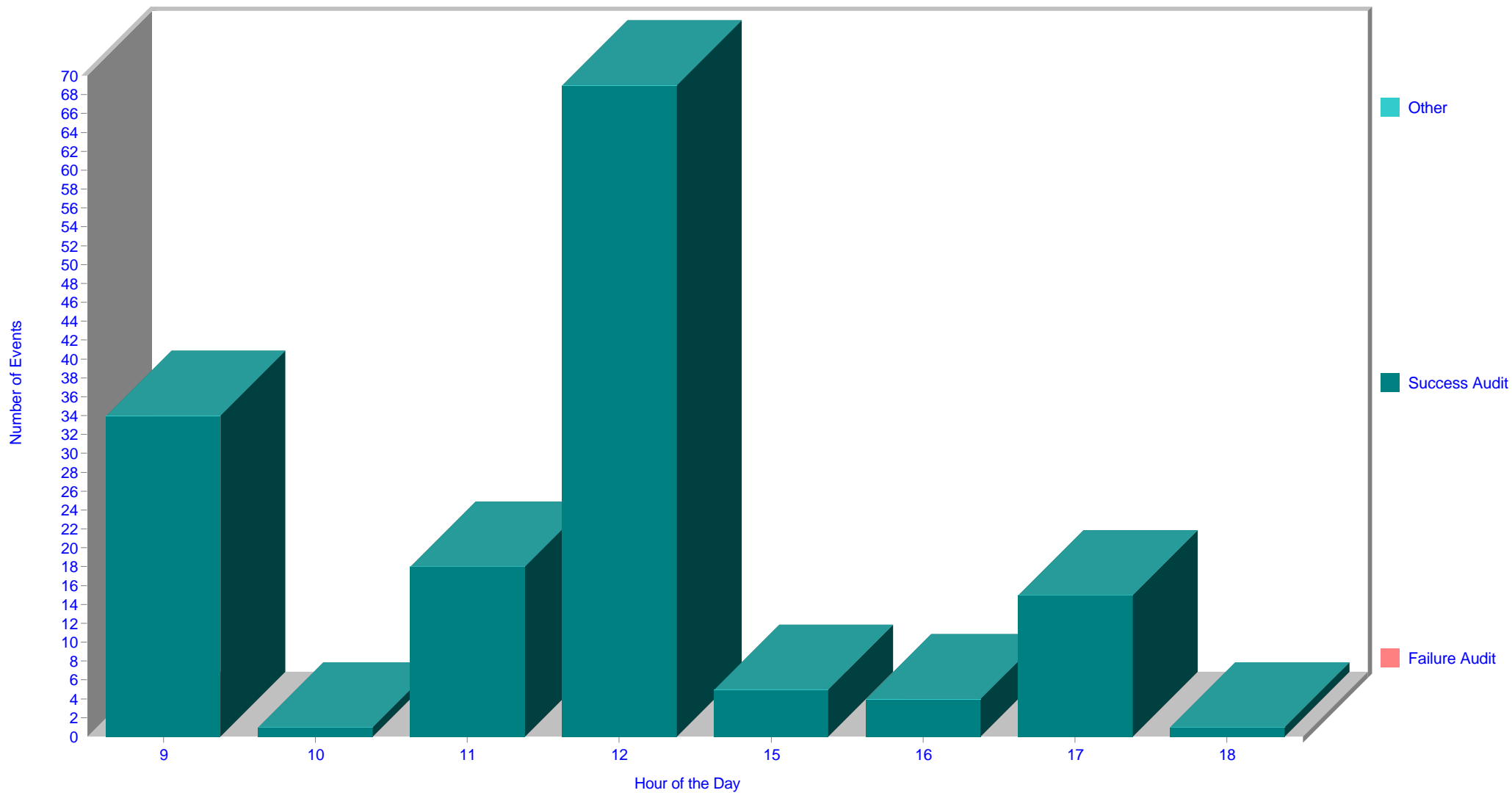
mercredi septembre 7, 2005



User	Failure Audit	Failure Audit %	Success Audit	Success Audit %	Other	Other %	Total Events	Total Events %
autorite nt\system			43	100,00%			43	100,00%
Total for mercredi 7 septembre 2005			43	100,00%			43	100,00%



Security Privilege Use Activity by Hour of the Day





Security Privilege Use Activity for the Top 30 Active Users

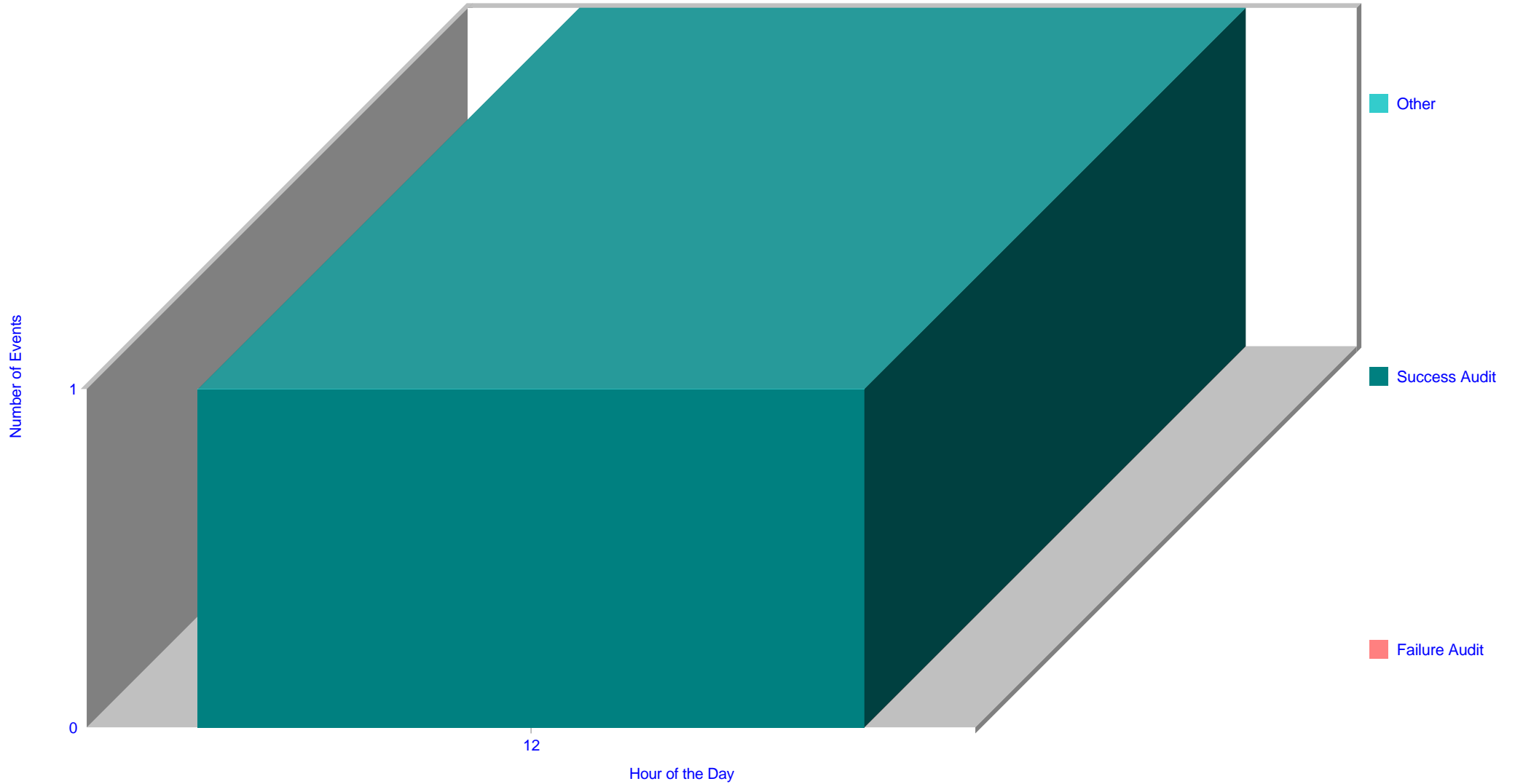
mercredi septembre 7, 2005



User	Failure Audit	Failure Audit %	Success Audit	Success Audit %	Other	Other %	Total Events	Total Events %
datasetdidier			114	77,55%			114	77,55%
autorite nt\system			26	17,69%			26	17,69%
datasetluc			4	2,72%			4	2,72%
skipperiusr_test1			2	1,36%			2	1,36%
skipper__vmware_user__			1	0,68%			1	0,68%
Total for mercredi 7 septembre 2005			147	100,00%			147	100,00%



Security Policy Change Activity by Hour of the Day





Security Policy Change Activity for the Top 30 Active Users

mercredi septembre 7, 2005



User	Failure Audit	Failure Audit %	Success Audit	Success Audit %	Other	Other %	Total Events	Total Events %
autorite nt\system			1	100,00%			1	100,00%
Total for mercredi 7 septembre 2005			1	100,00%			1	100,00%



List of All Security Account Management Changes

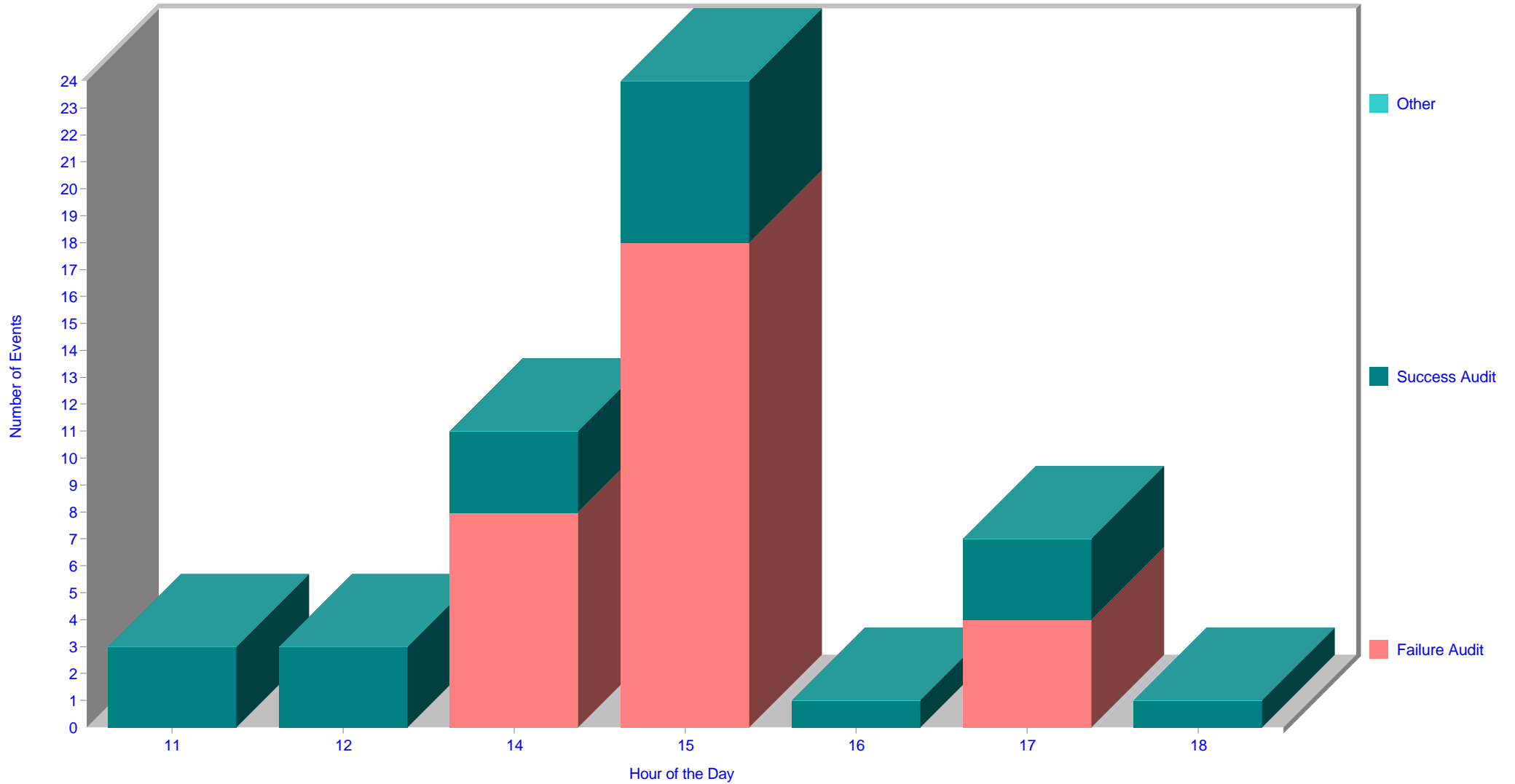
mercredi septembre 7, 2005



Date and Time	User	Computer Name	Event ID	Event Name	Event Type
07/09/2005 10:03:07	dataset\skipper\$	127.0.0.1	627	Change Password Attempt.	Success
07/09/2005 12:18:47	dataset\skipper\$	127.0.0.1	628	User Account password set.	Success
07/09/2005 12:18:47	dataset\skipper\$	127.0.0.1	642	User Account Changed.	Success
Total Number of Events for the Above User List:		3			



Security Account Logon Activity by Hour of the Day





Security Account Logon Activity for the Top 30 Active Users

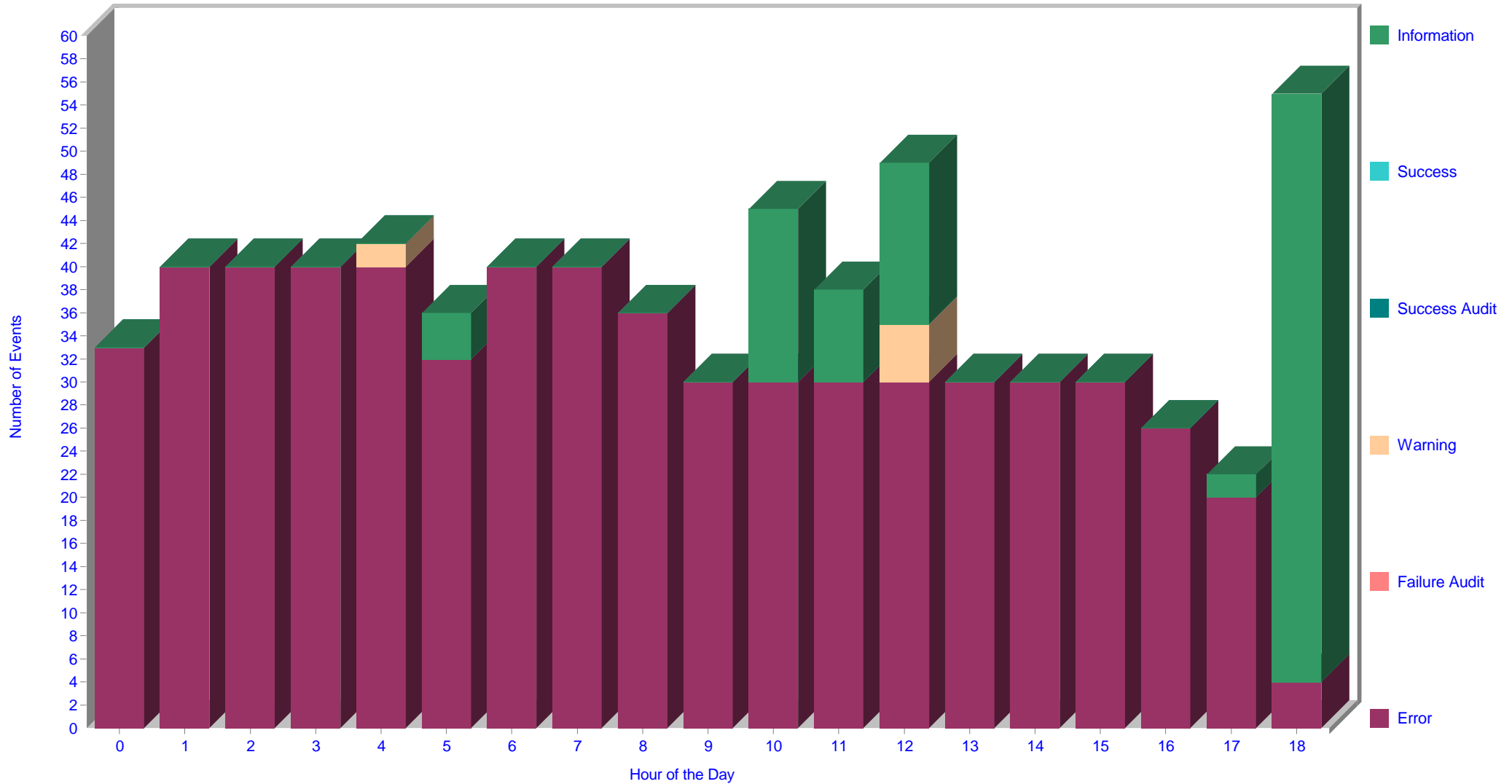
mercredi septembre 7, 2005



User	Failure Audit	Failure Audit %	Success Audit	Success Audit %	Other	Other %	Total Events	Total Events %
autorite nt\system	30	100,00%	20	100,00%			50	100,00%
Total for mercredi 7 septembre 2005	30	100,00%	20	100,00%			50	100,00%



Event Types by Hour of the Day





System Log Activity for the Top 30 Active Users

mercredi septembre 7, 2005



User	Error	Failure Audit	Warning	Success Audit	Success	Information	Total Events	Events %
autorite nt\system	601		7			11	612	87,18%
datasetvero						45	52	7,41%
datasetdidier						23	23	3,28%
datasetluc						14	14	1,99%
datasetluc						1	1	0,14%
Total for mercredi 7 septembre 2005	601		7			94	702	100,00%



Top 5 Users with their Top 5 Accessed Files or Directories

mercredi septembre 7, 2005








User	File or Directory	Successful Access	Failed Access	Total Access Attempts
dataset\pascal		16 766		16 766
	E:\mydev32\NetReport\NetReport\Setup\NRWZConfig	3 739		3 739
	E:\mydev32\NetReport\NetReport\Setup\NRWZConfig\Debug	1 679		1 679
	E:\mydev32\NetReport\NetReport\Setup\NRWZConfig\NRWZConfig.clw	1 171		1 171
	E:\mydev32\NetReport\NetReport\Distribution\ULA\Engine\NRFilterEngine\NRFilterEngineDLL	971		971
	E:\mydev32\NetReport\NetReport\Distribution\ULA\Engine\NRFilterEngine	252		252
dataset\didier		7 504		7 504
	C:\Program Files\NetReport\WebPortal\Runtime_Projects	3 085		3 085
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\WMI_3D.png	253		253
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\company_logo.gif	222		222
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\Body_Dashboard.PNG	140		140
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\WMI_User_077_057_2d.png	138		138
autorite nt\system		825		825
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\company_logo.gif	59		59
	\Device\HarddiskVolume3\NRWZConfig	57		57
	C:\Program Files\NetReport\WebPortal\Runtime_Projects	50		50
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\Body_Dashboard.PNG	50		50
	C:\Program Files\NetReport\WebPortal\Runtime_Projects\Sort_Descending.png	49		49
Total for the Above User List:		25 095		25 095



Top 5 Accessed Files or Directories with their Top 5 Users

mercredi septembre 7, 2005



File or Directory	User	Successful Access	Failed Access	Total Access Attempts
 				
E:\mydev32\NetReport\NetReport\Setup\NRWZConfig		3 739		3 739
dataset\pascal		3 739		3 739
C:\Program Files\NetReport\WebPortal\Runtime_Projects		3 135		3 135
dataset\didier		3 085		3 085
autorite nt\system		50		50
E:\mydev32\NetReport\NetReport\Setup\NRWZConfig\Debug		1 679		1 679
dataset\pascal		1 679		1 679
E:\mydev32\NetReport\NetReport\Setup\NRWZConfig\NRWZConfig.clw		1 171		1 171
dataset\pascal		1 171		1 171
E:\mydev32\NetReport\NetReport\Distribution\ULA\Engine\NRFilterEngine\NRFilterEngineDLL		971		971
dataset\pascal		971		971
Total for the Above User List:		10 695		10 695