Logging and Audit

Intro to log management and audit strategies

Stefan Kelm, DFN-CERT Services GmbH
WP8-T1

5 August 2020

Public

www.geant.org

Logging is fairly simple, isn't it?

```
Jul 04 14:10:59 shadow su:(to root) jones on /dev/pts2
```

Logging is fairly simple, isn't it?

- No, it isn't…
  - No standard format
  - No standard transport
  - No guidance on what to log and how
  - No guidance for developers

- **But you have to do it!**

Definitions / Terminology

- In general
  - **Logging** is commonly referred to as the act of keeping a log, a recording of **events** as well as the storage and analysis of these events
  - The **purpose of logging** is to have a record of events that happened in order to resolve
    - Errors / safety issues / security incidents / …

- From NIST (National Institute of Standards and Technology)
  - *"A **log** is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each **entry** contains information related to a specific **event** that has occurred within a system or network."*
  - *"**Log managament** is […] the process for generating, transmitting, storing, analysing, and disposing of log data."*

Logs, where art thou?

- Logs are everywhere
  - Operating systems
    - Linux Syslog, Windows Event Log, …
  - Server logs (HTTP, SMTP, SNMP, DNS, SQL, etc.) and many, many more…
    - Application logs were designed for troubleshooting/debugging, not investigating
  - Device logs
    - Routers, Switches, Firewalls, IDS, EDR, AV, …
    - Smartphones
    - Did anyone say “IoT”?

- All these logs will make our jobs easier, no?

Why is logging important?

- Logs assist us in
  - Detecting all things security
    - Intrusion Detection
    - Incident Containment and Response
    - Forensic Analysis / e-Discovery (“super timeline all the things”)
    - Real Time Alerting
  - Providing a Network Baseline
  - Determining the Health of the Network
    - Operational issues
    - Performance issues
  - Detecting policy breaches: Audit Trail
  - **Achieving**
    - **$$$ regulatory compliance** (GDPR, PCI DSS, ISO 27001, HIPAA, SOX, …) **$$$**
    - (Internal) policies **compliance**

Who wants logs?

- Who are typical log file users/consumers?
  - System and network administrators
  - Security administrators
  - Computer Security Incident Response Teams (CSIRT, CERT)
  - Application developers
  - Chief information security officers (CISO, CIO)
  - (External) auditors
  - Others in your org?

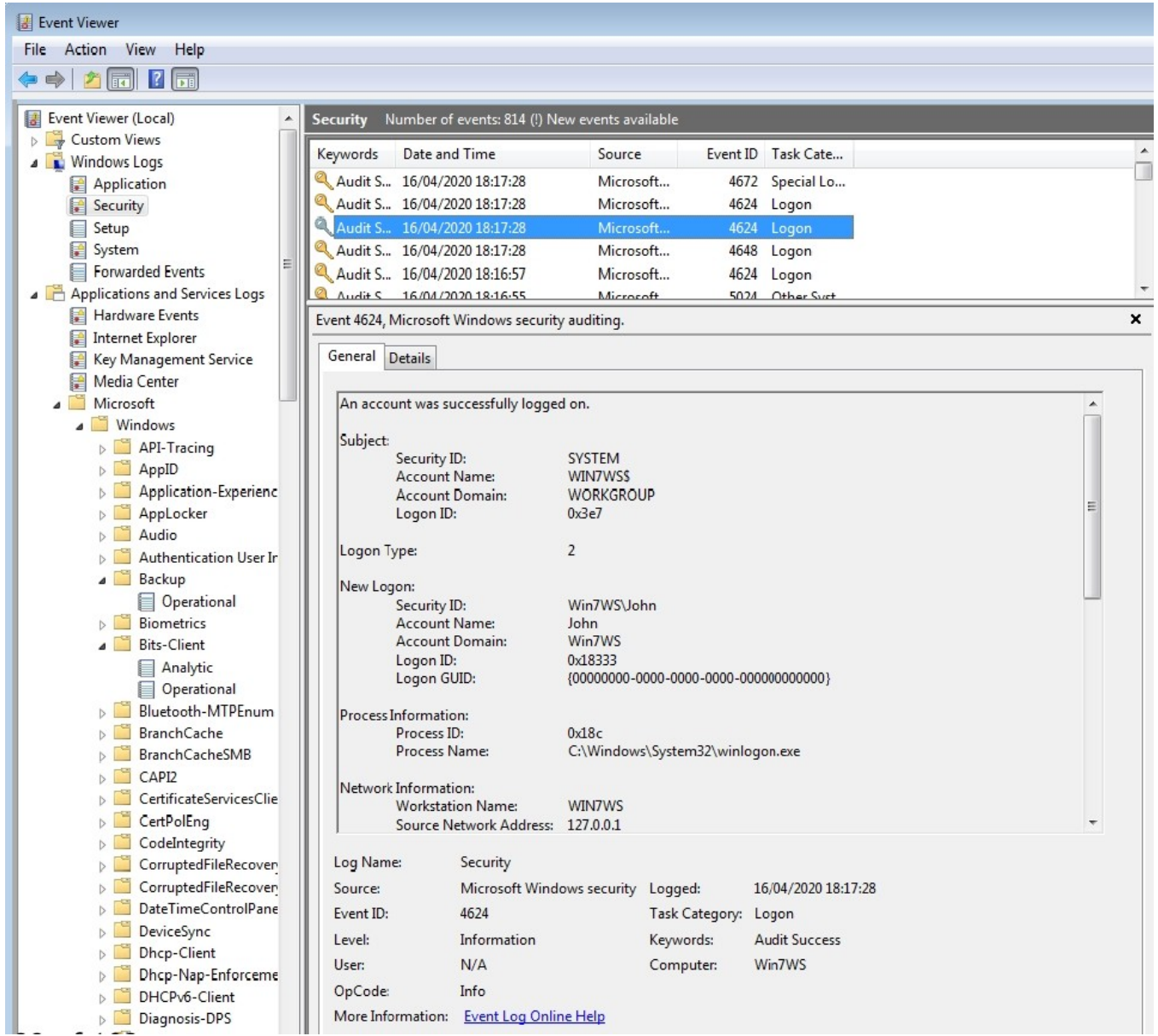
- Do all consumers want the same logs?
  - Do they all *need* the same logs?
  - Are they all *allowed* to look at the same logs?

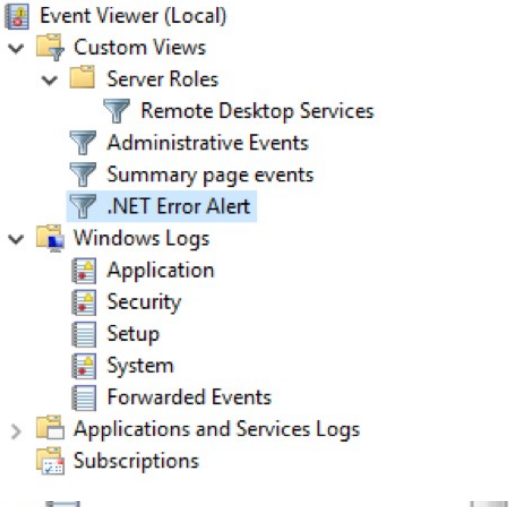
Let’s have a look…

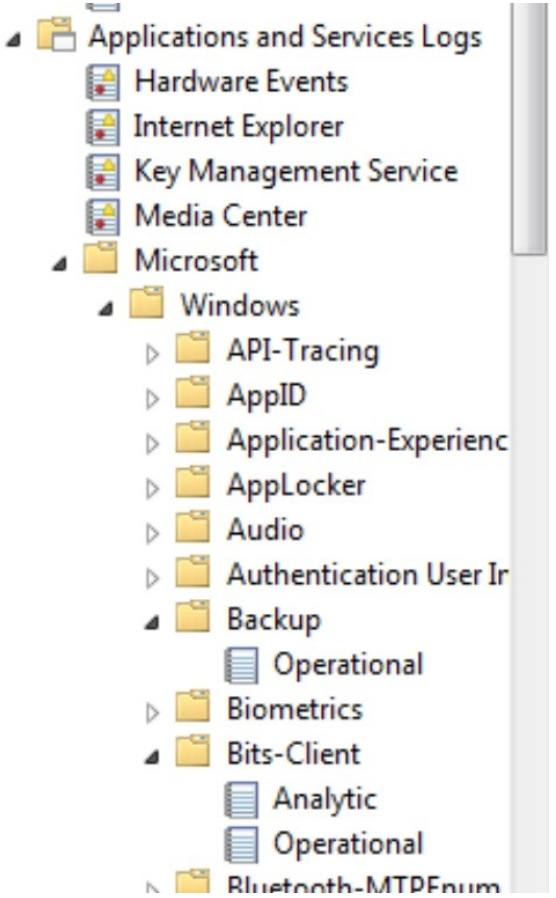
Windows Event Logs

- The dark ages (up to Windows XP)
  - Binary Event Log file format
  - Location: `%SystemRoot%\System32\Config`
  - Mainly 3 categories:
    - Security: `secevent.evt`
    - System: `sysevent.evt`
    - Application: `appevent.evt`
- Beginning with Vista
  - New binary XML format, new extension: `.evtx`
  - Location: `\Windows\System32\winevt\Logs\`
  - Many more files:
    - `Security.evtx`, `System.evtx`, `Application.evtx`
    - → 120 files ++

Example: logon event (Event Viewer)







What am I looking for? (=> check the Appendix for more)

	ID	Level	Event Log	Event Source
Account Lockouts	4740	Informational	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Informational	Security	Microsoft-Windows-Security-Auditing
Security-Enabled group Modification	4735	Informational	Security	Microsoft-Windows-Security-Auditing
Successful User Account Login	4624	Informational	Security	Microsoft-Windows-Security-Auditing
Failed User Account Login	4625	Informational	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Informational	Security	Microsoft-Windows-Security-Auditing

Linux Syslog: Facility (source) vs. Severity level

Facility code	Keyword	Description
0	kern	Kernel messages
1	user	User-level messages
2	mail	Mail system
3	daemon	System daemons
4	auth	Security/authentication messages
5	syslog	Messages generated internally by syslogd
6	lpr	Line printer subsystem
7	news	Network news subsystem
8	uucp	UUCP subsystem
9	cron	Clock daemon
10	authpriv	Security/authentication messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	security	Log audit
14	console	Log alert
15	solaris-cron	Scheduling daemon
16–23	local0 – local7	Locally used facilities

Value	Severity	Keyword	Deprecated keywords	Description
0	Emergency	`emerg`	`panic` [7]	System is unusable
1	Alert	`alert`		Action must be taken immediately
2	Critical	`crit`		Critical conditions
3	Error	`err`	`error` [7]	Error conditions
4	Warning	`warning`	`warn` [7]	Warning conditions
5	Notice	`notice`		Normal but significant conditions
6	Informational	`info`		Informational messages
7	Debug	`debug`		Debug-level messages

```
#
# print some stuff on tty10
#
kern.warning;*.err;authpriv.none    /dev/tty10

# Forward all messages to central loghost
*.*                                 @loghost

# Backup file of all messages
*.*                                  -/var/log/messages
```

Audit

Definition: Audit

- NIST

  *"**Audit** records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges."*

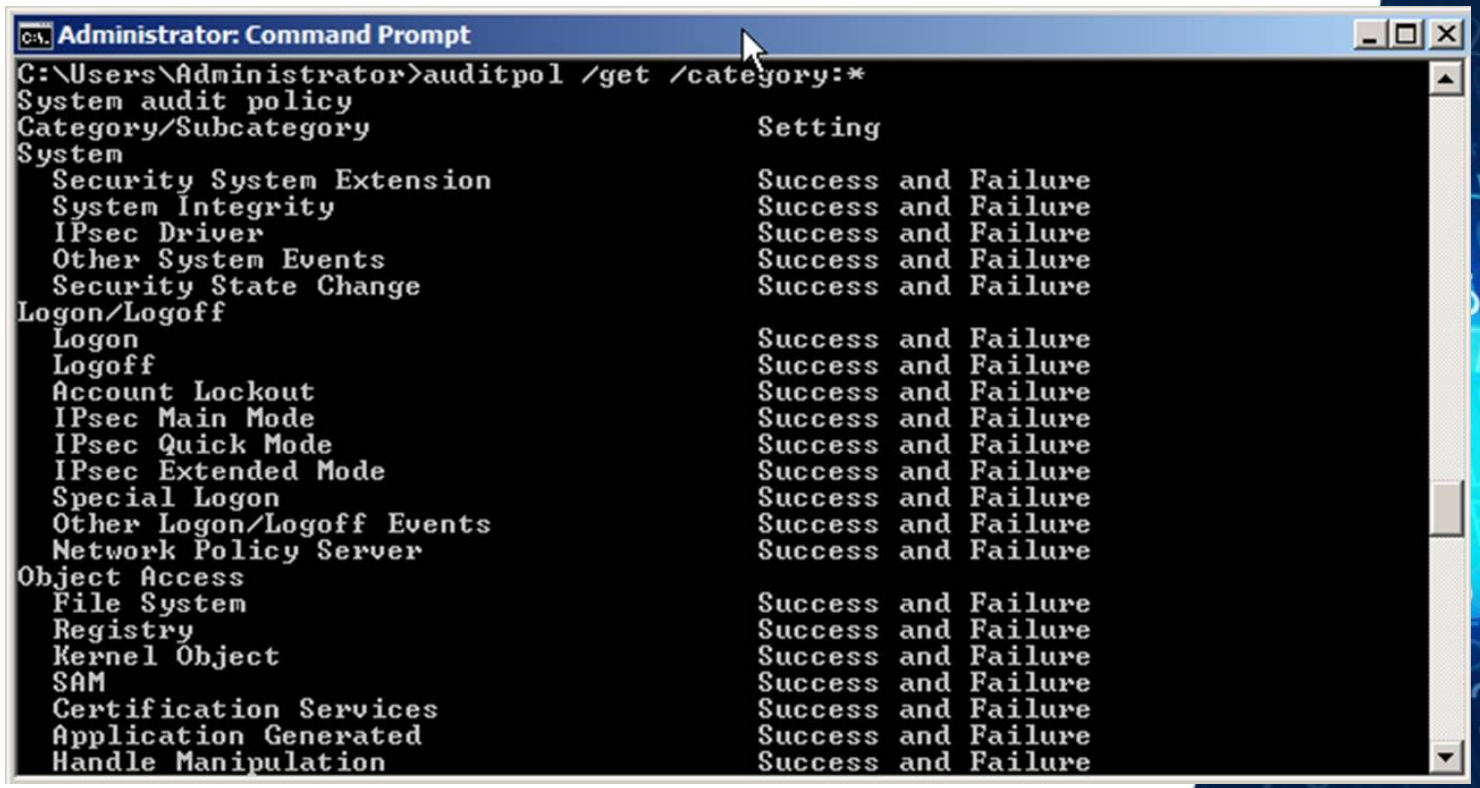
  - *"OSs typically permit system administrators to specify which types of events should be **audited** and whether successful and/or failed attempts to perform certain actions should be **logged**."*

- In other words

  - *"An **audit policy** determines which type of information about the system you'll find in the **logs**."*

Windows Audit: auditpol

- 9 categories / many sub-categories
  - Audit **account logon** events
  - Audit account management
  - Audit directory service access
  - Audit **logon** events
  - Audit object access
  - Audit policy change
  - Audit privilege use
  - Audit process tracking
  - Audit system events



- Log: success, failure, both, none

Linux Audit (audit.rules)

- Does this look familiar?
  - Watching file access
  - Monitoring system calls
  - Recording commands run by a user
  - Recording security events
  - Searching for events
  - Running summary reports
  - Monitoring network access
  - Changes to any trusted database such as `/etc/passwd`
  - …

```
-a exit,always -F arch=b64 -S execve -F path=/bin/rm -k Delete
-a exit,always -F arch=b64 -S execve -F path=/bin/vi -k Create_Edit_View_File

# Audit shutdown & Reboot command
-a exit,always -F arch=b64 -S execve -F path=/sbin/reboot -k Reboot
-a exit,always -F arch=b64 -S execve -F path=/sbin/init -k Reboot
-a exit,always -F arch=b64 -S execve -F path=/sbin/poweroff -k Reboot
-a exit,always -F arch=b64 -S execve -F path=/sbin/shutdown -k Reboot

# Audit mount unmount commands
-a exit,always -F arch=b64 -S execve -F path=/bin/mount -k mount_device
-a exit,always -F arch=b64 -S execve -F path=/bin/umount -k unmount_device

# Kill Process
-a exit,always -F arch=b64 -S kill -k Kill_Process

# Important files
-w /etc/passwd -p wa -k passwd_changes
-w /etc/group -p wa -k group_changes
```

However…

KIM ZETTER 10.13.05 07:00 AM

Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack

*"The company's server logs recorded **only unsuccessful log-in attempts**, not successful ones, frustrating a detailed analysis."*

You really want to have log management

- Log management 101
  - More logs don’t make you more secure
  - Better management does

Challenges in log management

- Log generation and storage
  - Many log sources:
    log data is scattered (sometimes even crossing borders) and has become **big data**
  - Inconsistent log contents
  - **Inconsistent timestamps / time zones / lots of different time formats**
  - Different vendors: different log formats
  - Different character sets
  - Log data is (sometimes) ephemeral

Challenges in log management

- Log analysis
  - boring, but that's what it's all about, no?
    - Log analysis is a unique skill
    - Log analysis takes time
  - **Correlation** of log entries
    - Multiple lines belonging to a single event
    - Similar log entries showing up in different log files
    - Timestamps
    - Probes over time
- Without sound processes for analyzing logs, their value is significantly reduced
  - Five Ws: *Who? What? When? Where? Why?*

Best Practices

- Start small
- Start small
- Start small
- Start small
- Start small
- Start really small

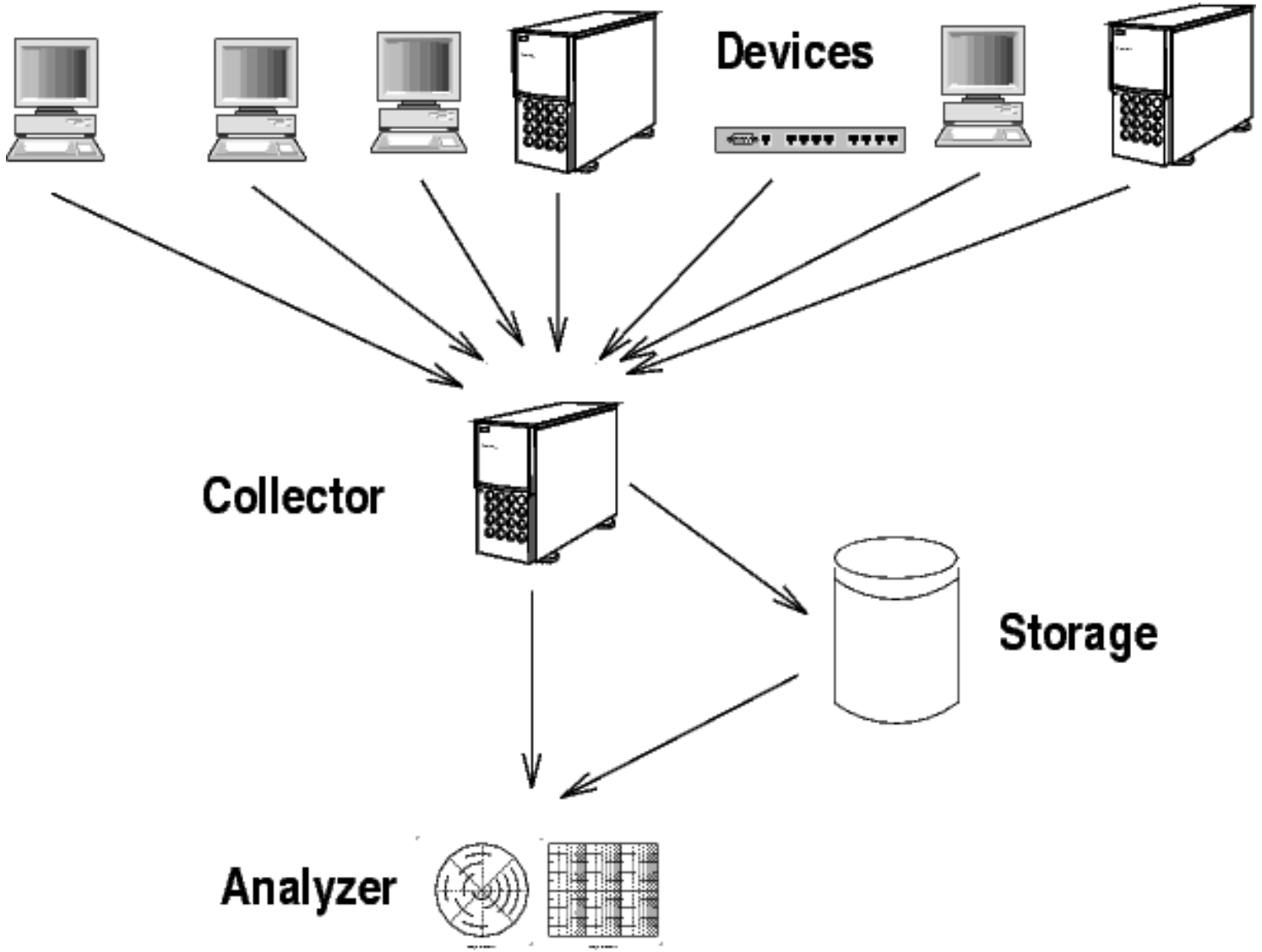
Best Practices

- First steps
  - Develop logging/audit policy – what to log and why
    - Don’t fall for the recommendation to enable only *Failure* events for audit categories
  - Simple use cases: determine what information is relevant to you
    - What devices/events are important?
    - What reports do you and the org want/need?
  - Create a baseline
    - Determine “normal” behaviour (systems and network)
    - Repeat at regular intervals
  - Ensure all devices use the same time source (if possible)
    - Use NTP from a secure source
    - Use UTC, especially if operating in more than one time zone
- Don’t forget to enable logging ;-)

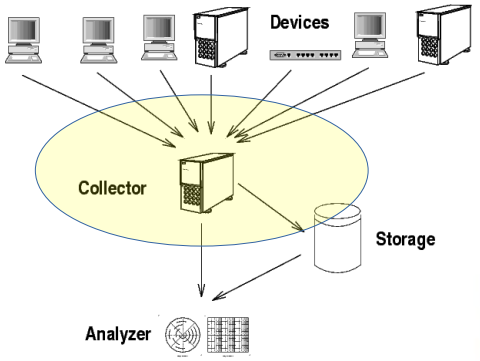
Best Practices

- Log security / log protection
  - Limit access to log files
  - Secure the processes that generate the log files
  - Configure log sources appropriately
    - What if logging fails?
    - What about “full” log files/partitions?
  - Implement secure mechanisms for transporting log data from the system(s) to the **centralized log management server(s)**
    - Consider using not only syslog via UDP (e.g., syslog-ng)
  - Are there regulatory requirements?
  - Anonymisation / Pseudonymisation?
  - Disk space / Storage / hardware requirements
    - Compression is very useful

Best Practices: Central log management

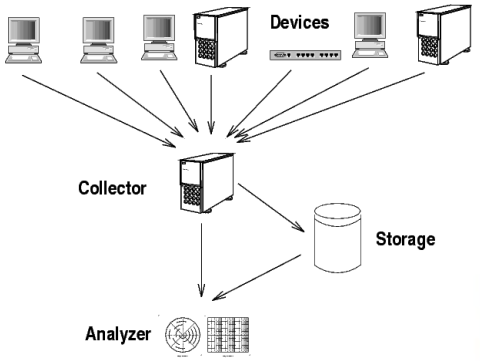


Best Practices: Central log management



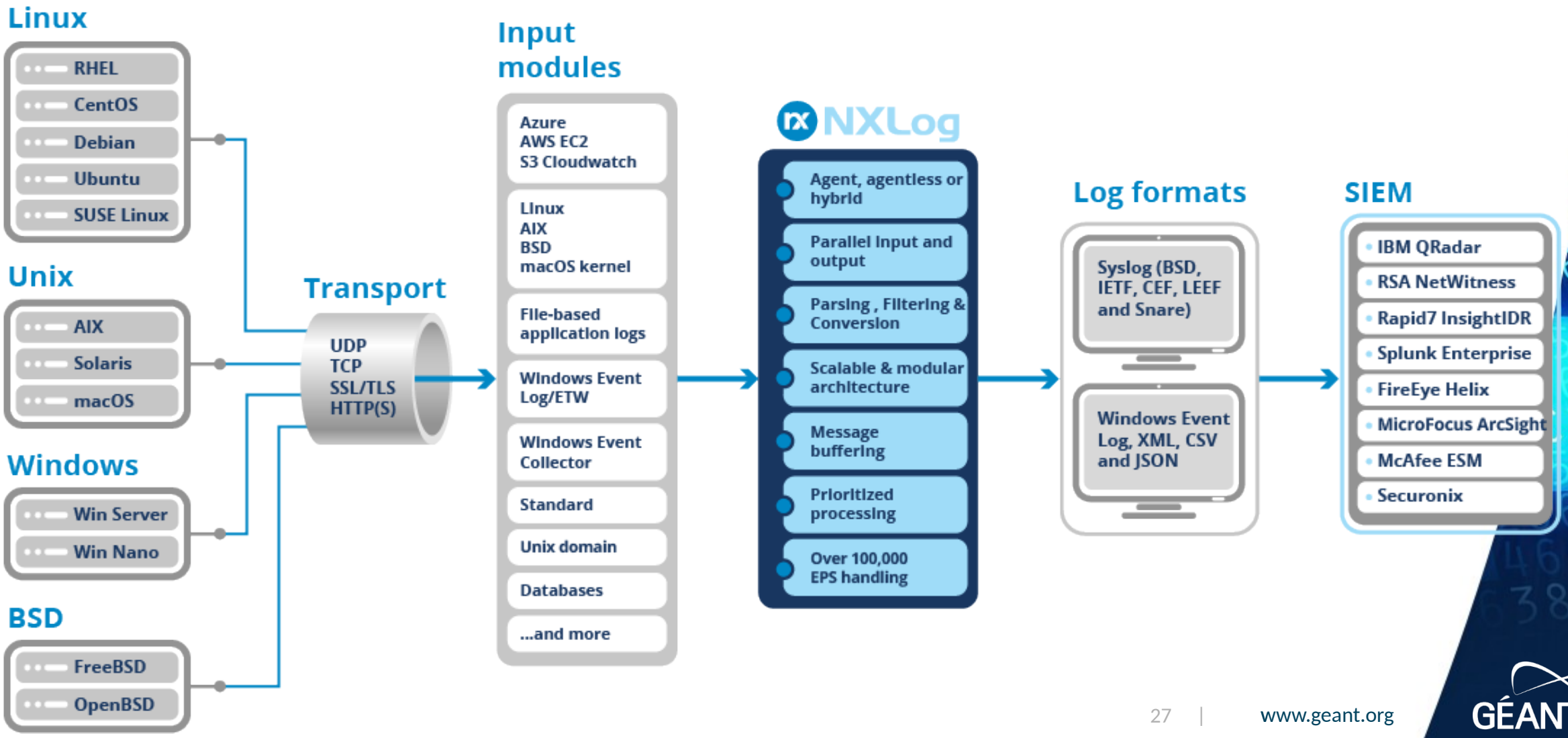
- Log host (Collector) requirements
  - (High) Availability / Scalability
    - Redundancy necessary?
  - Watch out for single point of failures
    - Network, routing
    - Power supply, environmental conditions (fire, water, …)
  - Log hosts are **highly critical systems**!
    - Just logging, no other services running
    - No connections from the outside
    - Will usually not “talk” to other systems
    - Harden the system, apply patches quickly
    - No general accounts, separation of duty!
  - Configure all devices to send logs to the dedicated log host
  - Check the license(s)!

Best Practices: Central log management



- Normalise the logs
  - Event Logs, syslog, SNMP, etc. need to be converted into the same format
- Log rotation
  - Determine time schedule, based on volume of data
  - Develop meaningful naming convention
- Log retention
  - Based on disk space
  - Based on regulatory requirements: Why? How? What? For how long?
  - Archive in secure area / external storage / offline backup?
- Visualise the logs (one interface to rule them all)
- Fortunately, you don’t have to do the above manually

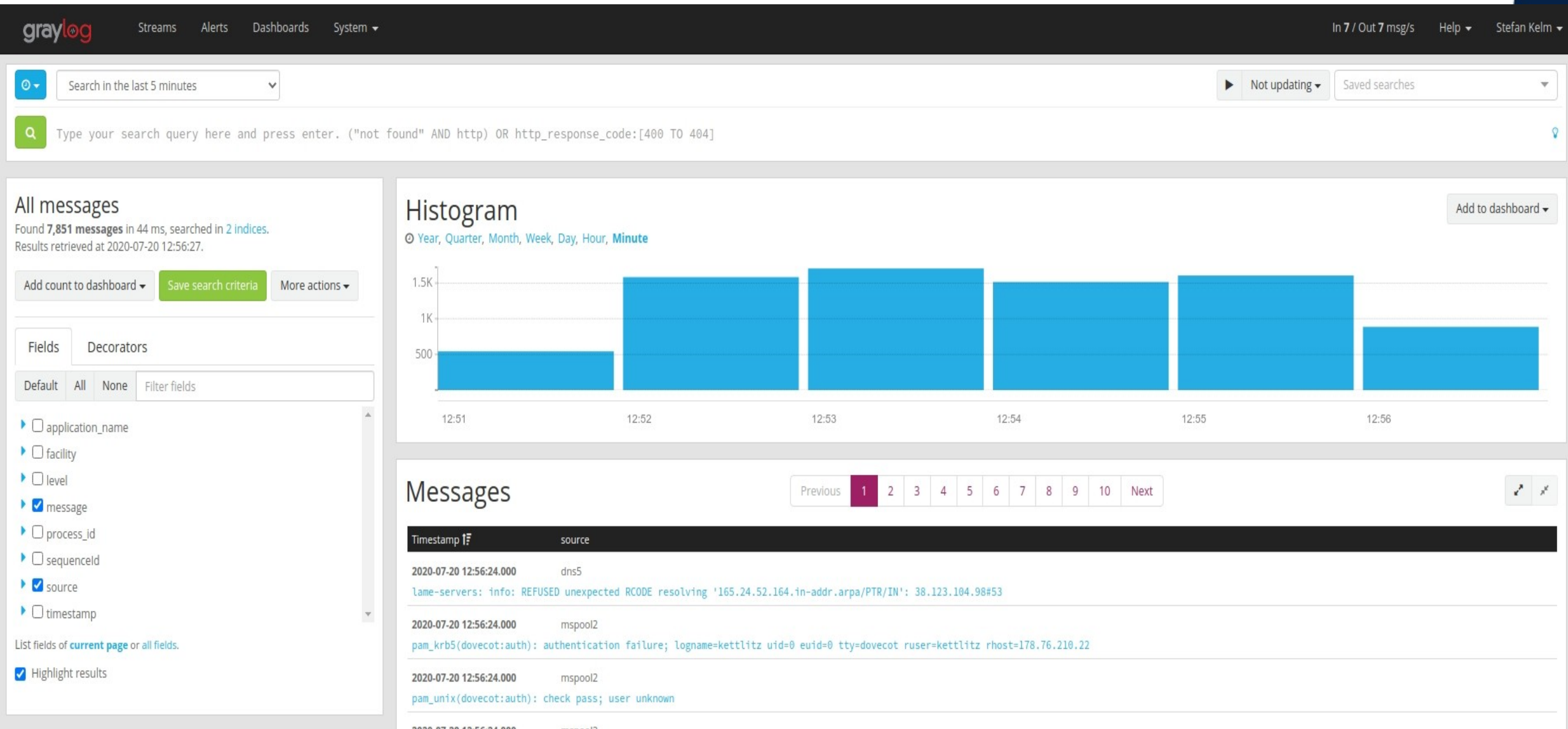
Example log mgmt: NXLog



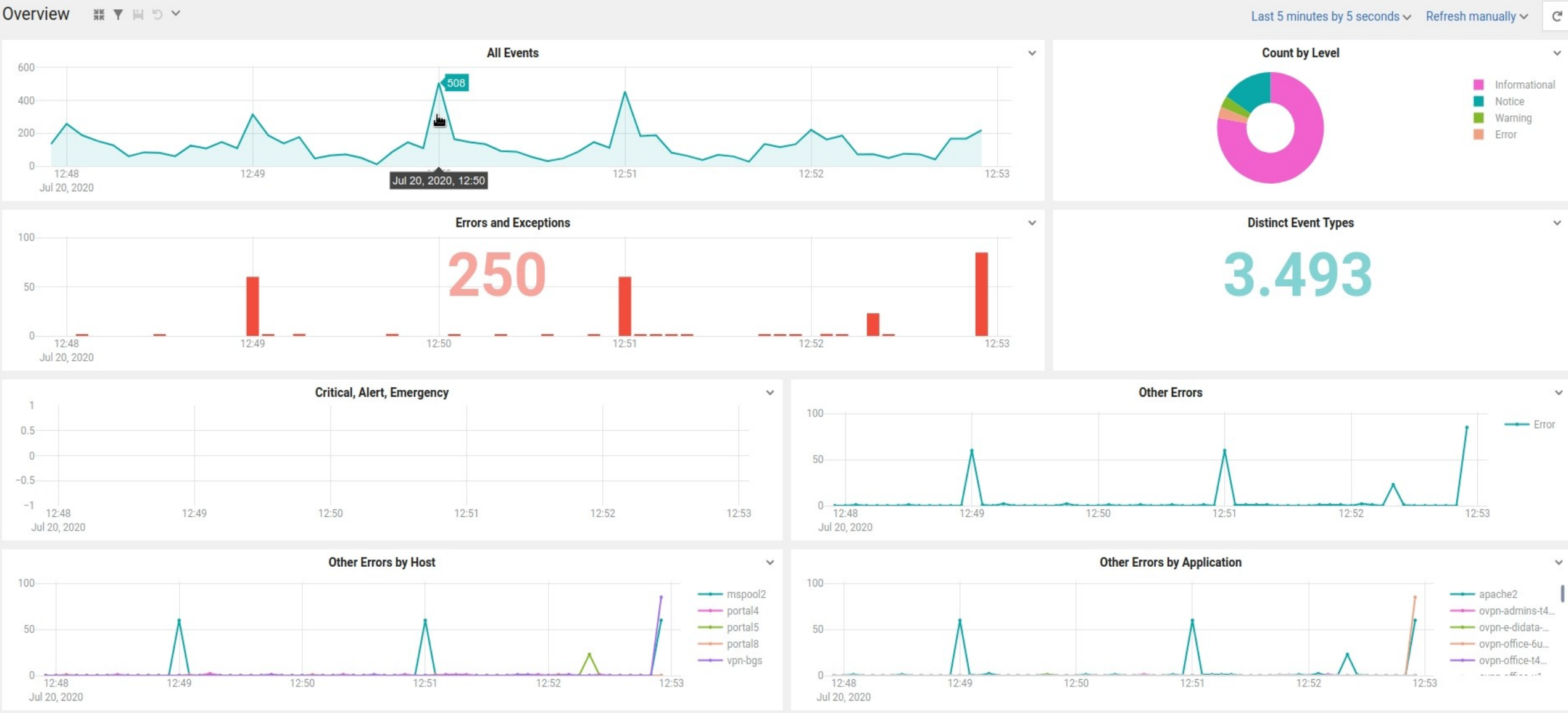
So many tools to choose from

- From **Log** management to **Security** Information and Event Management (**SIEM**)
  - NXLog
  - Rsyslog, Syslog-ng
  - Seq
  - Graylog
  - Snare
  - ELK: Logstash (+ Elasticsearch (+ Kibana))
  - Fluentd
  - ElasticSIEM
  - OSSIM
  - Apache Metron
  - Prelude OSS
  - Alienvault USM
  - Arcsight ESM
  - Splunk
  - IBM QRadar
  - Logrythm
  - RSA NetWitness
  - Exabeam
  - McAfee ESM
  - Securonix
  - Rapid7 InsightIDR
  - Tenzir

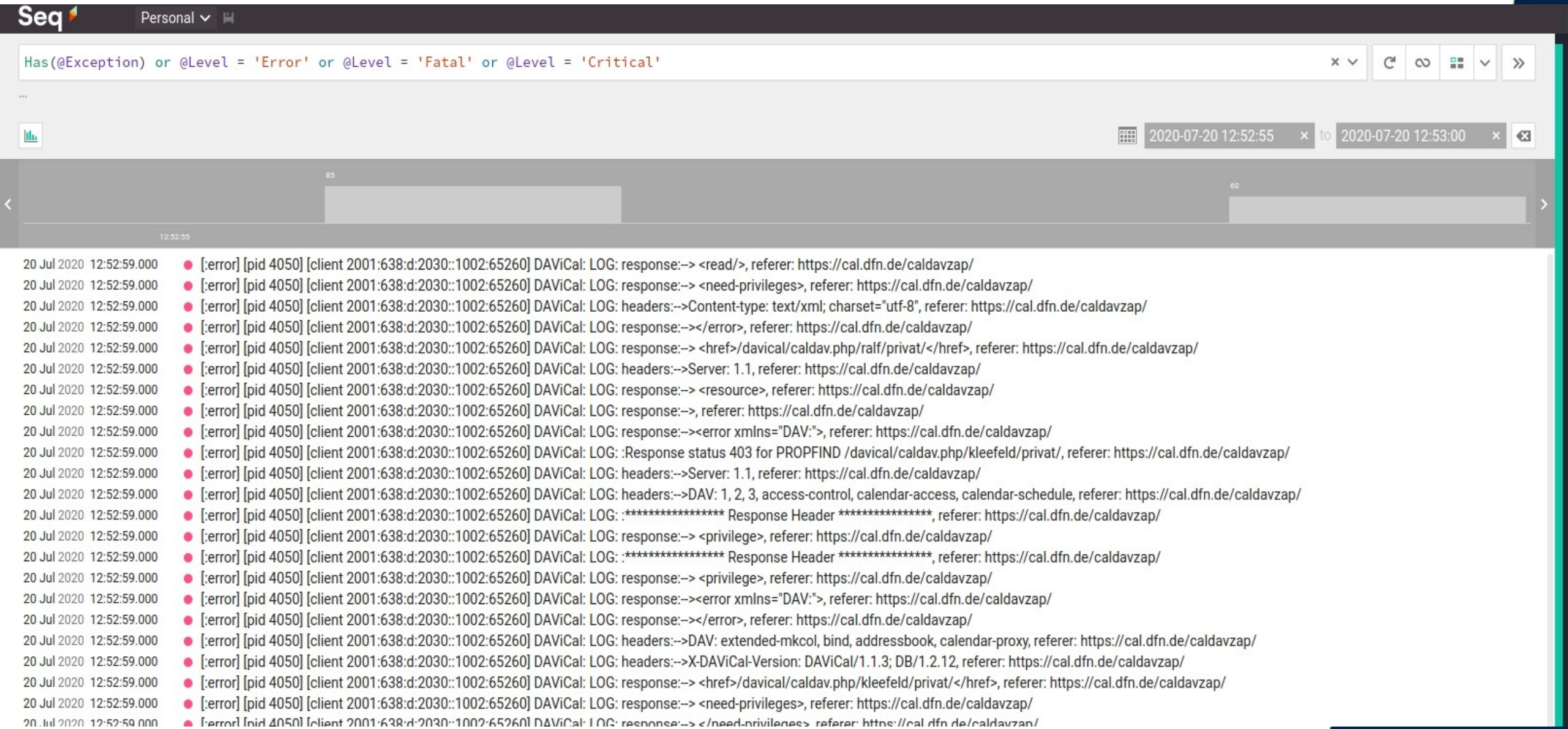
Graylog


graylog
Streams
Alerts
Dashboards
System
In 7 / Out 7 msg/s
Help
Stefan Kelm
Search in the last 5 minutes
Not updating
Saved searches
Type your search query here and press enter. ("not found" AND http) OR http_response_code:[400 TO 404]
All messages
Found 7,851 messages in 44 ms, searched in 2 indices.
Results retrieved at 2020-07-20 12:56:27.
Add count to dashboard
Save search criteria
More actions
Fields
Decorators
Default
All
None
Filter fields
application_name
facility
level
message
process_id
sequenceId
source
timestamp
List fields of current page or all fields.
Highlight results
Histogram
Add to dashboard
Year, Quarter, Month, Week, Day, Hour, Minute
1.5K
1K
500
12:51
12:52
12:53
12:54
12:55
12:56
Messages
Previous
1
2
3
4
5
6
7
8
9
10
Next
Timestamp
source
2020-07-20 12:56:24.000 dns5
lame-servers: info: REFUSED unexpected RCODE resolving '165.24.52.164.in-addr.arpa/PTR/IN': 38.123.104.98#53
2020-07-20 12:56:24.000 mspool2
pam_krb5(dovecot:auth): authentication failure; logname=kettlitz uid=0 euid=0 tty=dovecot ruser=kettlitz rhost=178.76.210.22
2020-07-20 12:56:24.000 mspool2
pam_unix(dovecot:auth): check pass; user unknown

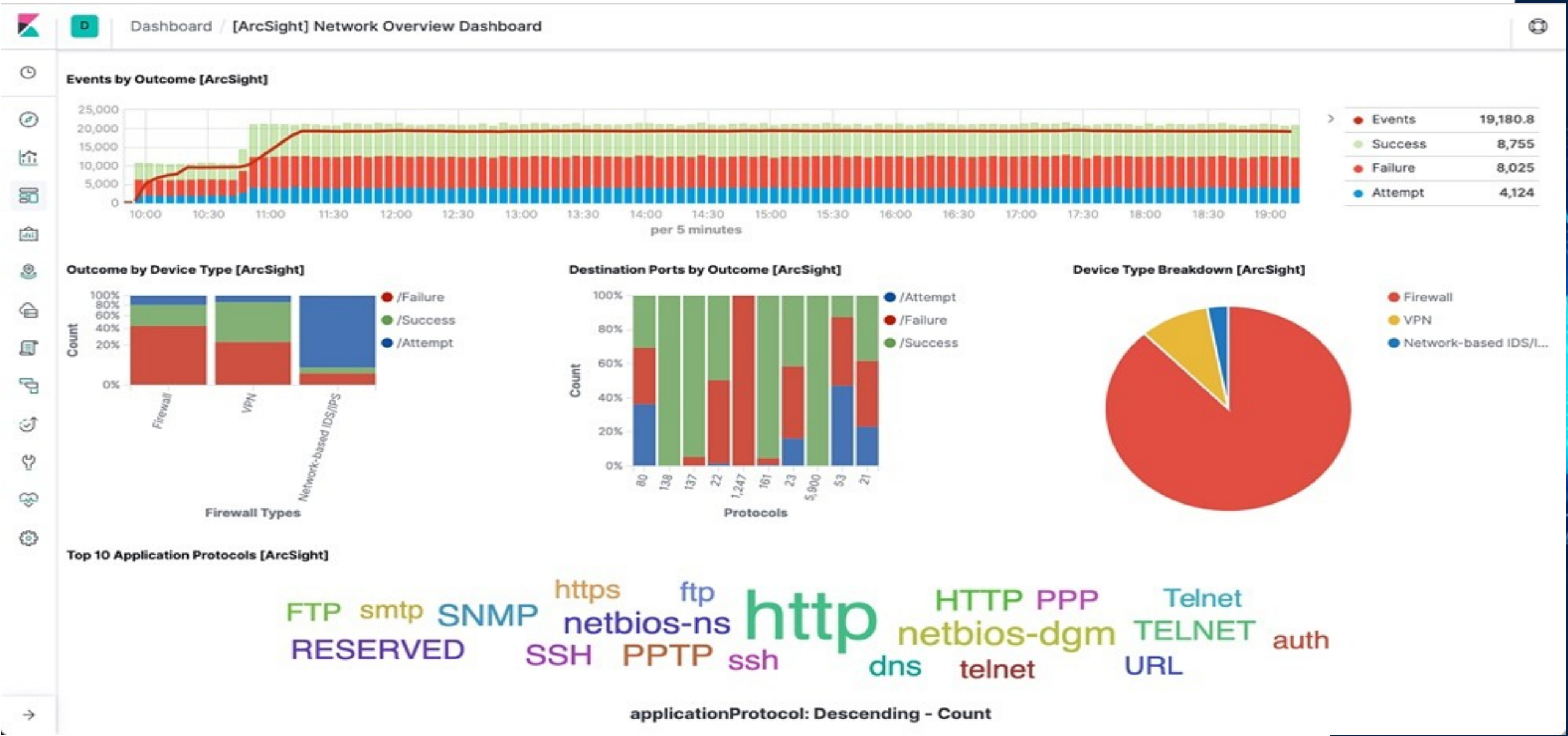
Seq


Overview
Last 5 minutes by 5 seconds
Refresh manually
All Events
600
400
200
0
508
12:48
Jul 20, 2020
12:49
Jul 20, 2020, 12:50
12:51
12:52
12:53
Count by Level
Informational
Notice
Warning
Error
Errors and Exceptions
100
50
0
250
12:48
Jul 20, 2020
12:49
12:50
12:51
12:52
12:53
Distinct Event Types
3.493
Critical, Alert, Emergency
1
0.5
0
−0.5
−1
12:48
Jul 20, 2020
12:49
12:50
12:51
12:52
12:53
Other Errors
100
50
0
Error
12:48
Jul 20, 2020
12:49
12:50
12:51
12:52
12:53
Other Errors by Host
100
50
0
mspool2
portal4
portal5
portal8
vpn-bgs
12:48
Jul 20, 2020
12:49
12:50
12:51
12:52
12:53
Other Errors by Application
100
50
0
apache2
ovpn-admins-t4...
ovpn-e-didata-...
ovpn-office-6u...
ovpn-office-t4...
12:48
Jul 20, 2020
12:49
12:50
12:51
12:52
12:53

Seq


Seq
Personal
Has(@Exception) or @Level = 'Error' or @Level = 'Fatal' or @Level = 'Critical'
2020-07-20 12:52:55
to
2020-07-20 12:53:00
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <read/>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <need-privileges>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->Content-type: text/xml; charset="utf-8", referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--></error>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <href>/davical/caldav.php/ralf/privat/</href>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->Server: 1.1, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <resource>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:-->, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--><error xmlns="DAV:">, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: :Response status 403 for PROPFIND /davical/caldav.php/kleefeld/privat/, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->Server: 1.1, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->DAV: 1, 2, 3, access-control, calendar-access, calendar-schedule, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: :********** Response Header **********, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <privilege>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: :********** Response Header **********, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <privilege>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--><error xmlns="DAV:">, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--></error>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->DAV: extended-mkcol, bind, addressbook, calendar-proxy, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: headers:-->X-DAViCal-Version: DAViCal/1.1.3; DB/1.2.12, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <href>/davical/caldav.php/kleefeld/privat/</href>, referer: https://cal.dfn.de/caldavzap/
20 Jul 2020 12:52:59.000 [:error] [pid 4050] [client 2001:638:d:2030::1002:65260] DAViCal: LOG: response:--> <need-privileges>, referer: https://cal.dfn.de/caldavzap/

Kibana (ELK Stack)



Pro tips: for future use

- Eventually you may want to do things like
  - File and folder auditing
    - file/folder creation/deletion, permission changes, ownership changes, …
  - Windows Registry Auditing
    - Forensicators love this!
  - Process command line logging
    - May catch fileless malware
  - Windows PowerShell Logging
    - a.k.a. “command line 2.0”
  - Windows Sysmon Logging
    - Greatly enhances the Windows Event Log
- Note: the above are all **very** noisy

Legal and Regulatory Compliance

- Not part of this talk (IANAL :-))
- But always **do** check with your data protection officer (DPO)!

Summary

- Log management usually is funded by compliance budgets!
  - *“Buy for compliance, use for security and operations.”*
- There’s no: one size fits all
  - Each network is unique
  - Keep it simple, stupid (KISS) --- Start really small!
- Ask yourself…
  - What logs am I going to collect locally?
  - What logs am I going to send to the central log host/SIEM and how?
  - What logs am I going to analyse centrally?

➲ **Start logging**
– then start collecting logs
– then start reviewing and analyzing logs

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

References (1)

- Useful web sites
  - Guide to Computer Security Log Management (NIST)
    - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
  - Microsoft TechNet
    - https://social.technet.microsoft.com/Forums/en-US/
  - Ultimate Windows Security
    - https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/
  - SolarWinds
    - https://www.loggly.com/ultimate-guide/centralizing-windows-logs/

References (2)

- Useful web sites
  - EventID.Net
    - https://eventid.net/
  - Security Event Log Collection from a Domain Controller
    - https://rockyprogress.wordpress.com/2011/12/04/security-event-log-collection-from-a-domain-controller/
  - Microsoft TechNet
    - https://social.technet.microsoft.com/Forums/en-US/
  - RHEL Audit System Reference
    - https://access.redhat.com/articles/4409591
  - Linux Audit Documentation Project
    - https://github.com/linux-audit/audit-documentation/wiki

References (3)

- Useful web sites
  - Spotting the Adversary with Windows Event Log Monitoring
    - https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm
  - Centralizing Windows Logs
    - https://www.loggly.com/ultimate-guide/centralizing-windows-logs/
  - Windows Logging Cheat Sheets
    - https://www.malwarearchaeology.com/cheat-sheets
  - OWASP Logging Cheat Sheet
    - https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html

References (4)

- Useful web sites
  - Processing Data to Protect Data: Resolving the Breach Detection Paradox
    - https://script-ed.org/article/processing-data-to-protect-data-resolving-the-breach-detection-paradox/

Further reading

- “Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management”
  - Chris Phillips, Kevin Schmidt, Anton Chuvakin
  - Syngress 2013
  - ISBN: 9781597496353

General logging configuration recommendations (NIST)

Table 4-1. Examples of Logging Configuration Settings

Category	Low Impact Systems	Moderate Impact Systems	High Impact Systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes

What am I looking for?

4.1 Application Whitelisting

Application whitelisting events should be collected to look for applications that have been blocked from execution. Any blocked applications could be malware or users trying to run unapproved software. Software Restriction Policies (SRP) is supported on Windows XP and above. The AppLocker feature is available for Windows 7 and above Enterprise and Ultimate editions only. [45] Application Whitelisting events can be collected if SRP or AppLocker are actively being used on the network.

	ID	Level	Event Log	Event Source
AppLocker Block	8003 8004	Error Warning	Microsoft-Windows-AppLocker/EXE and DLL	Microsoft-Windows-AppLocker
AppLocker Warning	8006 8007	Error Warning	Microsoft-Windows-AppLocker/MSI and Script	Microsoft-Windows-AppLocker
SRP Block	865, 866, 867, 868, 882	Warning	Application	Microsoft-Windows-SoftwareRestrictionPolices

Table 2: Whilelisting Events

What am I looking for?

4.2 Application Crashes

Application crashes may warrant investigation to determine if the crash is malicious or benign. Categories of crashes include Blue Screen of Death (BSOD), Windows Error Reporting (WER), Application Crash and Application Hang events. If the organization is actively using the Microsoft Enhanced Mitigation Experience Toolkit (EMET), then EMET logs can also be collected.

	ID	Level	Event Log	Event Source
App Error	1000	Error	Application	Application Error
App Hang	1002	Error	Application	Application Hang
BSOD	1001	Error	System	Microsoft-Windows-WER-SystemErrorReporting
WER	1001	Informational	Application	Windows Error Reporting
EMET	1 2	Warning Error	Application Application	EMET

Table 3: Application Events

What am I looking for?

4.3 System or Service Failures

System and Services failures are interesting events that may need to be investigated. Service operations normally do not fail. If a service fails, then it may be of concern and should be reviewed by an administrator. If a Windows service continues to fail repeatedly on the same machines, then this may indicate that an attacker is targeting a service.

	ID	Level	Event Log	Event Source
Windows Service Fails or Crashes	7022, 7023, 7024, 7026, 7031, 7032, 7034	Error	System	Service Control Manager

Table 4: System Events

What am I looking for?

4.4 Windows Update Errors

A machine must be kept up to date to mitigate known vulnerabilities. Although unlikely, these patches may sometimes fail to apply. Failure to update issues should be addressed to avoid prolonging the existence of an application issue or a vulnerability in the operating system or an application.

	ID	Level	Event Log	Event Source
Windows Update Failed	20, 24, 25, 31, 34, 35	Error	Microsoft-Windows-WindowsUpdateClient/Operational	Microsoft-Windows-WindowsUpdateClient
Hotpatching Failed	1009	Informational	Setup	Microsoft-Windows-Servicing

Table 5: Windows Update Failed Events

4.5 Windows Firewall

If client workstations are taking advantage of the built-in host-based Windows Firewall, then there is value in collecting events to track the firewall status. For example, if the firewall state changes from on to off, then that log should be collected. Normal users should not be modifying the firewall rules of their local machine.

	ID	Level	Event Log	Event Source
Firewall Rule Add	2004	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rule Change	2005	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Rules Deleted	2006, 2033	Informational	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security
Firewall Failed to load Group Policy	2009	Error	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall	Microsoft-Windows-Windows Firewall With Advanced Security

Table 6: Firewall Events

The above events for the listed versions of the Windows operating system are only applicable to modifications of the local firewall settings.

What am I looking for?

4.6 Clearing Event Logs

It is unlikely that event log data would be cleared during normal operations and it is likely that a malicious attacker may try to cover their tracks by clearing an event log. When an event log gets cleared, it is suspicious. Centrally collecting events has the added benefit of making it much harder for an attacker to cover their tracks. Event Forwarding permits sources to forward multiple copies of a collected event to multiple collectors thus enabling redundant event collection. Using a redundant event collection model can minimize the single point of failure risk.

	ID	Level	Event Log	Event Source
Event Log was Cleared	104	Informational	System	Microsoft-Windows-Eventlog
Audit Log was Cleared	1102	Informational	Security	Microsoft-Windows-Eventlog

Table 7: Log Activity Events

4.7 Software and Service Installation

As part of normal network operations, new software and services will be installed, and there is value in monitoring this activity. Administrators can review these logs for newly installed software or system services and verify that they do not pose a risk to the network.

	ID	Level	Event Log	Event Source
New Kernel Filter Driver	6	Informational	System	Microsoft-Windows-FilterManager
New Windows Service	7045	Informational	System	Service Control Manager
New MSI File Installed	1022, 1033	Informational	Application	MsiInstaller
New Application Installation	903, 904[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory[47]	Microsoft-Windows-Application-Experience
Updated Application	905, 906[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Removed Application	907, 908[46]	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Summary of Software Activities	800	Informational	Microsoft-Windows-Application-Experience/Program-Inventory	Microsoft-Windows-Application-Experience
Update Packages Installed	2	Informational	Setup	Microsoft-Windows-Servicing
Windows Update Installed	19	Informational	System	Microsoft-Windows-WindowsUpdateClient

Table 8: Software and Service Events