SAND2016-4040C

Exceptional service in the national interest

Sandia National Laboratories

Splunk as a Service for SysAdmins

Providing value to System Administrators through log aggregation and reporting

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

What makes it a service

- Instant Benefit
  - System Administrator can install the forwarder and will begin receiving directed emails about log events with no other configuration required
  - Provide the admin increased knowledge from log data
  - Save admin the time required to review all logs
- Easy to Setup for the client
  - Don’t burden admin to get these result

What it takes to offer the service

- Infrastructure overview
- Getting data in
- Getting good information out
- Get targeted information into right hands
- Identify missing data

Infrastructure Overview

- Multiple dedicated indexers
  - SSD – Hot storage
  - SAN – Cold Storage
- Dedicated Search Head
- Dedicated Deployment server
- Syslog forwarder
  - Linux syslog-ng
  - Multiple instances of universal forwarder

Infrastructure – User Access

- Allow users capability for Ad-Hoc access to data where they have Need-to-Know

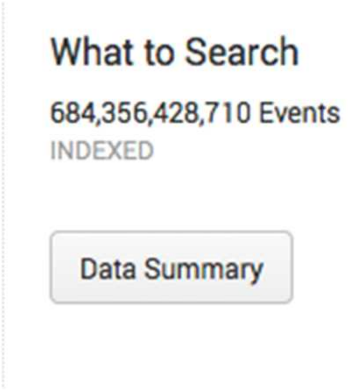
- Indexes to create NTK boundaries
  - Can also define special retention periods
- Roles assigned to specific indexes
- AD Group assigned to role
- User assigned to 1 or more AD groups.
  - Permission sets are added if user belongs to multiple roles

Getting Data In

- Use forwarders where possible
  - Cache data when connection fails
  - Compress data before sending and load balance with indexers
  - Acknowledge data successfully written
- Use Deployment Server to push common configurations
  - Can configure deployment client name to identify special serverclasses
- Follow Common Information Model
  - Make the effort now
  - Regret it later
    - P.S. I know which one you should choose from personal experience

Getting Data In

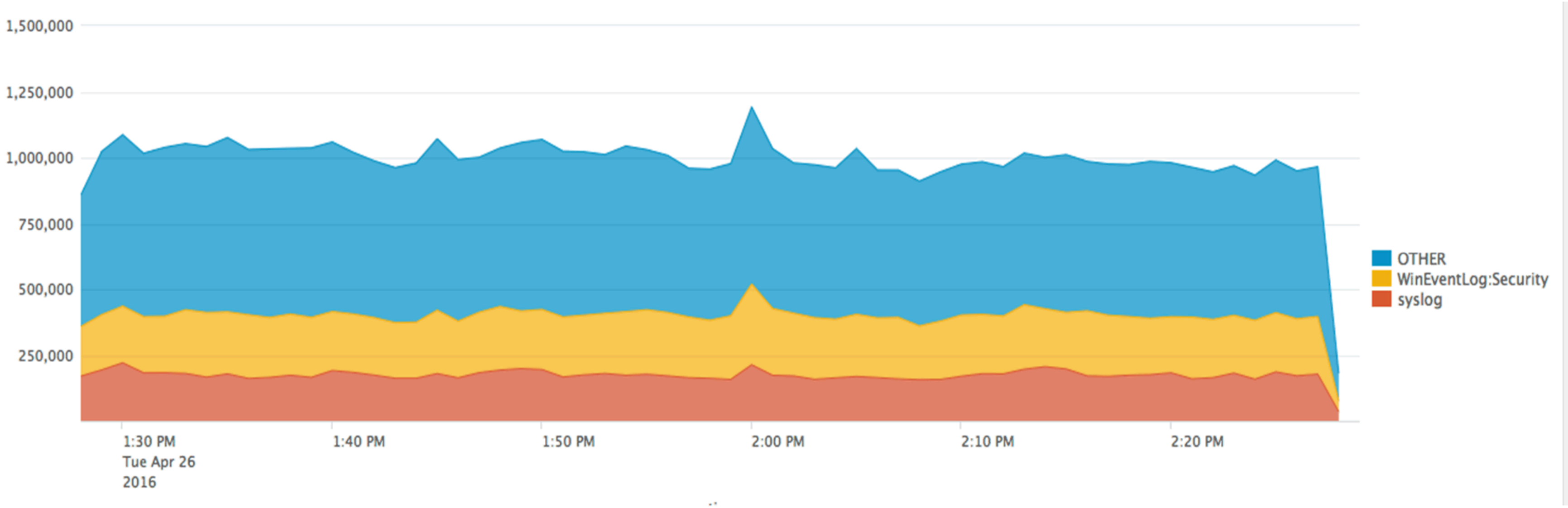
- How much data are we talking about
  - 3000 hosts
  - 2500 source types
  - 1.2 Billion events / Day



What to Search

684,356,428,710 Events

INDEXED



What to do with all that Data

- Nobody can review all of it
- Do we even know what to look for
- Does each admin interpret the data the same way

- Solution
  - Brainstorm ideas with other admins
  - Decide what you would like to have reported
  - Turn it into a service
    - Improve the results
    - Provide targeted results to all admins

What to search for

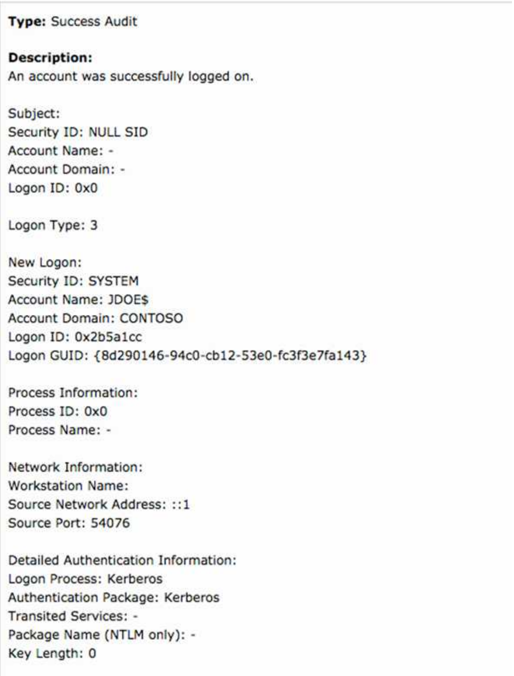
- Think about what you would want to have reported
- Randy Franklin’s www.ultimatewindowssecurity.com
- SANS
- Request from other admins
  - As requests come in, decide if it would be beneficial to everybody

Improve the results

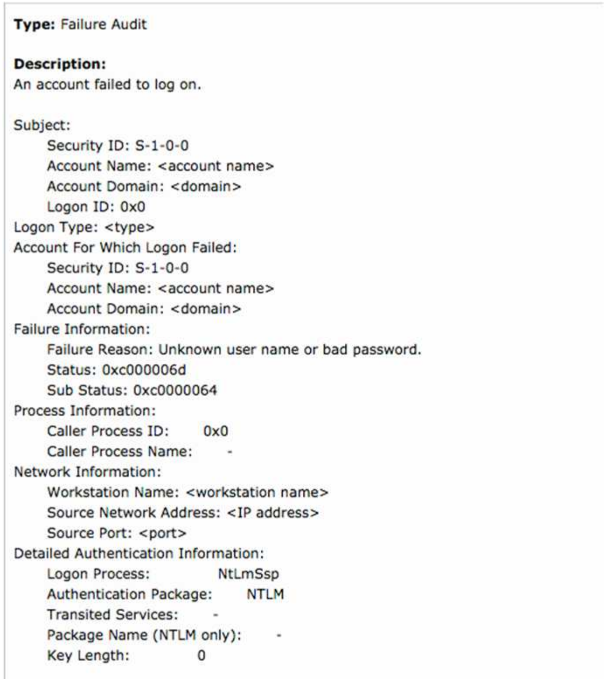
- Don’t return a table of all events
- Apply statistics to aggregate the data
- Incorporate external data to enhance results
- Evaluate the data to highlight important aspects

- Examples

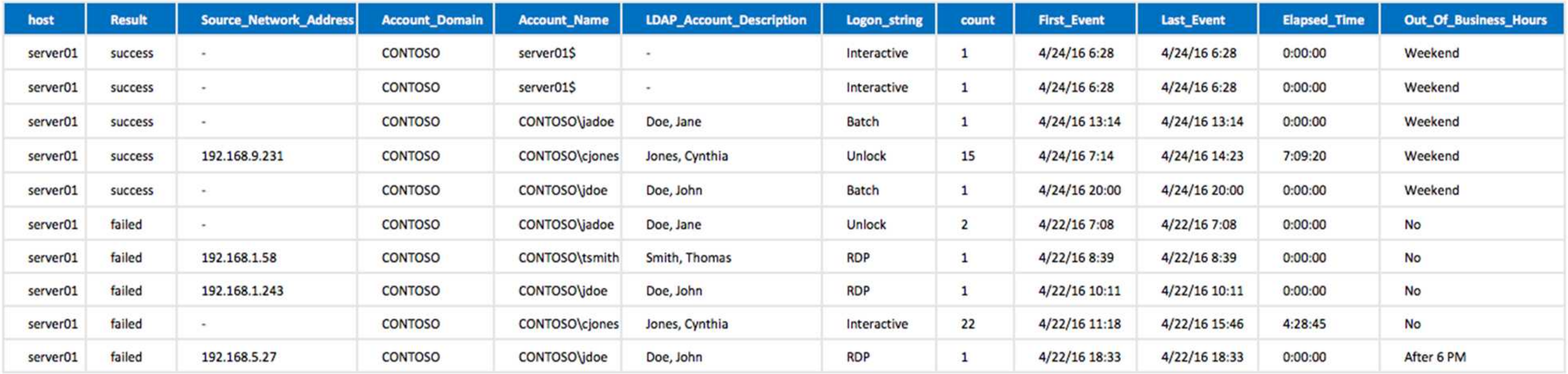
Logins



```
Type: Success Audit

Description:
An account was successfully logged on.

Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

New Logon:
Security ID: SYSTEM
Account Name: JDOE$
Account Domain: CONTOSO
Logon ID: 0x2b5a1cc
Logon GUID: {8d290146-94c0-cb12-53e0-fc3f3e7fa143}

Process Information:
Process ID: 0x0
Process Name: -

Network Information:
Workstation Name:
Source Network Address: ::1
Source Port: 54076

Detailed Authentication Information:
Logon Process: Kerberos
Authentication Package: Kerberos
Transited Services: -
Package Name (NTLM only): -
Key Length: 0
```



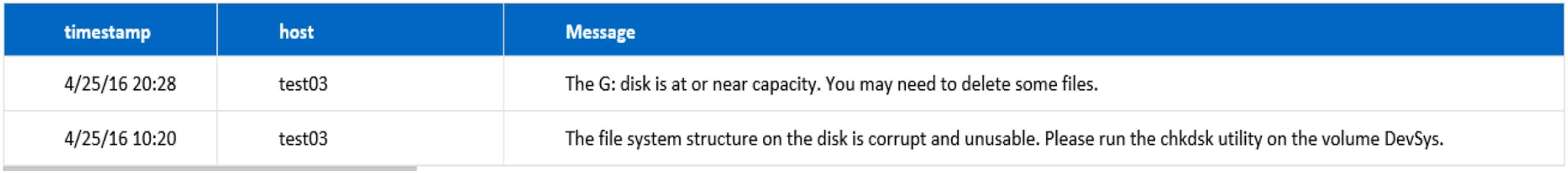
```
Type: Failure Audit

Description:
An account failed to log on.

Subject:
      Security ID: S-1-0-0
      Account Name: <account name>
      Account Domain: <domain>
      Logon ID: 0x0
Logon Type: <type>
Account For Which Logon Failed:
      Security ID: S-1-0-0
      Account Name: <account name>
      Account Domain: <domain>
Failure Information:
      Failure Reason: Unknown user name or bad password.
      Status: 0xc000006d
      Sub Status: 0xc0000064
Process Information:
      Caller Process ID:      0x0
      Caller Process Name:      -
Network Information:
      Workstation Name: <workstation name>
      Source Network Address: <IP address>
      Source Port: <port>
Detailed Authentication Information:
      Logon Process:            NtLmSsp
      Authentication Package:       NTLM
      Transited Services:      -
      Package Name (NTLM only):       -
      Key Length:            0
```



host	Result	Source_Network_Address	Account_Domain	Account_Name	LDAP_Account_Description	Logon_string	count	First_Event	Last_Event	Elapsed_Time	Out_Of_Business_Hours
server01	success	-	CONTOSO	server01$	-	Interactive	1	4/24/16 6:28	4/24/16 6:28	0:00:00	Weekend
server01	success	-	CONTOSO	server01$	-	Interactive	1	4/24/16 6:28	4/24/16 6:28	0:00:00	Weekend
server01	success	-	CONTOSO	CONTOSO\jadoe	Doe, Jane	Batch	1	4/24/16 13:14	4/24/16 13:14	0:00:00	Weekend
server01	success	192.168.9.231	CONTOSO	CONTOSO\cjones	Jones, Cynthia	Unlock	15	4/24/16 7:14	4/24/16 14:23	7:09:20	Weekend
server01	success	-	CONTOSO	CONTOSO\jdoe	Doe, John	Batch	1	4/24/16 20:00	4/24/16 20:00	0:00:00	Weekend
server01	failed	-	CONTOSO	CONTOSO\jadoe	Doe, Jane	Unlock	2	4/22/16 7:08	4/22/16 7:08	0:00:00	No
server01	failed	192.168.1.58	CONTOSO	CONTOSO\tsmith	Smith, Thomas	RDP	1	4/22/16 8:39	4/22/16 8:39	0:00:00	No
server01	failed	192.168.1.243	CONTOSO	CONTOSO\jdoe	Doe, John	RDP	1	4/22/16 10:11	4/22/16 10:11	0:00:00	No
server01	failed	-	CONTOSO	CONTOSO\cjones	Jones, Cynthia	Interactive	22	4/22/16 11:18	4/22/16 15:46	4:28:45	No
server01	failed	192.168.5.27	CONTOSO	CONTOSO\jdoe	Doe, John	RDP	1	4/22/16 18:33	4/22/16 18:33	0:00:00	After 6 PM

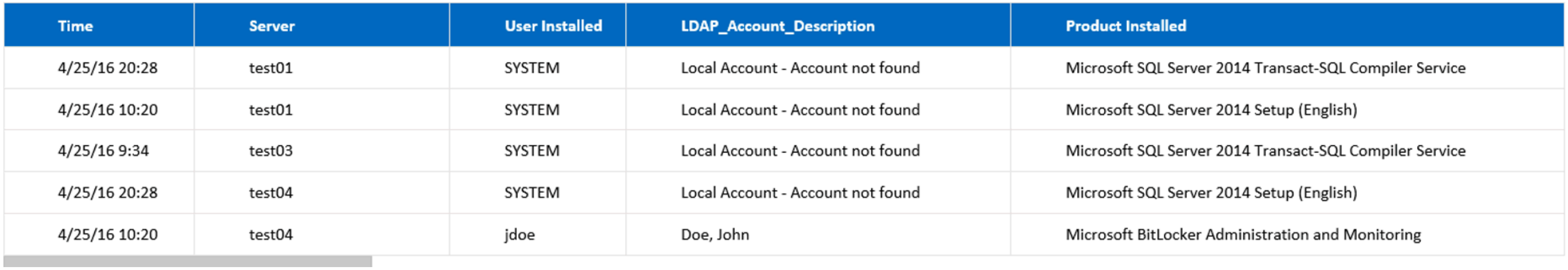
System Events

- Disk Errors



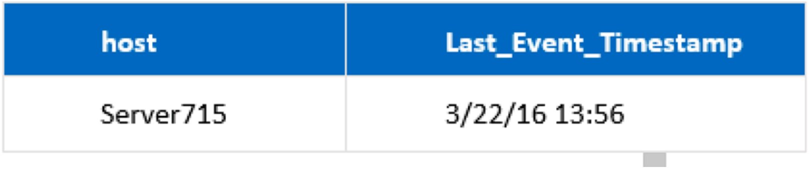
timestamp	host	Message
4/25/16 20:28	test03	The G: disk is at or near capacity. You may need to delete some files.
4/25/16 10:20	test03	The file system structure on the disk is corrupt and unusable. Please run the chkdsk utility on the volume DevSys.

- Installed applications



Time	Server	User Installed	LDAP_Account_Description	Product Installed
4/25/16 20:28	test01	SYSTEM	Local Account - Account not found	Microsoft SQL Server 2014 Transact-SQL Compiler Service
4/25/16 10:20	test01	SYSTEM	Local Account - Account not found	Microsoft SQL Server 2014 Setup (English)
4/25/16 9:34	test03	SYSTEM	Local Account - Account not found	Microsoft SQL Server 2014 Transact-SQL Compiler Service
4/25/16 20:28	test04	SYSTEM	Local Account - Account not found	Microsoft SQL Server 2014 Setup (English)
4/25/16 10:20	test04	jdoe	Doe, John	Microsoft BitLocker Administration and Monitoring

- Host Stopped sending logs



host	Last_Event_Timestamp
Server715	3/22/16 13:56

Get the information into the right hands

- Dashboards
  - Build searches based on sourcetypes
  - Build panels from specific CIM fields
  - Add dropdown or selectors so admins can limit returned info

- Roles will limit the searches to just the data they have NTK for.
  - This will allow each dashboard to be built generically
  - Information returned will be specific to user logged in

Get the information into the right hands

- Scheduled Searches – This is where our service shines
  - Define the owner of each system/account using external data
    - Inventory database, AD, LDAP, CSV files
    - Add owner email as field in each event
  - Email results directly to responsible parties with the “SendTo” app
    - Groups results by email address then creates html email with results
    - Admins are not burdened with unimportant noise

Identify and report missing data

- An admin that relies on results will be blind if data is incorrect

- Items to account for
  - Systems that stop sending log data
  - Systems that have a different hostname vs Splunk name or inventory name
  - Systems without a valid email address field
  - Indexing delays longer than reporting periods
  - Hosts sending data to the wrong index

Summary

- Plan index and roles to match NTK
- Follow Common Information Model for field extractions
- Build searches to be specific
  - Remove noise without removing important information
- Use external data to supplement reports
- Use SendTo app to email appropriate admins

Questions?

Contact Info:

Edward (Eddie) Roberts
Sandia National Laboratories
505-284-3851
eddie@sandia.gov