Indiana University: Splunking Distributed Logs for IT Policy Alignment

Allen Tucker, Manager
Kelly Zimmerman, Systems Administrator
Daniel Daily, Systems Administrator
HELPnet Central Systems Team

splunk>

Disclaimer

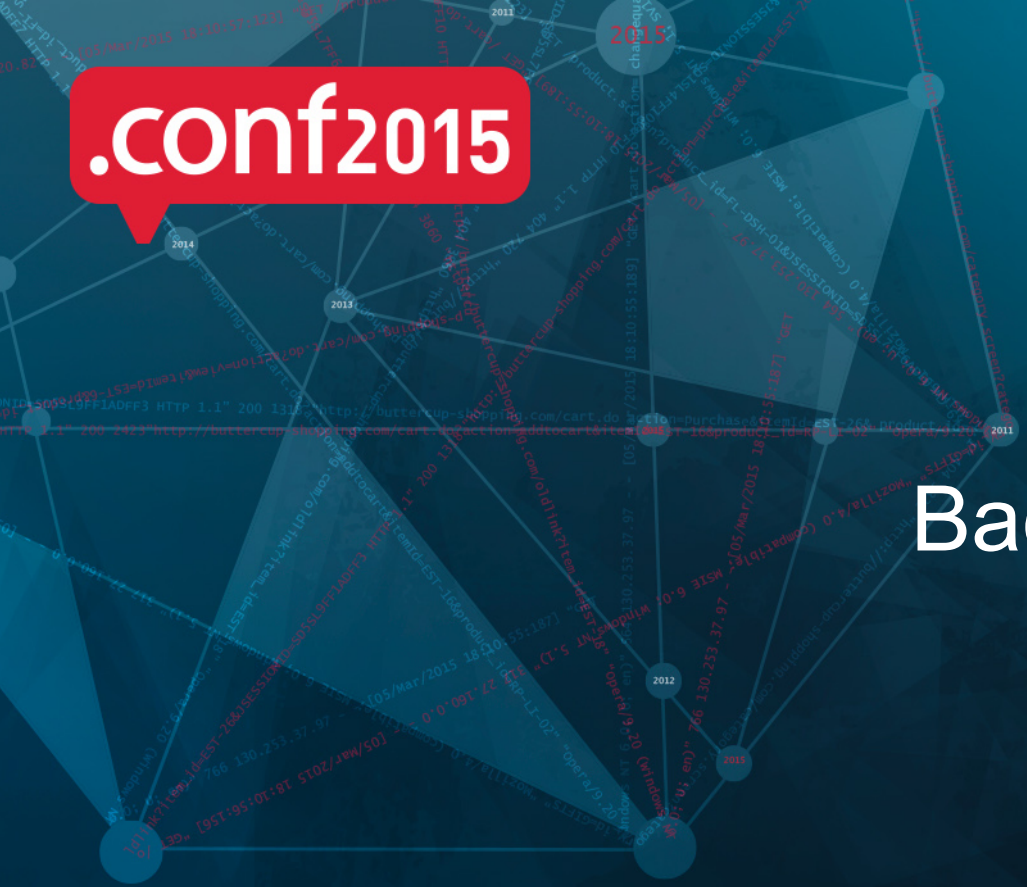
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Referenced customers for ITSI product participated in a limited release software program that included items at no charge.

Agenda

- Background and Culture
- Architecture
- Scalable Architecture
- Departmental onboarding
- App Dev Phases
- Expansion of service
- Q&A



Background and Culture

splunk>

Indiana University, *est. 1820*

- **$3.3B** enterprise
- Partnered with **$6B** IU Health system

- **115,000** Students
- **1.3M** Credit Hours per semester
- **>20,000** Degrees per year
- **$1.1B** in Financial Aid
- **$450M** in research grants

- **8,000** Acres
- **882** buildings, 36M square feet
- **>600,000** *living* Alumni

- **10,500** Faculty and Staff

CENTRALIZED enterprise IT
with
DECENTRALIZED departmental IT

109 Departmental IT Groups
5213 Total Servers within IU

Safeguards

- IU IT Policy
  - IT-12 list of ‘best practices’ for system management
- IU Internal Audits
  - In depth departmental checks for IT operations
  - Alignment with IT policies
- Log Management
  - Success/Failed User Logons, Success/Failed File Accesses

Implications

- Costs associated with log review
  - Its overwhelming
  - Costly if departments DIY
  - Staff time is at a premium

Service Timeline

splunk>

Internal HELPnet Deployment

- 120 Servers

Cost Recovery Offering

Departmental Growth & UITS Interest

- 20 Departments
- Many Regionals
- ~375 servers

Issues with Scalability

New Product Testing & PoC

Proposal to Cabinet

- Approval in August 2014

Deployment

- Training
- Certification
- Build of Architecture
- App Development

Customer Onboarding (Since June)

- 42 Departments
- 2000 Active Servers

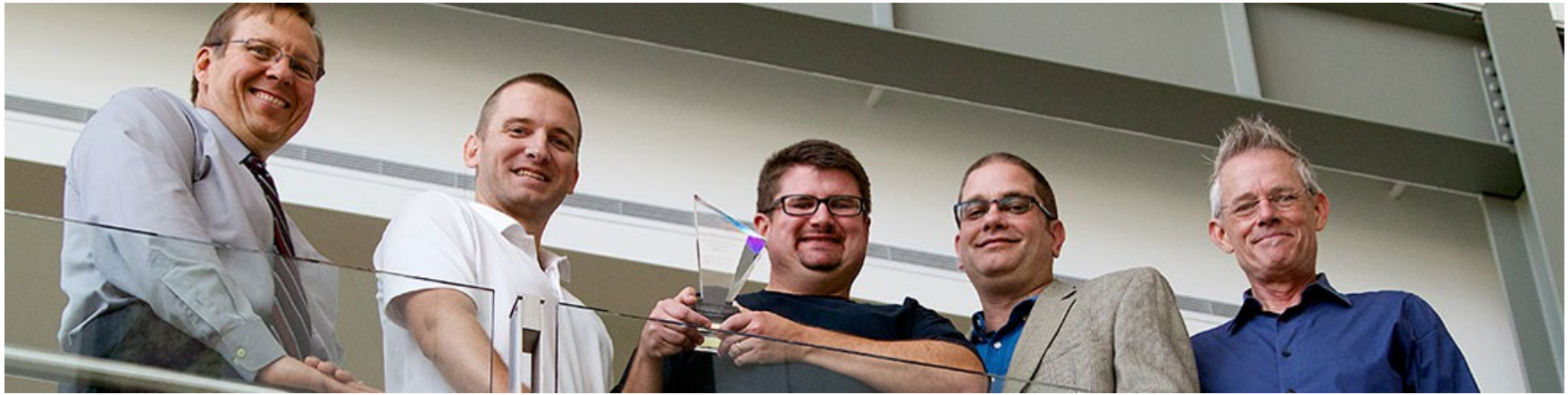
Iterative Changes

- Expanded Detail
- UI / Usability

Architecture

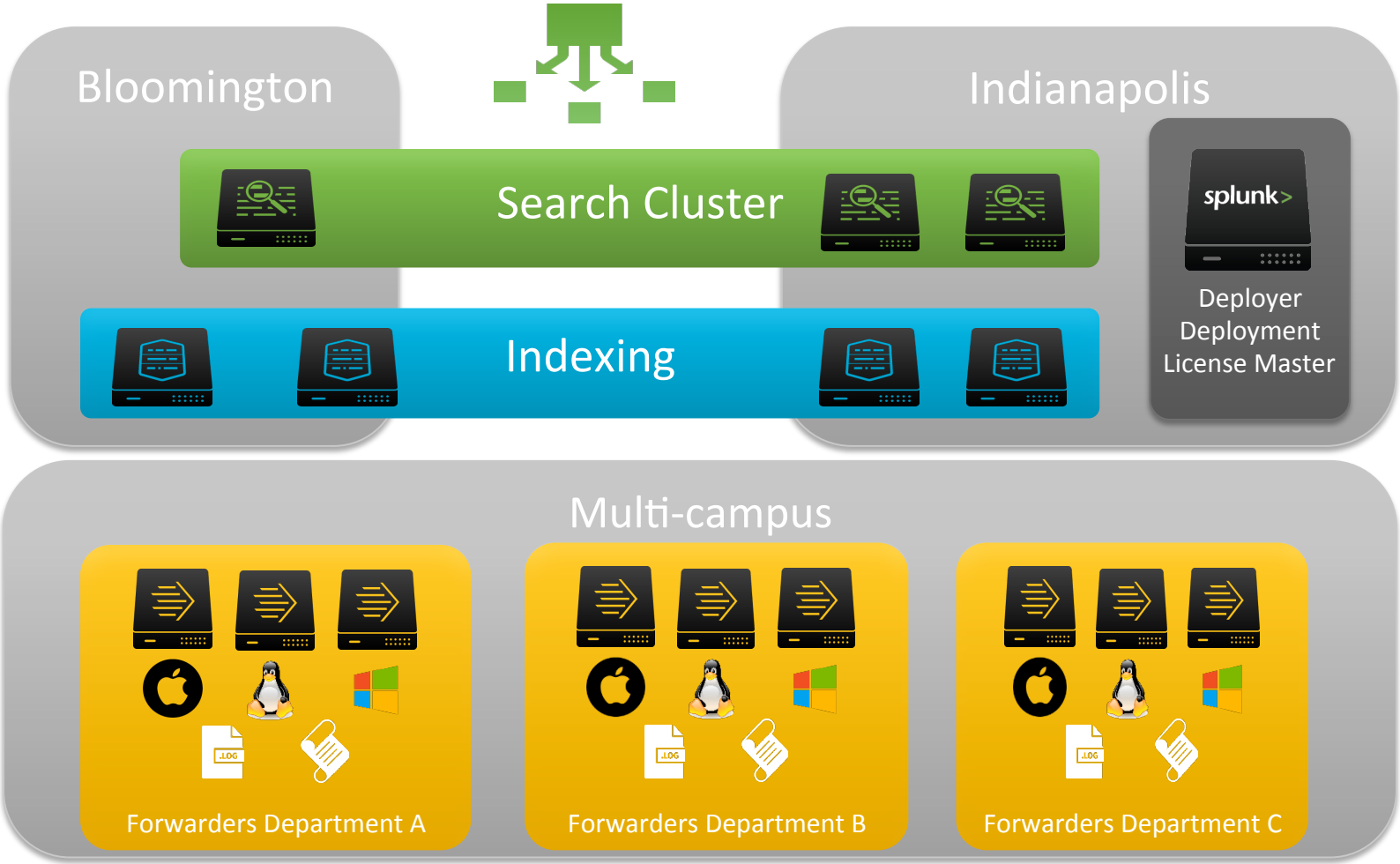
splunk>

Indiana University Storage and Virtualization



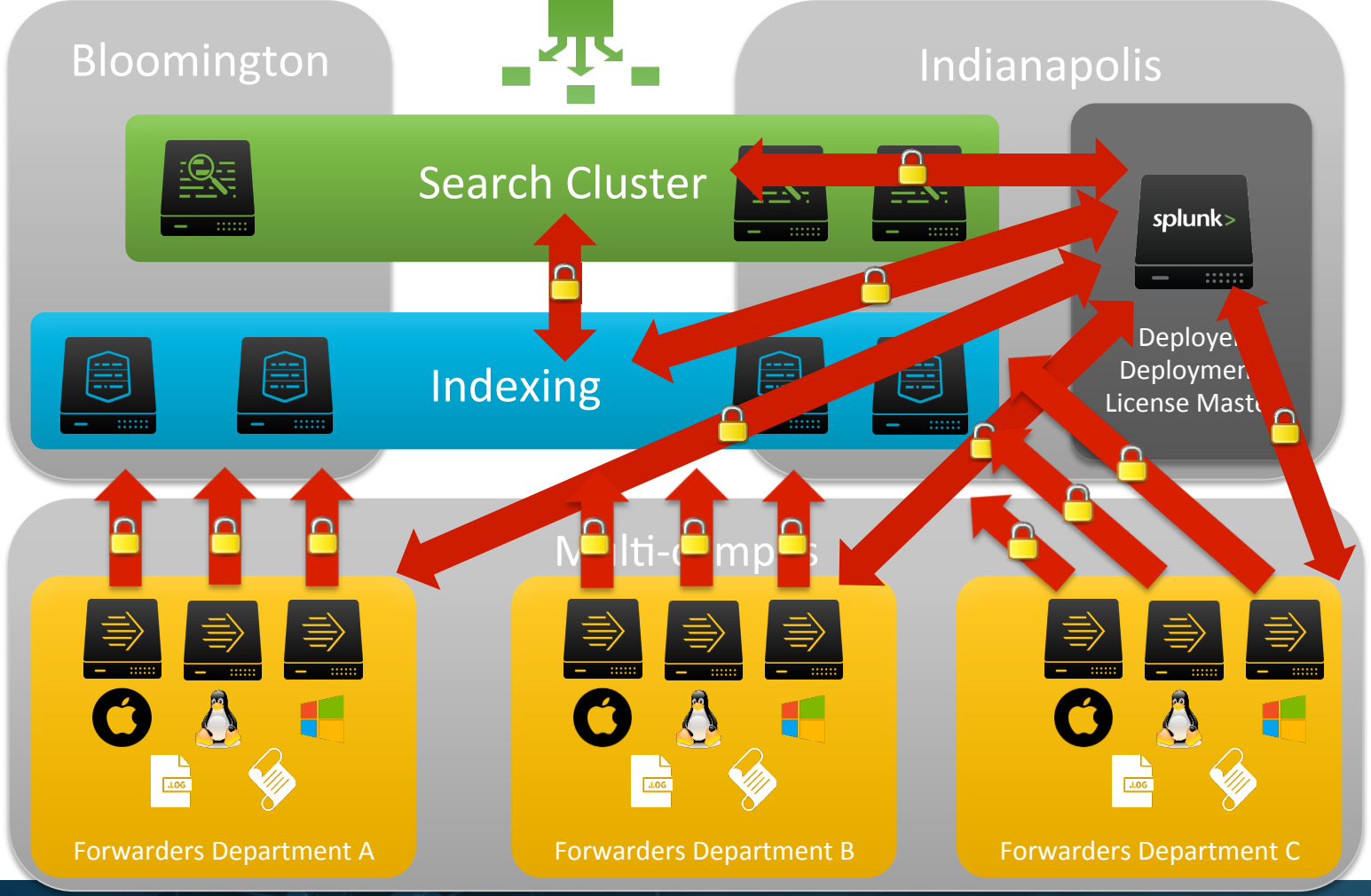
VMware ESX Physical Hardware

- Dell PowerEdge M620 - 20 CPU cores 3GHz, E5-2690
- 512GB Memory - DDR3
- Hitachi VSP G1000 SAN


Bloomington
Indianapolis
Search Cluster
Indexing
splunk>
Deployer
Deployment
License Master
Multi-campus
Forwarders Department A
Forwarders Department B
Forwarders Department C

Performance Statistics

- IOPS > 1062 Via Bonnie++
- ~270,000 Events per second dense search in smart mode
- ~5400 Events per second sparse search in smart mode


Bloomington
Indianapolis
Search Cluster
splunk>
Indexing
Deploye
Deploymer
License Mast
Forwarders Department A
Forwarders Department B
Forwarders Department C

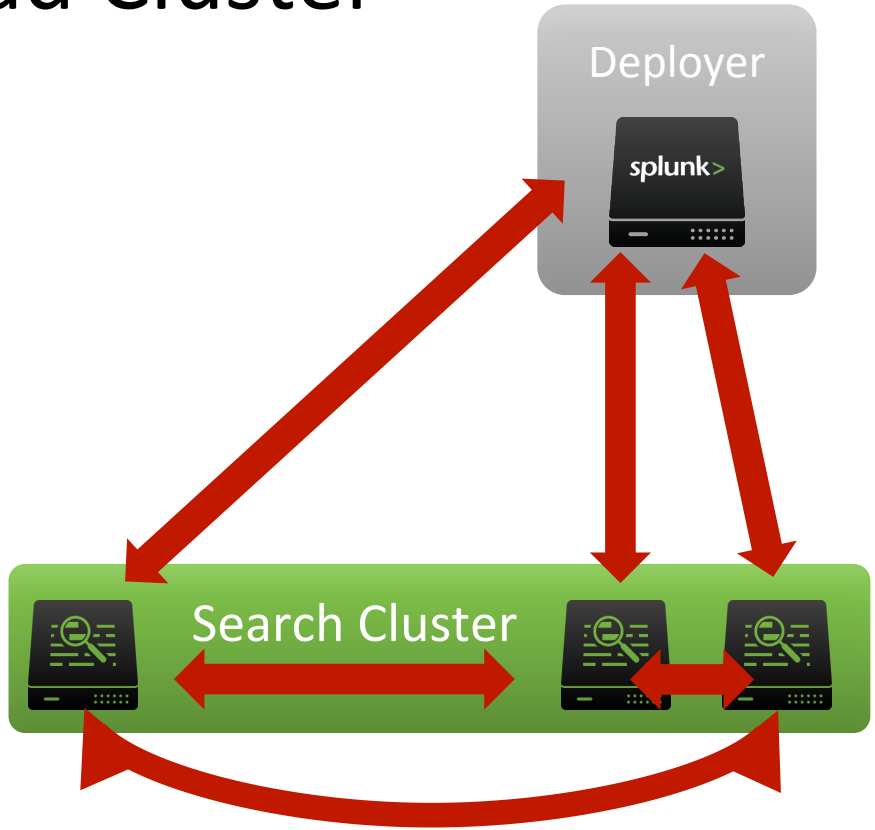

HELP!

Scalable Architecture

splunk>

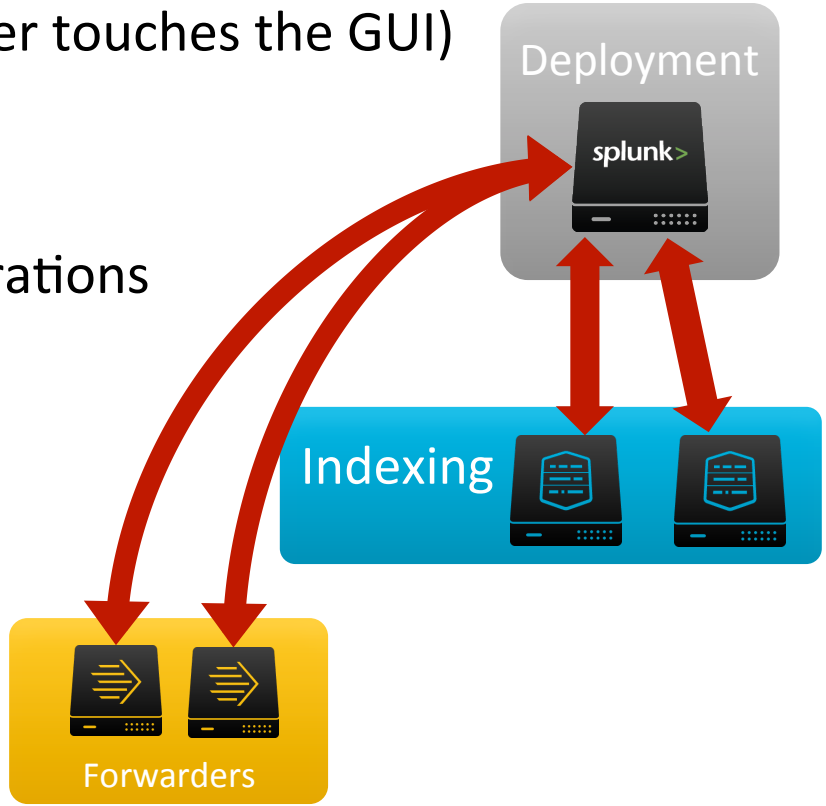
Search Head Cluster

- Use of a deployer
- Knowledge object replication
- Additional search head expansion



Deployment Server
(For the admin that never touches the GUI)

- Houses all important Splunk configurations
  - Indexer configurations
  - Configuration push to 2000+ servers



Departmental on-boarding

splunk>

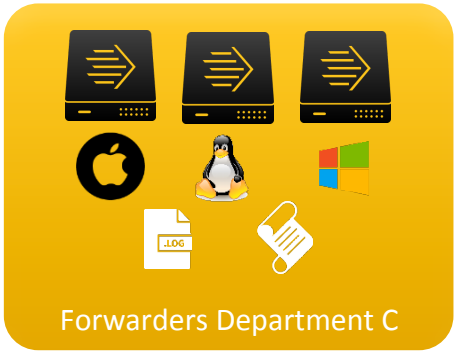

Search Cluster


Indexing


splunk>
Deployer
Deployment
License Master

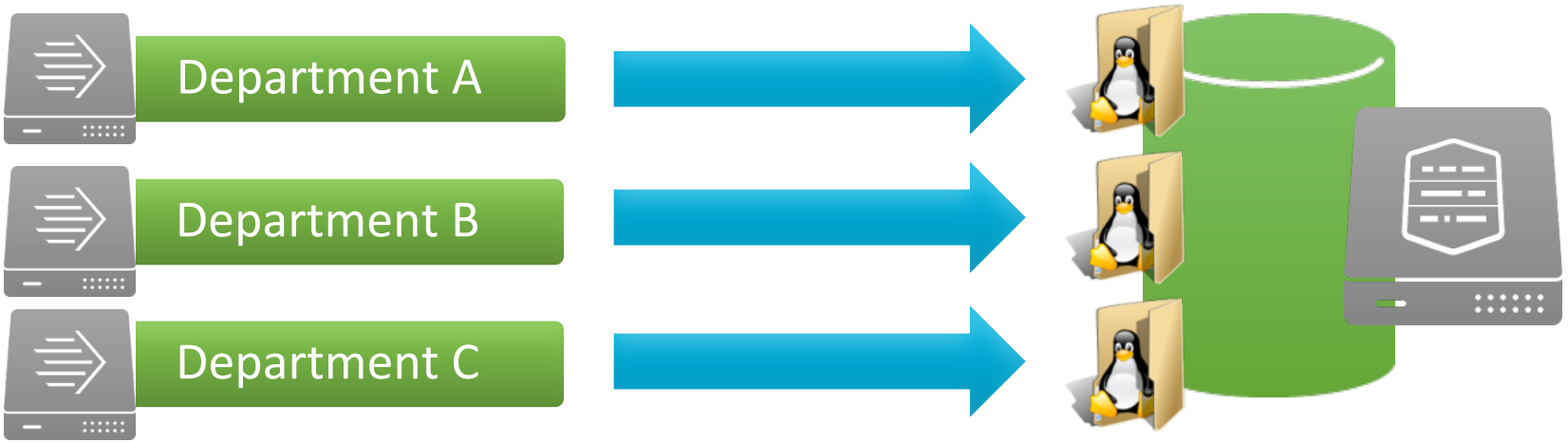

Forwarders Department A


Forwarders Department B


Forwarders Department C

Data Silos by Tenant

Each department has a unique index



Making Deployment Easier

splunk>

Overcoming Distributed IT Administration

- NO ADMIN RIGHTS
  - Solution: Each department gets a shared Box folder
    - Splunk Universal Forwarder
    - Installation scripts
    - How to docs

- SCCM (Windows) or Ansible (Linux) helps a great deal

- The magic of deploymentclient.conf

Simplify Onboarding

Using an Onboard Script on Our Deployment Server

```
#################################################
#################################################
### Splunk> Client Onboarding  Script        ###
### Author:   Daniel Daily                   ###
### Version:  1.0                            ###
#################################################
#################################################


red='\033[0;31m'
yellow='\033[1;33m'
NC='\033[0m'
hostname=$(/bin/hostname)
old_cron=$(awk -F"[ ]" '/^cron_schedule/ {print $1,$2,$3;exit;}' /opt/splunk/etc
/shcluster/apps/it12_template/local/savedsearches.conf)
new_cron=$(awk -F"[ ]" '/^cron_schedule/ {print $1,$2,$3+1;exit;}' /opt/splunk/e
tc/shcluster/apps/it12_template/local/savedsearches.conf)
cron_number=$(awk -F"[ ]" '/^cron_schedule/ {print $3+1;exit;}' /opt/splunk/etc/
shcluster/apps/it12_template/local/savedsearches.conf)
PS3='Select an option and press Enter: '

if [[ $USER != "splunk" ]]; then
     echo -e "${red}This script must be run as the splunk user!!${NC}"
     exit 1
else

     echo -e "${yellow}What is the client name?${NC}"
     read client
fi

client=$(echo $client | tr '[A-Z]' '[a-z]')

CLIENT=${client^^}

echo -e "${red}Lets add the serverclasses!${NC}"

sleep 2

echo -e "${yellow}What location will the new groups servers be sent to?${NC}"

select location in Indianapolis Bloomington Both ; do
     case $location in
          "Indianapolis") echo -e "${yellow}What OS will be needed in Indianap
olis?${NC}"
                     select OS in "Windows" "Unix" "Both-Windows and Unix" ; d
```

- Checks user logon
- Asks for location, OS type (user input phase)
- Adds server classes and indexes
- Copies source application template
- Replaces department variables
- Assigns roles (authorize.conf, authentication.conf)
- Assigns a default_namespace

Script Details

- Script executes the .msi silently then stops the Splunk service
- Defines location, OS, Department & Host
- Injects these variables into the deploymentclient.conf file
- Assigns the client a deployment server
- Starts the service so it can phone home



- Verifies if Splunk is installed
- Installs via package or tar.gz
- Configures Deploymentclient.conf
- Modifies auditd.conf for Splunk access
- Configures Splunk to start on boot
- Sets ownership and permissions

<u>Differences</u>

- Dropping all unnecessary event IDs
- Ingesting full auditd

Script to Deploy to Many

One script to install them all

- Mass deployment of forwarder to 600+ servers remotely.

remoteinstallsplunk.ps1*

```
#get list of pcs
$computername = Get-Content 'C:\Parkinglot\splunkmsi\serverlist.txt'

#get the location of the msi for splunk Universal Forwarder
# this line declares your copy from locations. you need to copy both msi if you are not sure 32 bit or 64 bit
$sourcefile1 = "\\HOSTNAME\c$\Parkinglot\Splunkmsi\splunkforwarder-6.2.3-264376-x64-release.msi"
$sourcefile2 = "\\HOSTNAME\c$\Parkinglot\splunkmsi\splunkforwarder-6.2.3-264376-x86-release.msi"

#This will copy splunk files then launch the installer script
foreach ($computer in $computername)
{
    $destinationFolder = "\\$computer\C$\splunkfiles\"
    $s = new-pssession -computername $computer #-credential ads\hnetkah #(only if needed)

#This section will copy the $sourcefile to the $destinationfolder. If the Folder does not exist it will create it.
    if (!(Test-Path -path $destinationFolder))
    {
        New-Item $destinationFolder -Type Directory
    }
    Copy-Item -Path $sourcefile1, $sourcefile2 -Destination $destinationFolder
    #launch installer script --remote on machine destination
    # the script lives on your 'runfrom' machine in the below drectory (if not exsist create it!) it will be then run on the destination server in your serverlist.txt
    Invoke-Command -ComputerName $computer  "c:\Splunkfiles\script.ps1"
}
```

App Dev Phases

splunk>

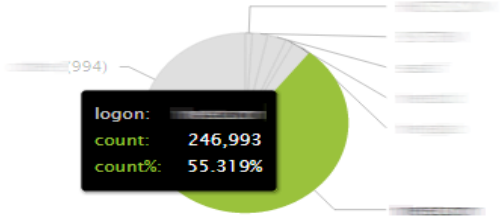
VERSION 1

IT-12

This Dashboard shows all information for IT-12

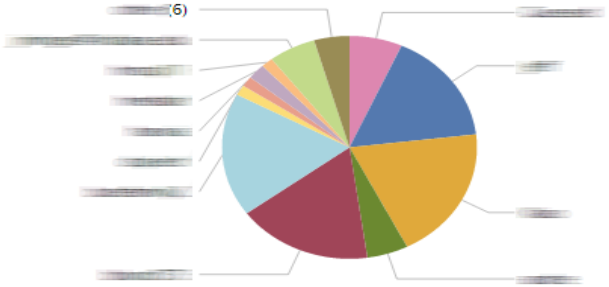
All Successful Logins

2h ago



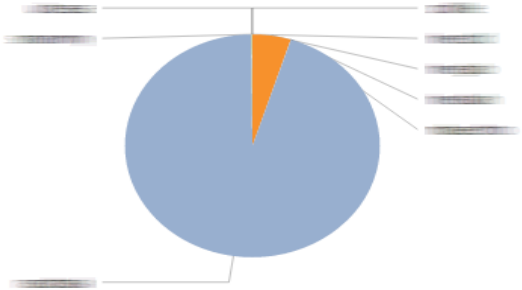
All Failed Logons

2h ago



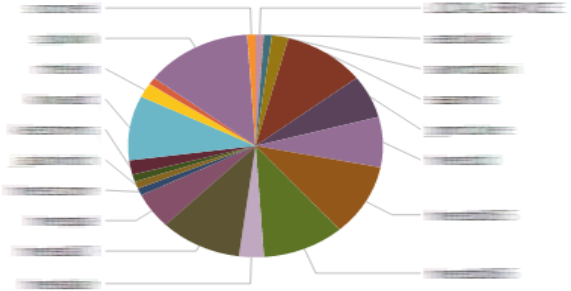
All Successful File Access By User

2h ago



All Failed File Access By User

2h ago



VERSION 1

Failed File Access

Notice: If searching for a "\" in File Path you must enter a second " \" Example: "D:\\"

User: × All | Host: × All | File Path: * | Last 24 hours | Submit

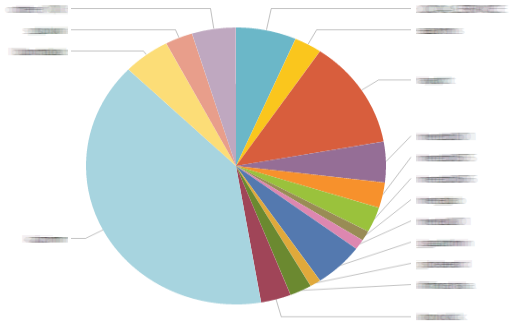
11m ago

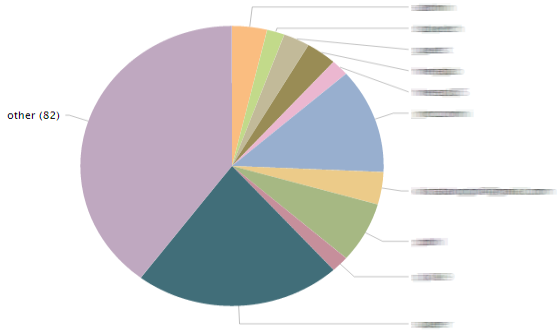
Time	Host	User	File Path	Raw Log
08/31/2015 18:04:43.49	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:04:43.499:73637) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:04:43.499:73637) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308c416178 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xc items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:03:41.88	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:03:41.887:73636) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:03:41.887:73636) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f3087237118 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0x16 items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:03:06.2	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:03:06.206:73635) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:03:06.206:73635) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f307f94b478 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0x10 items=1 ppid=1 pid=15631 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:02:40.34	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:02:40.346:73634) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:02:40.346:73634) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308a44fb18 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xb items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:01:38.44	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:01:38.444:73633) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:01:38.444:73633) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308c6474b8 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xd items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:01:05.93	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:01:05.938:73632) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:01:05.938:73632) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308c645338 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0x10 items=1 ppid=1 pid=15631 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 18:00:36.07	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 18:00:36.074:73625) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 18:00:36.074:73625) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f3085521818 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xd items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 17:54:43.13	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 17:54:43.135:73618) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 17:54:43.135:73618) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308cd90b38 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xc items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)
08/31/2015 17:53:41.74	[redacted]	splunk	/opt/splunk/etc/users/[redacted]	type=PATH msg=audit(08/31/2015 17:53:41.741:73617) : item=0 name=/opt/splunk/etc/users/[redacted] inode=2099841 dev=fd:02 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=unconfined_u:object_r:file_t:s0 nametype=NORMAL type=SYSCALL msg=audit(08/31/2015 17:53:41.741:73617) : arch=x86_64 syscall=open success=no exit=-13(Permission denied) a0=0x7f308183ac98 a1=O_RDONLY|O_NONBLOCK|O_DIRECTORY|O_CLOEXEC a2=0x2 a3=0xd items=1 ppid=1 pid=15632 auid=[redacted] uid=splunk gid=splunk euid=splunk suid=splunk fsuid=splunk egid=splunk sgid=splunk fsgid=splunk tty=(none) ses=1804 comm=splunkd exe=/opt/splunk/bin/splunkd subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)

Lessons Learned

- Training
- Optimizing Searches
- Data Inputs
- Reporting

VERSION 2





Failed File Access Total

	logon	host	count	total
1			135	135
2			43	43
3			22	22
4			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	18

Failed User Logons Total

logon	host	count	total
		47	47
		26	26
		15	15
		8	8
		8	8

« prev 1 2 3 4 5 6 7 8 9 10 next »

VERSION 2

Failed File Access

Notice: All boxes must contain at least one selection.

User [redacted] | Host All | File Path * | Exclude Logon NONE | Exclude Host NONE | Exclude File Path NONE | Last 24 hours | Submit

<1m ago

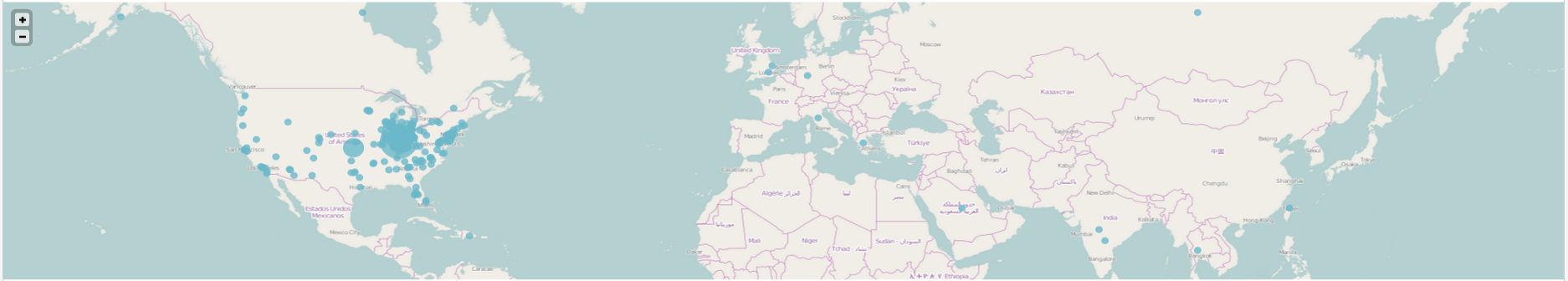
Time	Host	User	File Path	Raw Log
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015516 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: SYNCHRONIZE ReadData (or ListDirectory) ReadAttributes Access Reasons: SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadAttributes: Granted by ACE on parent folder D:(A;OICIID;FA;;;S-1-5-21-1085031214-1292428093-527237240-83581) Access Mask: 0x100081 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015515 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: SYNCHRONIZE ReadData (or ListDirectory) ReadAttributes Access Reasons: SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadAttributes: Granted by ACE on parent folder D:(A;OICIID;FA;;;S-1-5-21-1085031214-1292428093-527237240-83581) Access Mask: 0x100081 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]\Desktop\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015514 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015513 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Desktop\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015512 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015511 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015510 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Links\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015509 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Links\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015 09:21:04	[redacted]	[redacted]	D:\Redirects\IU-HNET\[redacted]Favorites\desktop.ini	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info RecordNumber=17015508 Keywords=Audit Failure Message=A handle to an object was requested. Subject: Security ID:[redacted] Account Name: kzimm Account Domain: ADS Logon ID: 0x207EA822 Object: Object Server: Security Object Type: File Object Name: D:\Redirects\IU-HNET\[redacted]Favorites\desktop.ini Handle ID: 0x0 Resource Attributes: - Process Information: Process ID: 0x4 Process Name: Access Request Information: Transaction ID: {00000000-0000-0000-0000-000000000000} Accesses: READ_CONTROL SYNCHRONIZE ReadData (or ListDirectory) ReadEA ReadAttributes Access Reasons: READ_CONTROL: Not granted SYNCHRONIZE: Not granted ReadData (or ListDirectory): Not granted ReadEA: Not granted ReadAttributes: Not granted Access Mask: 0x120089 Privileges Used for Access Check: - Restricted SID Count: 0
09/08/2015	[redacted]	[redacted]	D:\Redirects\IU-	09/08/2015 09:21:04 AM LogName=Security SourceName=Microsoft Windows security auditing. EventCode=4656 EventType=0 Type=Information ComputerName=[redacted] TaskCategory=File System OpCode=Info

Expansion of Services

splunk>

Failed Authentication Count by Location for the last 4 hours

1m ago



Failed Authentication Attempts in the Last 4 hours by Client IP

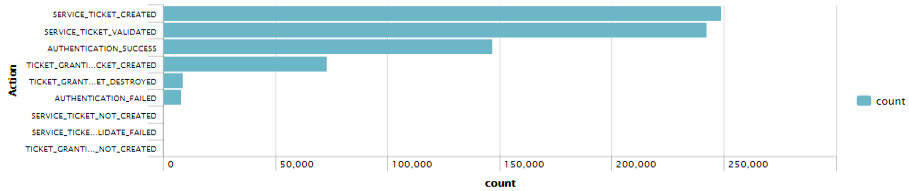
1m ago

client_ip	City	Country	Region	lat	lon	count
[redacted]	Absecon	United States	New Jersey	39.48990	-74.47730	68
[redacted]		United States		38.00000	-97.00000	66
[redacted]		United States		38.00000	-97.00000	65
[redacted]	New Albany	United States	Indiana	38.28130	-85.84010	55
[redacted]	Plainfield	United States	Indiana	39.68580	-86.41060	31
[redacted]		United States		38.00000	-97.00000	28
[redacted]		United States		38.00000	-97.00000	27
[redacted]	Indianapolis	United States	Indiana	39.76840	-86.15800	23
[redacted]	Bloomington	United States	Indiana	39.24990	-86.45550	21
[redacted]	South Bend	United States	Indiana	41.67680	-86.21610	20

« prev 1 2 3 4 5 6 7 8 9 10 next »

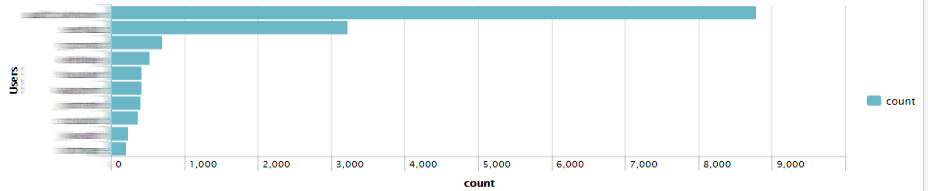
CAS Actions taken over the last 4 hours

1m ago



Number of Actions taken by CAS Users over the last 4 hours

1m ago



Top 10 Service Ticket Created by Service for the last 4 hours

1m ago

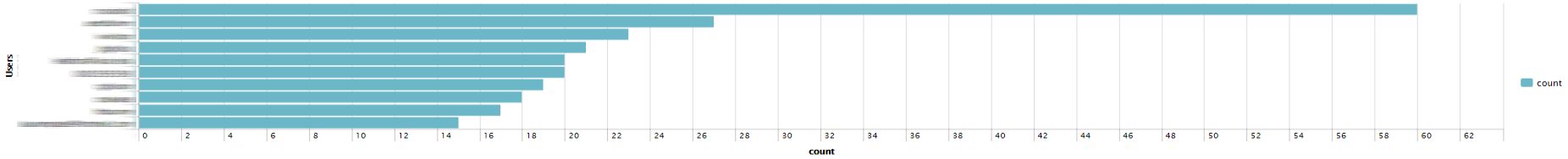
Top 10 Service Ticket Created by Service for the last 4 hours

1m ago

Action	url	count	percent
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/SSERV/SISSELFSERVICE/CS/c/SA_LEARNER_SERVICES.SSS_STUDENT_CENTER.GBL?	3457	38.445285
SERVICE_TICKET_CREATED	https%3A%2F%2Fsis.iu.edu%2Fpsp%2FPS1PRD%2FIU%2FCS%2Fh%2F%3Ftab%3DDEFAULT	1045	11.621441
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/SSERV/SISSELFSERVICE/CS/c/SA_LEARNER_SERVICES.SSR_SSENRL_LIST.GBL?	863	9.597420
SERVICE_TICKET_CREATED	https%3A%2F%2Fhrself.iu.edu%2Fpsp%2FHRSELF_newwin%2FHRSELFSERVICE%2FHRMS%2Fc%2FROLE_EMPLOYEE.IU_HRSS_ACK.GBL%3FIU_HRSS_ACK_TYPE%3DSSPC	435	4.837633
SERVICE_TICKET_CREATED	https%3A%2F%2Fsis.iu.edu%2Fpsp%2FPS1PRD%2FIU%2FCS%2Fc%2FSSR_ADVISEE_OVRD.IU_SS_ADMIN_CENTER.GBL%3F	240	2.669039
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/PSFAC/SISSELFSERVICE/CS/c/SA_LEARNING_MANAGEMENT.SS_FACULTY.GBL?	211	2.346530
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/SSERV/SISSELFSERVICE/CS/c/SA_LEARNER_SERVICES.SS_ADM_APP_STATUS.GBL?	134	1.490214
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/SSERV/SISSELFSERVICE/CS/c/CC_PORTFOLIO.SS_CC_DEMOG_DATA.GBL?	129	1.434609
SERVICE_TICKET_CREATED	https%3A%2F%2Fhrms.iu.edu%2Fpsp%2FPH1PRD%2FIU%2FHRMS%2Fh%2F%3Ftab%3DDEFAULT	118	1.312278
SERVICE_TICKET_CREATED	https://iuself.iu.edu/psp/SSERV/SISSELFSERVICE/CS/c/SA_LEARNER_SERVICES.SSR_SSENRL_GRADE.GBL?	105	1.167705

Top 10 Users who Failed to Authenticate in the last 4 hours

1m ago



Shibboleth Users and Services over the last 4 hours

1m ago

Date	principalName	relyingPartyId	auditEventTime
09/08/2015 20:38:11.000000	[redacted]	http://iu.instructure.com/saml2	20150908T203811Z
09/08/2015 20:38:11.000000	[redacted]	google.com	20150908T203811Z
09/08/2015 20:38:10.000000	[redacted]	http://iu.instructure.com/saml2	20150908T203810Z
09/08/2015 20:38:10.000000	[redacted]	http://iu.instructure.com/saml2	20150908T203810Z
09/08/2015 20:38:10.000000	[redacted]	http://iu.instructure.com/saml2	20150908T203810Z
09/08/2015 20:38:09.000000	[redacted]	google.com	20150908T203809Z
09/08/2015 20:38:09.000000	[redacted]	google.com	20150908T203809Z
09/08/2015 20:38:09.000000	[redacted]	google.com	20150908T203809Z
09/08/2015 20:38:08.000000	[redacted]	google.com	20150908T203808Z
09/08/2015 20:38:09.000000	[redacted]	http://iu.instructure.com/saml2	20150908T203809Z

« prev 1 2 3 4 5 6 7 8 9 10 next »

Failed Authentication by IP with list of User names

1m ago

client_ip	Users	count	total
[redacted]	0003005671	1	68
	0003146506	1	
	0003186751	1	
	0003300434	1	
	0003482799	1	
	0003513476	2	

Down the Road

- Further development IT-12 application for departments
- Expand UITS I.T. Ops.

Questions?

splunk>

THANK YOU

splunk>