comforte

GTUG
German NonStop User Group e.V.
Member of Connect Deutschland

GTUG Präsentation 17. Nov. 2021

Helmut Bernhard
Senior Solutions Architect

AGENDA

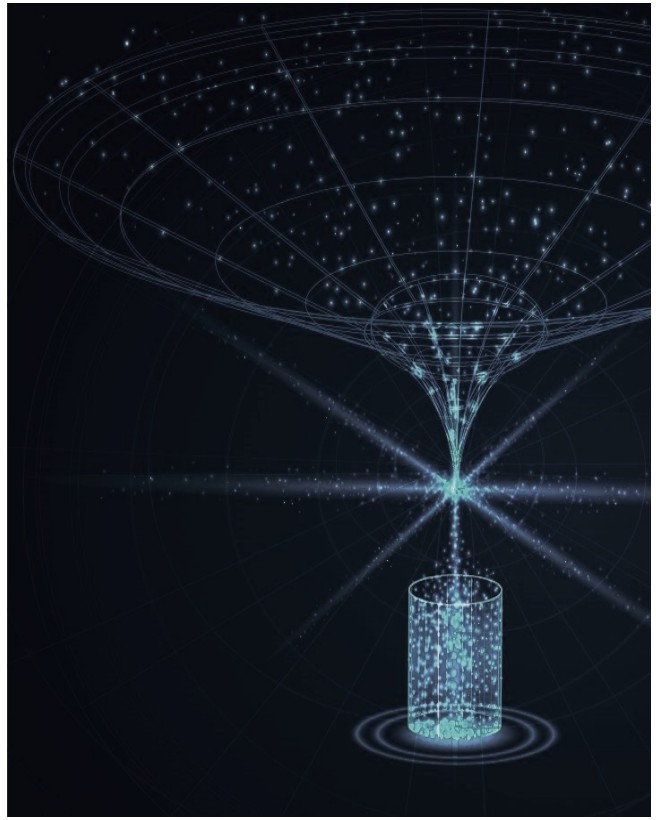
- SafePoint LogStream
- uLinga for Kafka
- TOP
- Outlook for next GTUG

© 2021 comforte, Inc. All rights reserved

Modern LogStreaming on NonStop

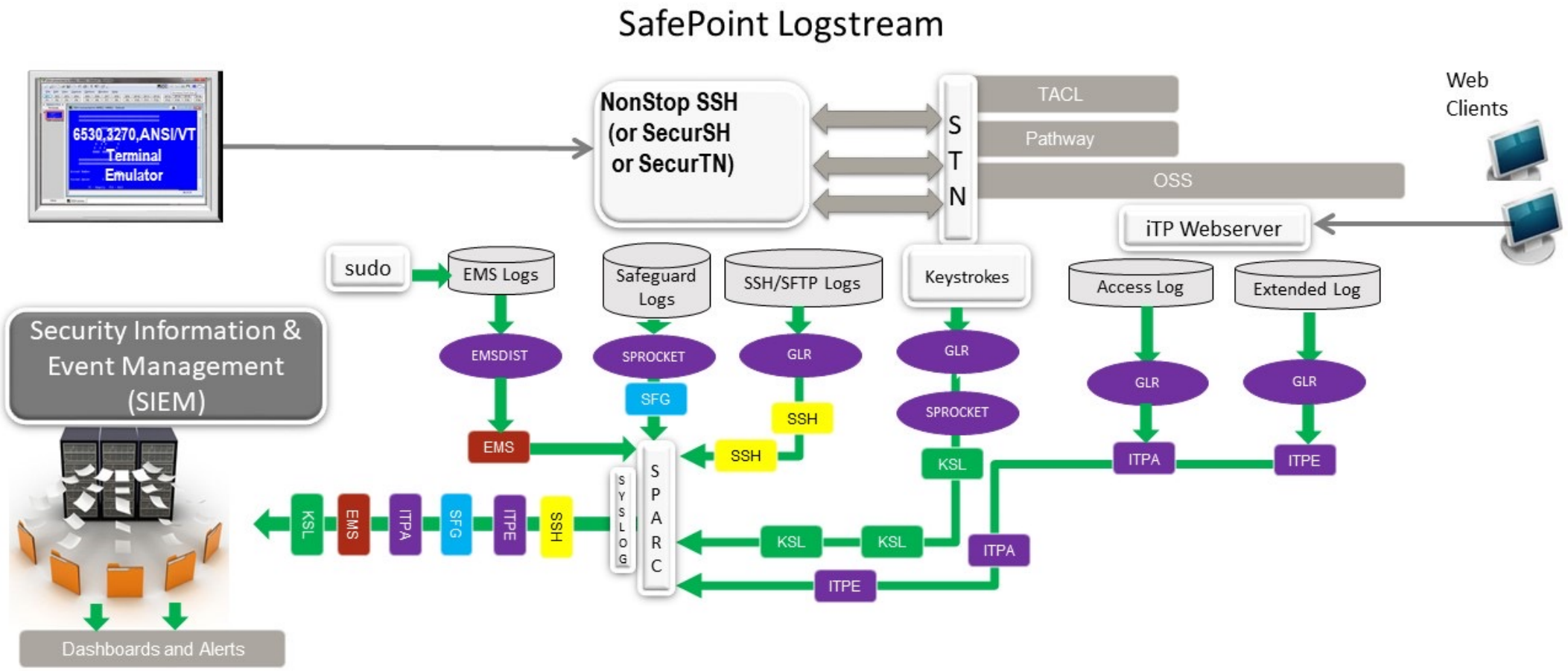
Requirements

- Compliant with data privacy and governance rules per country, per sector (e.g. PCI-DSS)
- Decision criterias for migrating to new architectures, e.g. ZT
- Besides SYSLOG outbound capabilities like ZIP, SFTP, etc.
- Using the Nonstop fundamentals
  - High performance parallel processing of multiple audit trails on multiple machines
  - Fault tolerant and real-time
  - Fully automated, i.e. self-healing and self-restarting
- Relational database searches can find key events and trends
- Dashboards for easy monitoring of status and events
- Prebuilt dashboards and panels provide easy customization for NonStop
- Real-time alerting via dashboards and Splunk Alerts



© 2021 comforte, Inc. All rights reserved

NonStop Data Analytics: Collecting & Streaming the Data



NonStop data is sent off the NonStop onto an Enterprise-wide SIEM where data from other platforms also resides. It is then available for real-time and forensic analysis, perhaps in context with data from other platforms.

© 2021 comforte, Inc. All rights reserved

NonStop Data Analytics: Many Raw Data Sources, Many Data Formats

ITP WEBSERVER:

```
10.126.17.10 - - [20/Sep/2020:12:17:10 -0900] "GET /g9/menu.js HTTP/1.1" 304 0
log {start 1547814747.391934} {addr 10.0.0.178} {port 99} {method GET} {url /} {agent
{Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/71.0.3578.98 Safari/537.36}} {status 200} {end 1547814747.392899} {host
172.16.125.7}log {start 1547814747.969273} {addr 10.0.0.178} {port 99} {method GET} {url
/favicon.ico} {agent {Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36}} {referrer http://10.0.0.178:99/}
{error {(#90) file not found}} {status 404} {end 1547814747.969696}
```

SSH:

```
$SSH00|26Aug20 02:52:09.82|50|10.104.2.249:50465:10.10.10.105: accepted connection from
client $SSH00|26Aug20 02:52:09.83|50|10.104.2.249:50465:10.10.10.105: client version string:
SSH-2.0-OpenSSH_8.1$SSH00|26Aug20 02:52:10.37|50|10.104.2.249:50465:10.10.10.105: key-
exchange done and server authentication by client successful. $SSH00|26Aug20
02:52:10.39|40|10.104.2.249:50465:10.10.10.105: SSH session established.  $SSH00|26Aug20
02:52:10.76|40|10.104.2.249:50465:10.10.10.105: signature ok, authentication of comf.js
successful$SSH00|26Aug20 02:52:10.99|50|10.104.2.249:50465:10.10.10.105: channel request for
```

KEYSTROKE:

```
\PROD02 $Y2XY   $SYSTEM SYS04   TACL   safecom thaw user comf.lee
\PROD04 $Y2XY   $SYSTEM SYS04   TACL   who —Ï¡\PROD04 $JSTN8  #Z00
ò×%o%<;¬}aÿÿ€joel_sandberg                    \PROD04 $Y2XY   $SYSTEM SYS04   TACL
```

SAFEGUARD:

```
\PROD04.$SYSTEM.TOPS.MIP7=COMF.LEE  3n=COMF.LEE  PROD04 \PROD04.$MIP
\PROD04.$YMIOP.#CLCI  ·SUPER.SUPER   SUPER.SUPER    \PROD04.$ZSMP   TANDEM  SEC.SUPER
```

EMS:

```
\PROD02.$BFT00:111034649þF   \PROD02.$SYSTEM.ZSSH.SSH2 ÿ dTANDEM    r10|Could not listen on
process $ZTC2D, interface 0.0.0.0, port 8422: Socket: bind operation failed with error 4114ÿä Ê
ĂCOMFORTE É        ÿþ# @ èòÖ¸q¡%òÖ¸q¡Þÿÿ     þ   .     \PROD02.$BFT00:111034649þF
\PROD02.$SYSTEM.ZSSH.SSH2 ÿ dTANDEM    #10|Retrying to listen…
```

© 2021 comforte, Inc. All rights reserved

NonStop Data Analytics: Normalizing the Data

SafePoint Logstream

- Garbage in, garbage out. Data is only as useful as its quality. Normalization is the key.
- Distinct data fields within raw data records are parsed and mapped into distinct field names, and stored in an indexed relational database.
- *Database normalization is a process used to organize a database into tables and columns.* Columns are attributes, tables are relations.
- Some data (Safeguard audit) is normalized on the NonStop side prior to streaming to SIEM. Some is normalized in the SIEM.
- Splunk can normalize all data:
  - Splunk Field Extraction is the process by which Splunk extracts fields from raw data.
  - CIM (Common Information Model) is an open standard for normalizing data. Logstream uses CIM to normalize much of the NonStop data from EMS, SSH, iTP Webserver, and other sources.

© 2021 comforte, Inc. All rights reserved

Normalized NonStop Data in Splunk

Search Results: Data is a normalized collection of NonStop Attribute=Value pairs

Search | Splunk 8.0.4.1 | NonStop Security Analytics, Fron | Data Security Services | comforte | Search | Splunk 8.0.4.1

localhost:8000/en-US/app/SPLogstream1/search?q=search%20index%3D*%20"operation-detail%3DRENAME"&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=-7d%40h...

Git - Reference | Projects · Dashboar... | conanfile.py referen... | introduction-to-git.... | New folder | Bash Scripting Bash... | Splunk Training Das... | Login | Splunk | 501c3 IRS Annual... | 501c3 CA filing req... | Delaware Annual R... | Michigan | Internal... | Taxes - Nonprofit In...

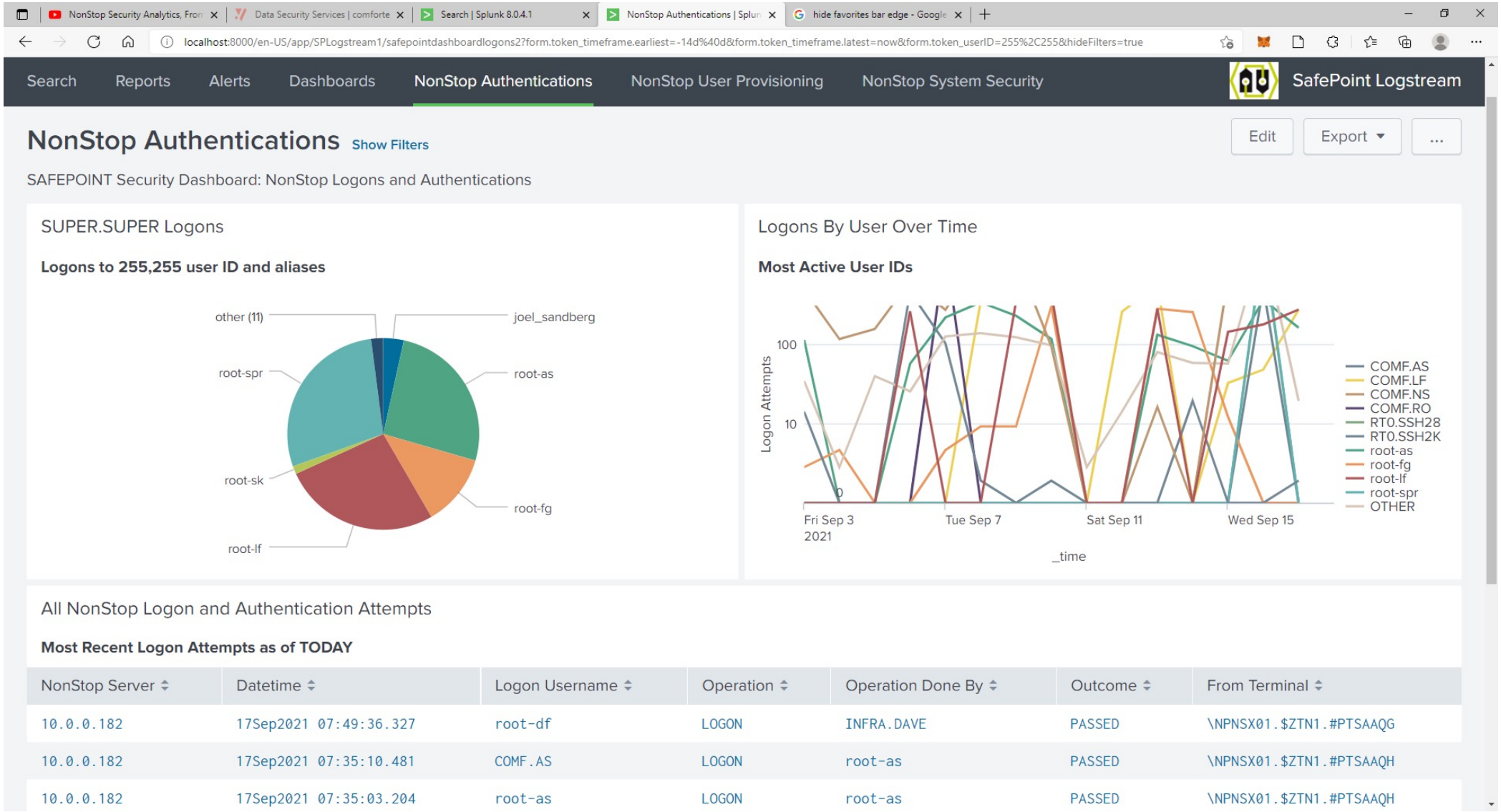
> Show Fields List ▾ Format 20 Per Page ▾

i	Time	Event
>	9/10/21 1:08:48.492 PM	<85>Sep 15 00:02:33 10.0.0.178 CEF:0|comforte|SafePoint Logstream|2.10|00307|RENAME|5|SUBSYSTEM=FUP SYSTEMNAME=\NPNSX01 TERMINALNAME=\NPNSX01.$ZPTY.#ZWN3695 DATETIME=10Sep2021 13:08:48.492 OPERATION=00307 OPERATION-DETAIL=RENAME OBJECTNAME=$FG.SDMAIN.SDATA OBJECTTYPE=DISKFILE OUTCOME=FAILED SUBJECT-PROCESS-NAME=\NPNSX01.$X4Z9 SUBJECT-PROGRAM-NAME=\NPNSX01.$SYSTEM.SYS06.TACL BY-USERNAME=root-fg BY-USERID=255,255 FOR-USERNAME=SUPER.SUPER FOR-USERID=255,255 IP-ADDRESS=0.0.0.0 BEFORE=$FG.SDMAIN.SDATA AFTER=$FG.SDMAIN.SDATA0 BY_USERNAME = root-fg | DATETIME = 10Sep2021 13:08:48.492 | IP_ADDRESS = 0.0.0.0 | OBJECTNAME = $FG.SDMAIN.SDATA \| OBJECTTYPE = DISKFILE \| OPERATION_DETAIL = RENAME \| OUTCOME = FAILED \| SUBJECT_PROCESS_NAME = \NPNSX01.$X4Z9 | byUserID = 255,255 | opDetail = RENAME | sourcetype = NonStop SafePoint

> Show Fields List ▾ Format 20 Per Page ▾

i	Time	Event
>	9/15/21 1:29:56.640 AM	<85>Sep 15 01:41:22 10.0.0.178 CEF:0|comforte|SafePoint Logstream|2.10|00306|ALTER-CI-PRI|5|SUBSYSTEM=SAFE SYSTEMNAME=\NPNSX01 TERMINALNAME=\NPNSX01.$ZTN1.#PTSAAP1 DATETIME=15Sep2021 01:29:56.640 OPERATION=00306 OPERATION-DETAIL=ALTER-CI-PRI OBJECTNAME=SAFEGUARD-CONFIGURATION OBJECTTYPE=SFG-CONFIGURATION OUTCOME=GRANTED SUBJECT-PROCESS-NAME=\NPNSX01.0,1138 SUBJECT-PROGRAM-NAME=\NPNSX01.$SYSTEM.SYS06.SAFECOM BY-USERNAME=joel_sandberg BY-USERID=255,255 FOR-USERNAME=SUPER.SUPER FOR-USERID=255,255 IP-ADDRESS=0.0.0.0 BEFORE=104 AFTER=112 BY_USERNAME = joel_sandberg | DATETIME = 15Sep2021 01:29:56.640 | IP_ADDRESS = 0.0.0.0 | OBJECTNAME = SAFEGUARD-CONFIGURATION | OBJECTTYPE = SFG-CONFIGURATION | OPERATION_DETAIL = ALTER-CI-PRI | OUTCOME = GRANTED | SUBJECT_PROCESS_NAME = \NPNSX01.0 | byUserID = 255,255 | opDetail = ALTER-CI-PRI | sourcetype = NonStop SafePoint

SafePoint Logstream Dashboard Example Monitoring Logon Attempts



© 2021 comforte, Inc. All rights reserved

SafePoint LogStream Dashboard Example Monitoring User Provisioning

NonStop User Provisioning

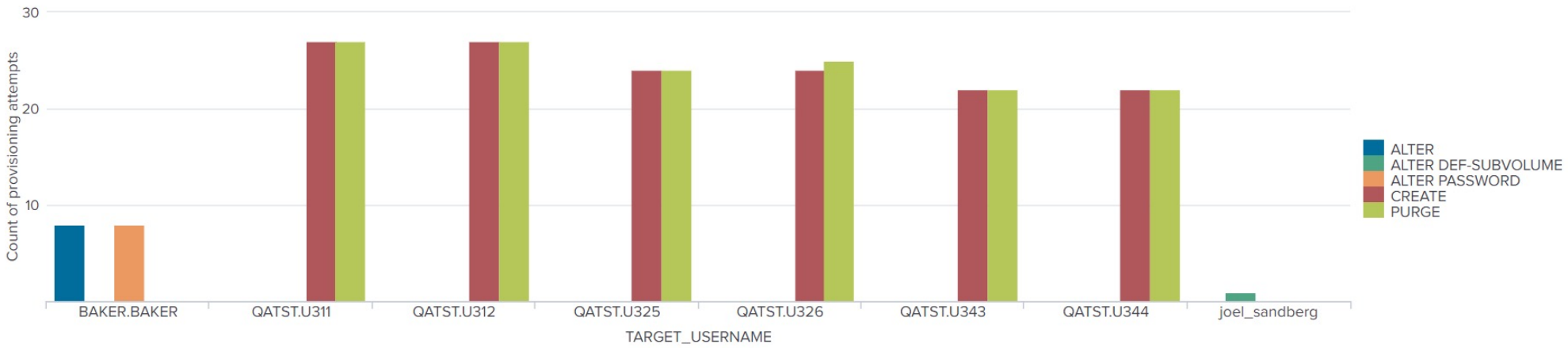
Show Filters

Edit | Export | ...

SAFEPOINT Security Dashboard: User Provisioning

User Provisioning for All Users

Recent Attempts



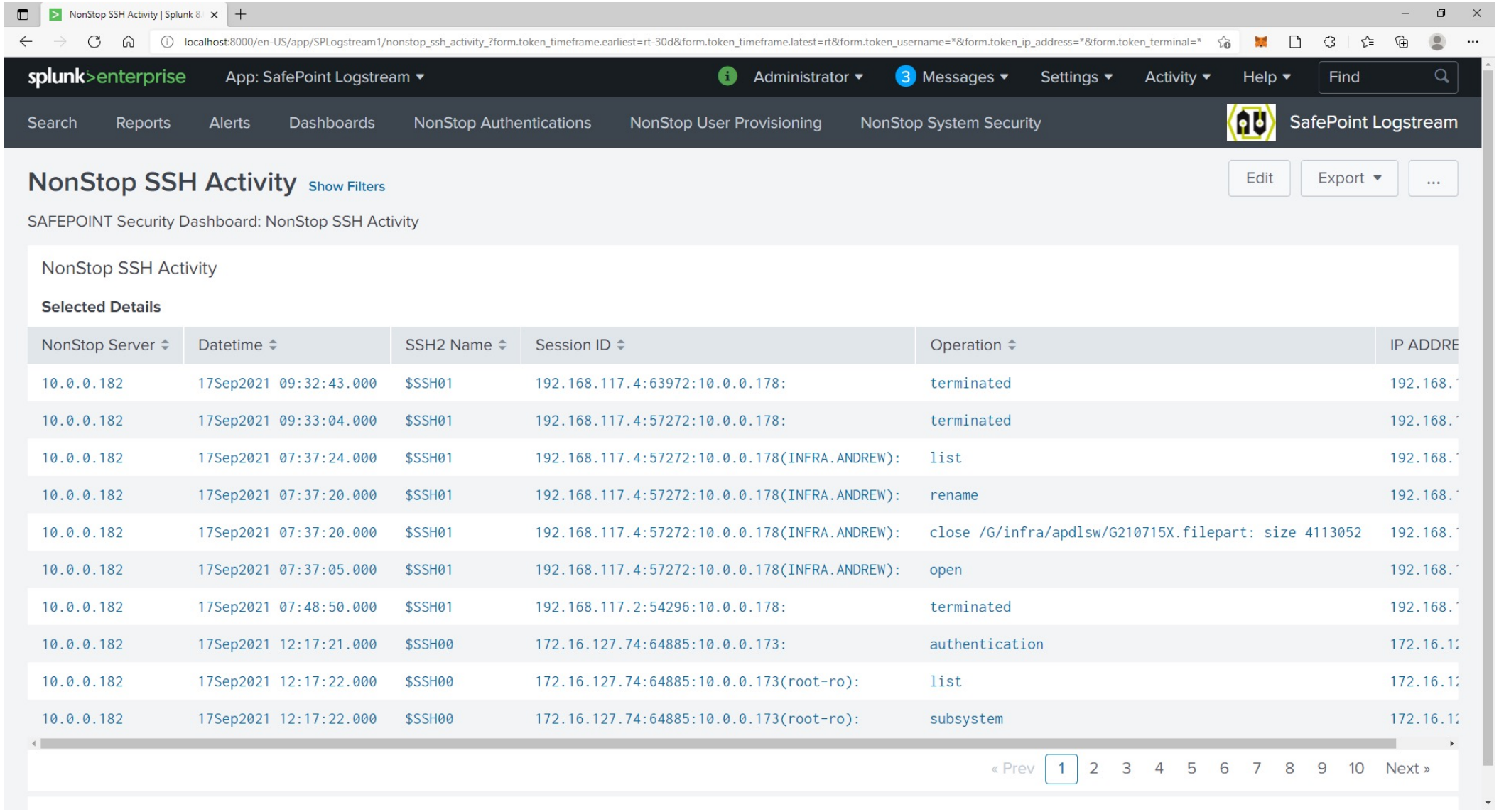
NonStop User Provisioning Attempts

Selected Provisioning Attempt Details

NonStop Server	Datetime	Target Username	Operation	Operation Done By	Outcome	From Terminal
bwns02.comforte.local	09Jul2021 18:09:59.770	QATST.U311	PURGE	root-ro	GRANTED	\BWNS02.$SQ3.#C32.TERM
bwns02.comforte.local	09Jul2021 18:01:36.184	QATST.U311	CREATE	root-ro	GRANTED	\BWNS02.$SQ3.#C32.TERM
bwns02.comforte.local	11Jun2021 18:10:54.149	QATST.U311	PURGE	root-ro	GRANTED	\BWNS02.$SQ.#C32.TERM

© 2021 comforte, Inc. All rights reserved

SafePoint NonStop SSH Activity



NonStop Server	Datetime	SSH2 Name	Session ID	Operation	IP ADDRE
10.0.0.182	17Sep2021 09:32:43.000	$SSH01	192.168.117.4:63972:10.0.0.178:	terminated	192.168.
10.0.0.182	17Sep2021 09:33:04.000	$SSH01	192.168.117.4:57272:10.0.0.178:	terminated	192.168.
10.0.0.182	17Sep2021 07:37:24.000	$SSH01	192.168.117.4:57272:10.0.0.178(INFRA.ANDREW):	list	192.168.
10.0.0.182	17Sep2021 07:37:20.000	$SSH01	192.168.117.4:57272:10.0.0.178(INFRA.ANDREW):	rename	192.168.
10.0.0.182	17Sep2021 07:37:20.000	$SSH01	192.168.117.4:57272:10.0.0.178(INFRA.ANDREW):	close /G/infra/apdlsw/G210715X.filepart: size 4113052	192.168.
10.0.0.182	17Sep2021 07:37:05.000	$SSH01	192.168.117.4:57272:10.0.0.178(INFRA.ANDREW):	open	192.168.
10.0.0.182	17Sep2021 07:48:50.000	$SSH01	192.168.117.2:54296:10.0.0.178:	terminated	192.168.
10.0.0.182	17Sep2021 12:17:21.000	$SSH00	172.16.127.74:64885:10.0.0.173:	authentication	172.16.1
10.0.0.182	17Sep2021 12:17:22.000	$SSH00	172.16.127.74:64885:10.0.0.173(root-ro):	list	172.16.1
10.0.0.182	17Sep2021 12:17:22.000	$SSH00	172.16.127.74:64885:10.0.0.173(root-ro):	subsystem	172.16.1

© 2021 comforte, Inc. All rights reserved

SafePoint Logstream

What are the benefits?

- Fault-tolerant. Utilizes NonStop Process Pairs and Kernel Persistent Processes.
- High performance parallel processing of multiple audit trails.
- Satisfies PCI requirements 10.1, 10.2, 10.3, 10.5, 10.6, 10.7, 11.4, 12.10.5
- Relational database searches can find key events and trends.
- Dashboards for easy monitoring of status and events.
- Prebuilt dashboards and panels provide easy customization for NonStop.
- Real-time alerting via dashboards and Splunk Alerts.
- SafePoint LogStream + SafePoint Splunk App = a turnkey solution for NonStop data analytics.

© 2021 comforte, Inc. All rights reserved

uLinga for Kafka

© 2021 comforte, Inc. All rights reserved

What is Kafka?

Introduction

- Kafka is the most popular open-source stream-processing software for collecting, processing, storing and analyzing data at scale *
- Kafka is used by thousands of companies including 60% of the Fortune 100. Users include Goldman Sachs, Rabobank, Barclays, PayPal in the finance space, and household names including Netflix, Oracle, LinkedIn and AirBnB, among many others
- NonStop applications can be a valuable source of data for Kafka – need a highly performant, simple integration solution

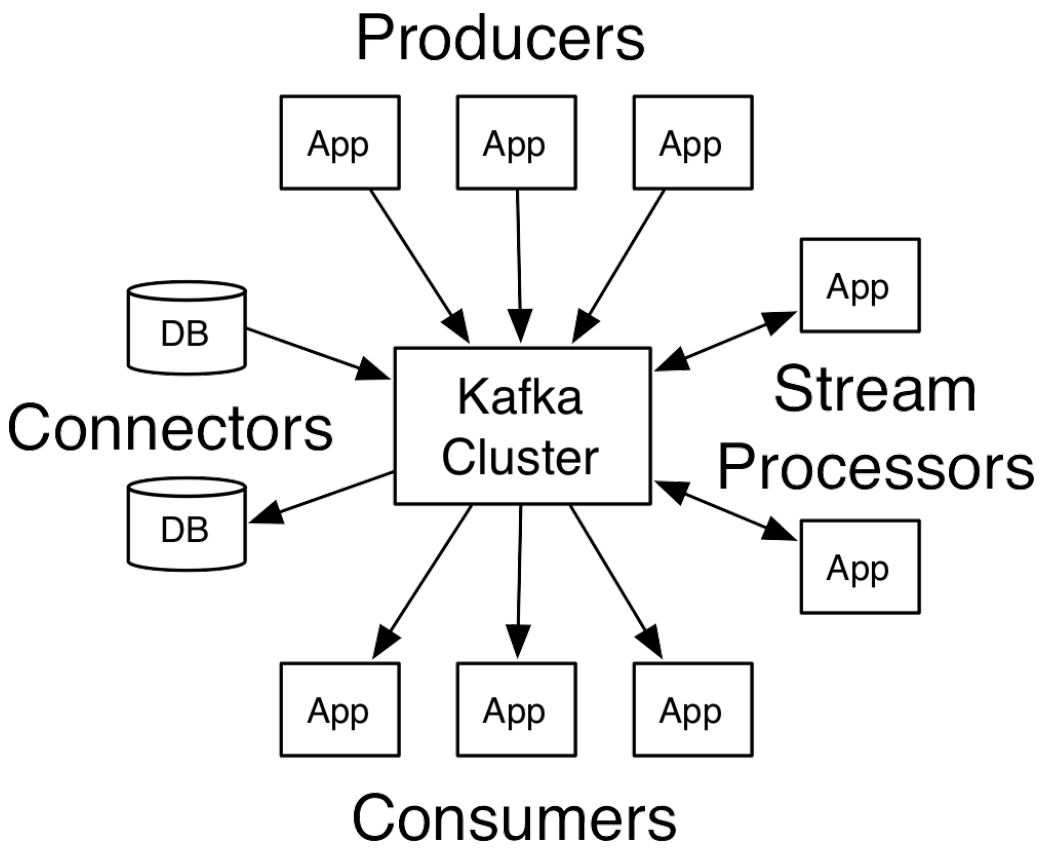
kafka

* source https://kafka.apache.org/

© 2021 comforte, Inc. All rights reserved

Introduction uLinga for Kafka

- uLinga for Kafka acts as a Kafka Producer, streaming data directly to a Kafka cluster
- Supports native Kafka wire protocols, meaning no additional software required – will give best performance
  - Other Kafka solutions are written in Java, require additional interim servers, may introduce single point of failure
- Runs like any other uLinga product – process pair, runs under Guardian and OSS (on NonStop), managed via WebCon
  - Proven uLinga architecture can handle massive data throughput



© 2021 comforte, Inc. All rights reserved

Kafka and uLinga – the architectural fit

Access Points

- TCP/IP
- HTTP

NonStop Access Points

- FILE READER
- SNAX/HLS
- SNAX/APC
- Pathsend
- IPC
- X25AM PTP

uLinga Core

- Support for all NonStop platforms, Windows and Linux
- Fault-tolerance, scalable and highly performant
- Web-based Management GUI
- Extensive tracing and logging facilties

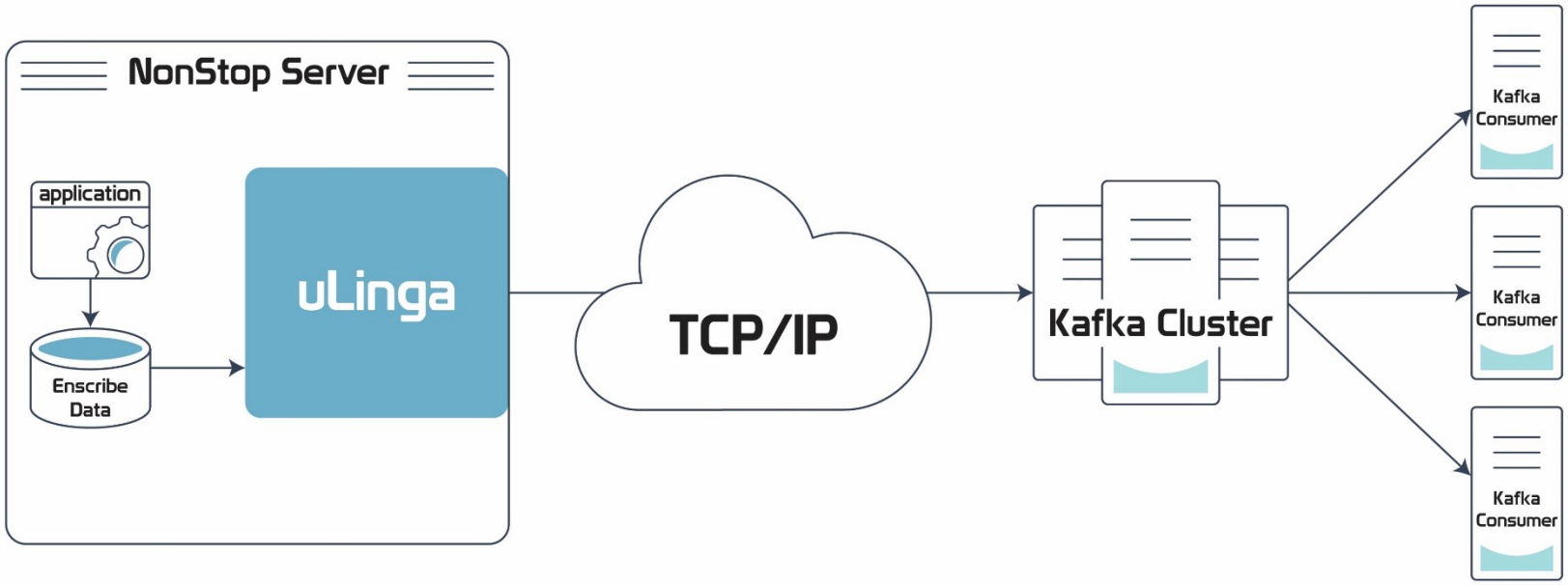
Connection Points

- EE (Enterprise Extender)
- IMS
- CICS
- Kafka
- DLSw
- XOT
- TCP/IP
- HTTP

NEW!

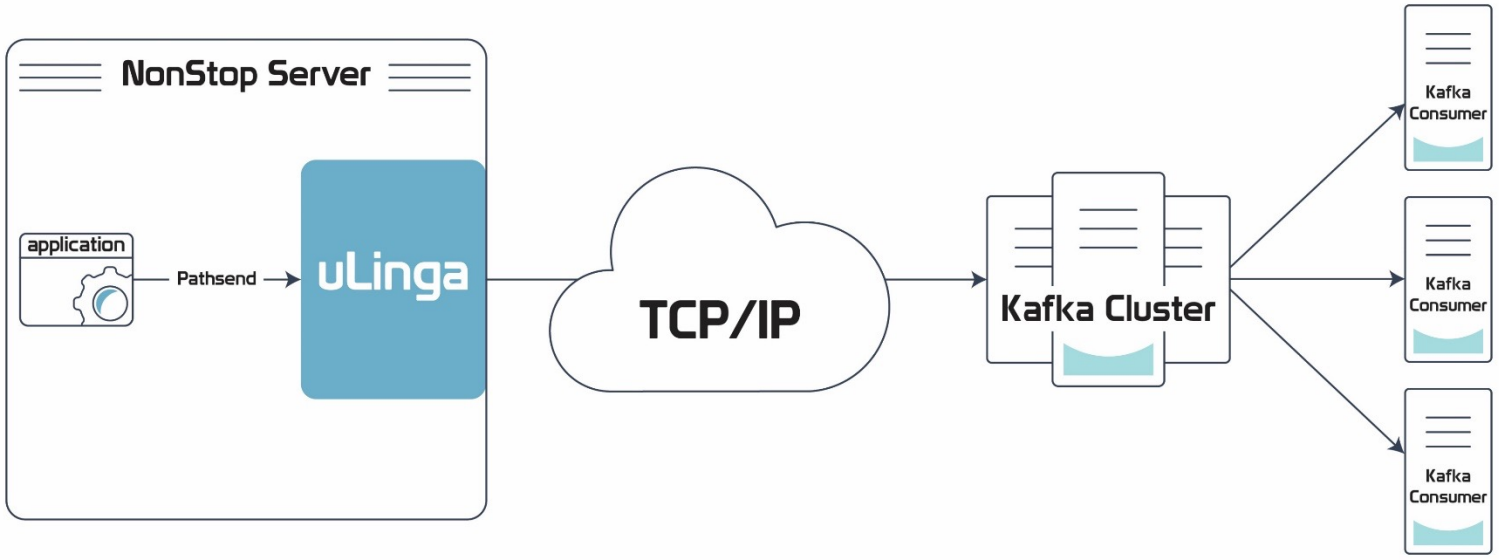
© 2021 comforte, Inc. All rights reserved

Use Case Enscribe File Support



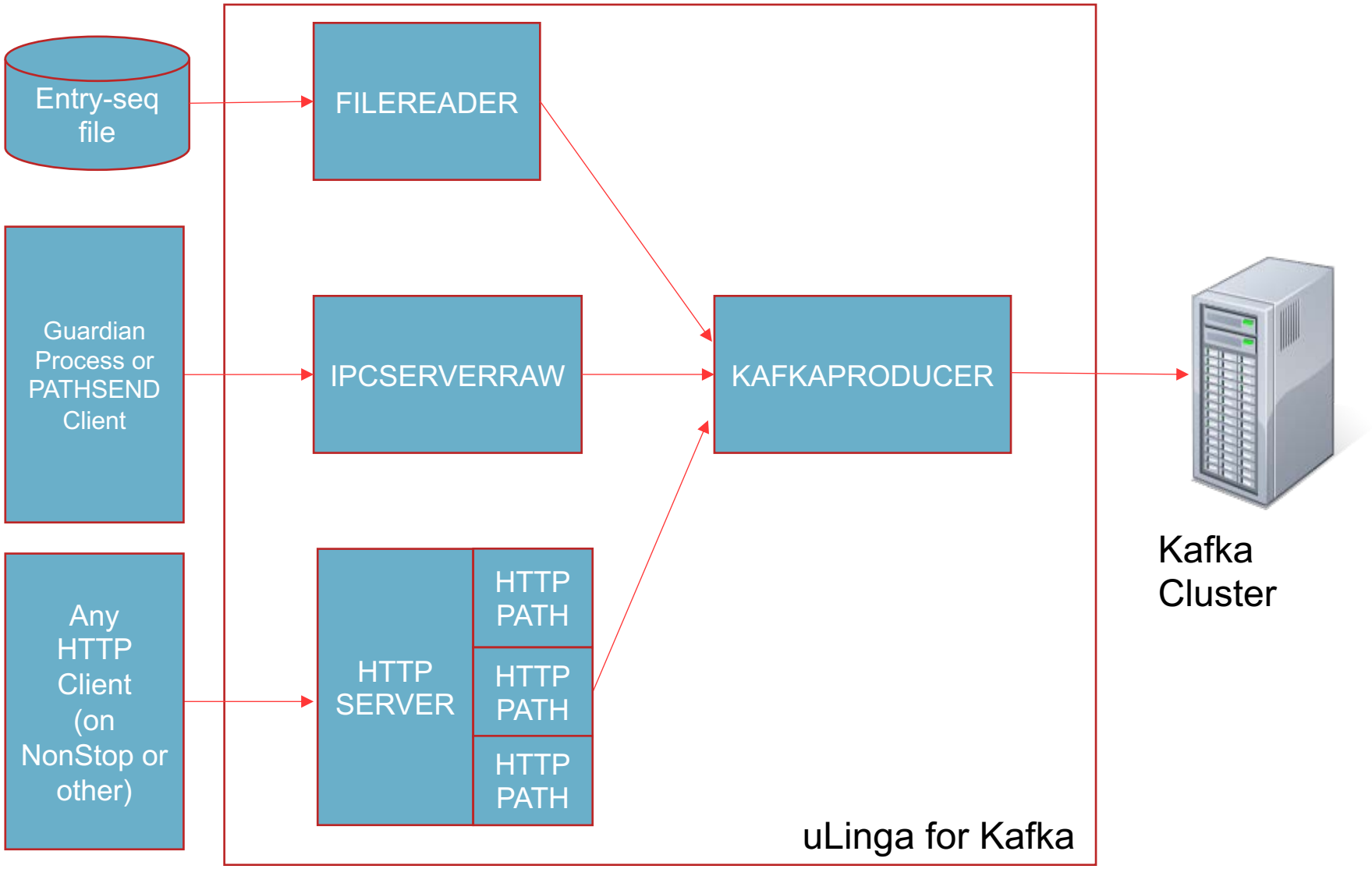
© 2021 comforte, Inc. All rights reserved

Use Case Pathsend/IPC Support



© 2021 comforte, Inc. All rights reserved

uLinga for Kafka – Complete Scenario



© 2021 comforte, Inc. All rights reserved

uLinga for Kafka - Summary

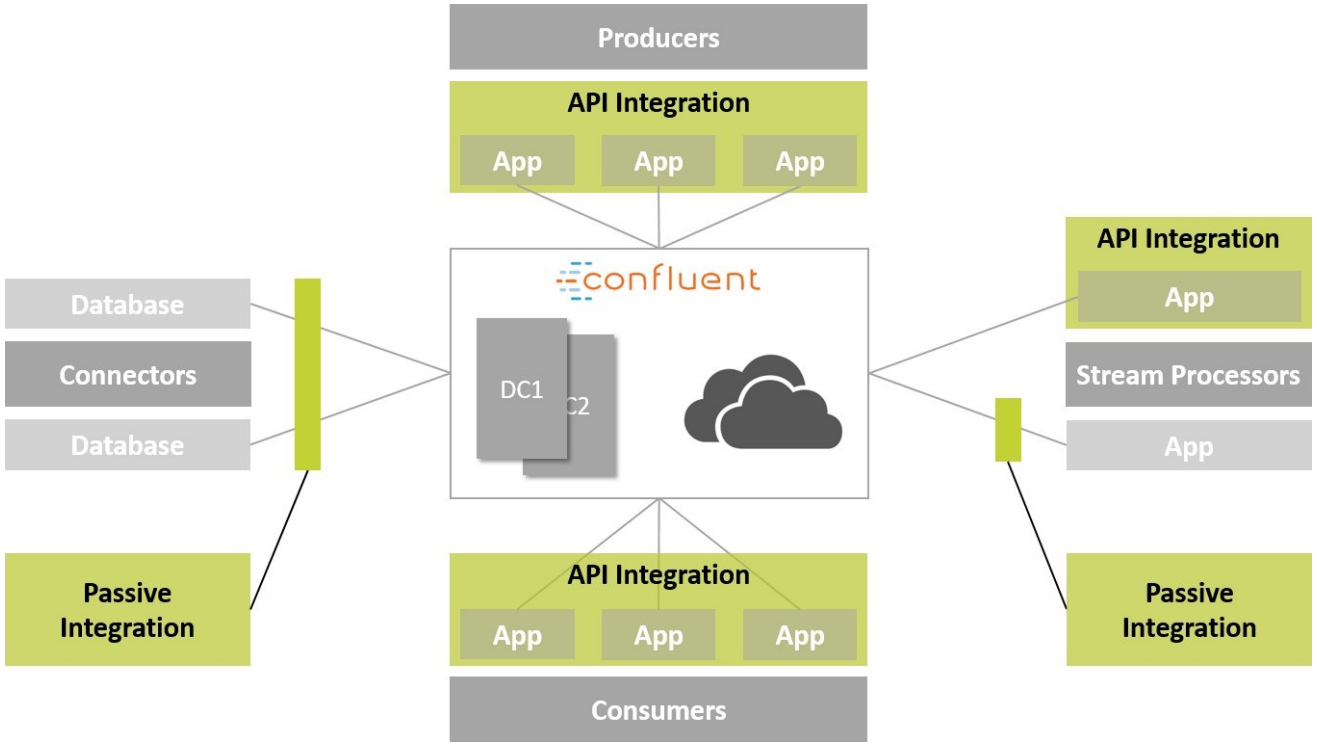
- uLinga for Kafka provides:
  - Excellent performance, written in C, with no additional components required
    - > 10,000 – 25,000 recs/second (real life measurements dependent on customer configurations)
    - All the advantages of other uLinga products:
      - Well-proven
      - NonStop process pair
      - Extensive tracing and diagnostics
      - WebCon browser-based user interface
- Variety of mechanisms to input data to uLinga, and from there to Kafka cluster:
    - FILEREADER for Enscribe files
    - IPC mechanism for Guardian/OSS $RECEIVE and Pathsend clients
    - HTTP mechanism to allow HTTP/REST clients to stream data

© 2021 comforte, Inc. All rights reserved

Kafka Security Integration Options with SecurDPS Enterprise

Recommended option

- For Kafka Producers and Consumers, SecurDPS integration can be performed using the SmartAPI.
- For Kafka Streams SecurDPS provides a dedicated “passive”/ transparent Kafka Streams Integration module out-of-the-box




```
{"ID":"42","CustomerName":"Arthur Dent","CustomerPAN":"424242EBAIFC4242"}
{"ID":"43","CustomerName":"Ford Prefect","CustomerPAN":"123456JHDCIA3456"}
{"ID":"44","CustomerName":"Zahod Beeble","CustomerPAN":"987654FIGABJ3456"}
```


© 2021 comforte, Inc. All rights reserved

TOP

© 2021 comforte, Inc. All rights reserved

The Challenge with NonStop Operation Support

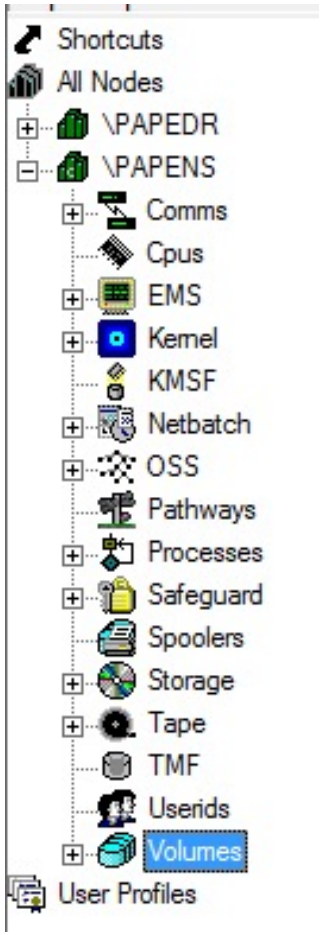
Some topics

- Not enough trained resources on NonStop
- Education classes are hard to schedule and expensive
- Non-dedicated operation support for NonStop
  - Corporate Help Desk
  - Off shore Support
- Task and process oriented
- Need to get trained faster

© 2021 comforte, Inc. All rights reserved

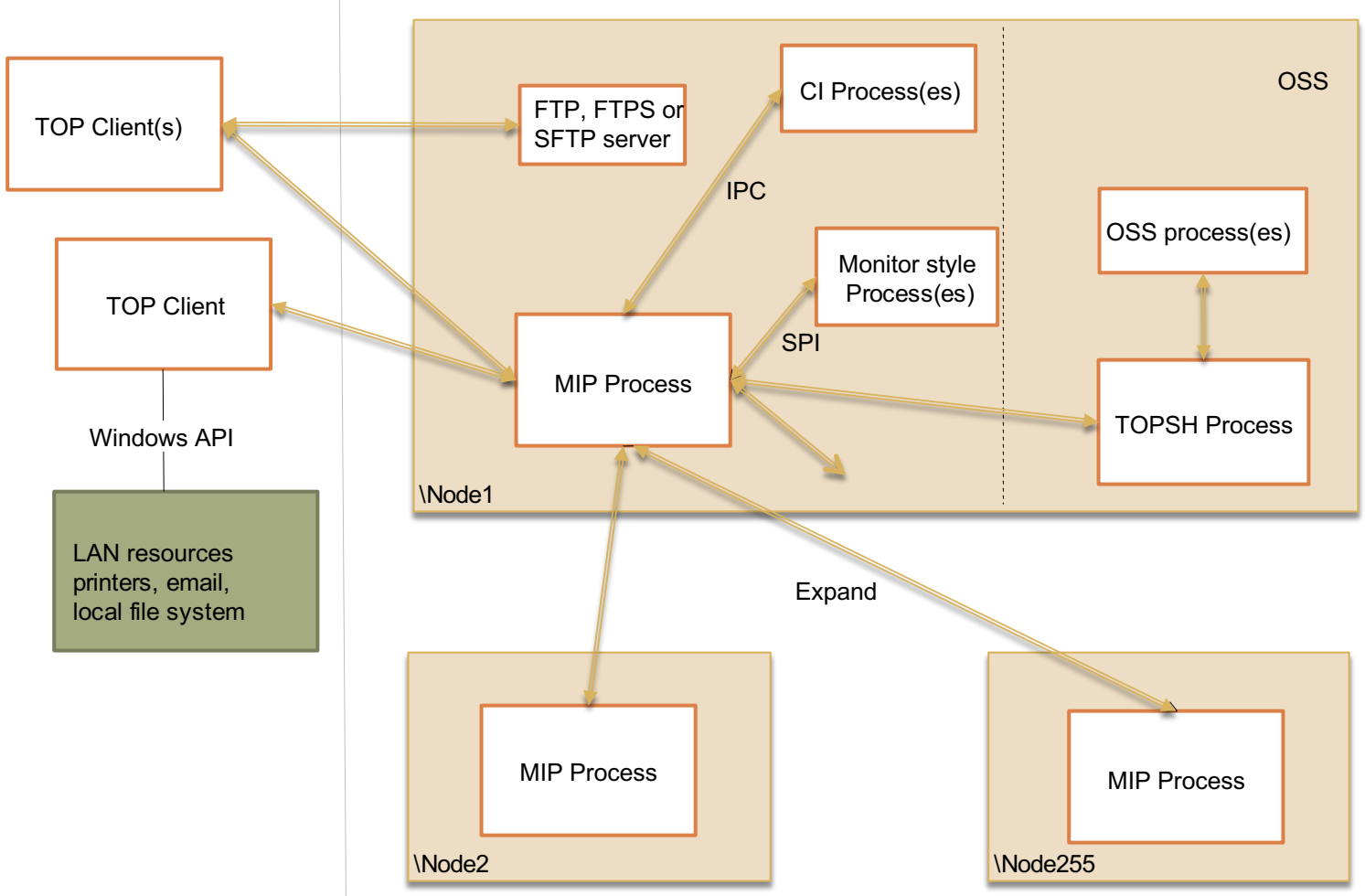
TOP – The GUI-Tool for NonStop

- The Operation Pack (TOP)
  - Communications
  - CPU
  - EMS
  - Netbatch
  - Pathway
  - Safeguard
  - Spooler
  - Many, many more…



© 2021 comforte, Inc. All rights reserved

Top Architecture



© 2021 comforte, Inc. All rights reserved

Windows File Explorer

Windows

Computer ▾ OS (C:) ▾ Windows ▾

Organize ▾ | Open | Include in library ▾ | Share with ▾ | Burn | Compatibility files | New folder

- MSOCache
- msys
- PerfLogs
- Pop3MimeClient
- Program Files
- Program Files (x86)
- ProgramData
- SoapUI-5.0.0
- SOG

Name	Date modified	Type	Size
bfsvc.exe	11/20/2010 10:24 ...	Application	70 KB
bootstat.dat	7/12/2017 3:04 AM	DAT File	66 KB
Casel.ini	3/9/2015 10:51 AM	Configuration sett...	1 KB
csup.txt	1/14/2015 7:05 PM	TXT File	1 KB
DocumentationSetUp.PUB	3/18/2015 9:48 AM	Microsoft Office P...	1 KB
DPINST.LOG	9/25/2015 11:53 AM	Text Document	8 KB
explorer.exe	8/29/2016 11:04 AM	Application	3,154 KB
f5unistall.INI	10/25/2016 3:26 PM	Configuration sett...	0 KB

TOP File Explorer

Location \TIC.Volumes.$system.system

TIC.PHIL

- olddata
- oldmnudb
- paytest
- pr03data
- pr08data
- prtest
- ptrain
- raytest
- rntldata
- rntldev
- roagacct
- robert
- robkup
- rodwacct
- roger
- rogerobj

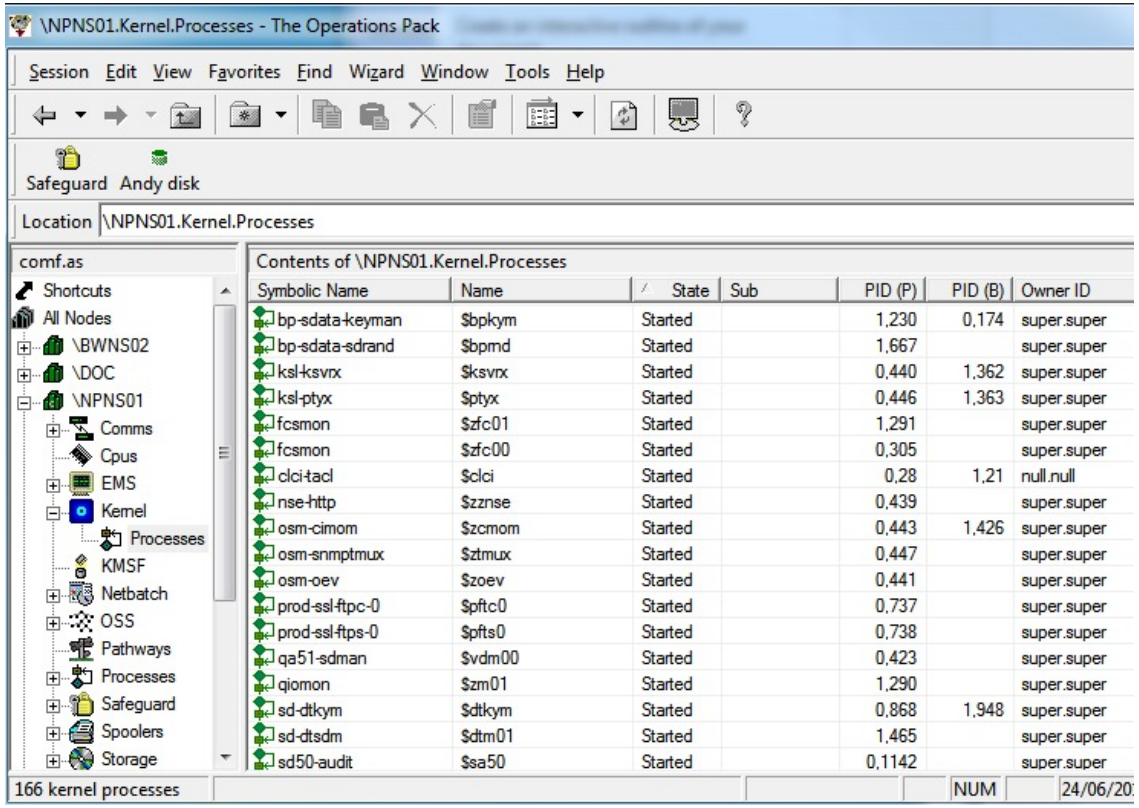
Contents of \TIC.Volumes.$system.system

Filename	Last Modified	Open	Description	EOF
aclh	9/4/2013 03:45		Edit file	530
adcshell	7/26/2009 23:45		Edit file	78,132
algoricc	10/14/2012 23:25		Edit file	75,668
algorit2	10/14/2012 23:25		Edit file	65,342
algoritm	10/14/2012 23:22		Edit file	197,672
announce	1/20/2017 15:27		Edit file	29,642
ar	11/21/2011 22:53		TNS/E native object file	303,560
arstvdb	6/21/2017 13:01		C data file	1,352
asserth	9/4/2013 03:45		Edit file	742
audserv	12/11/2013 03:06		TNS object file	2,721,792

© 2021 comforte, Inc. All rights reserved

TOP Summary

- Now is the time to train more NonStop Operation staff
- GUI increases productivity
- TOP is a productivity tool
  - Facilitate training new users
  - Benefit experienced NonStop users



© 2021 comforte, Inc. All rights reserved

Teaser for next GTUG

© 2021 comforte, Inc. All rights reserved

“A ZT approach is primarily focused on **data** and **service** protection

NIST

Hear more on ZT at the next GTUG 2022 ☺

comforte

Secure your growth