

Splunk>

Kateřina Nová



Splunk

- Co je to splunk?
- Jaká data zpracovává?
- Vyhledávání v datech
- Prezentování výsledků
- Výstrahy
- Spolupráce
- Reference



Co je to splunk?

- Software, který indexuje data z aplikací, serverů či síťových zařízení
- Umožňuje procházet, prohledávat, analyzovat a vizualizovat různá data z jednoho místa
- V reálném čase nebo nad historickými daty



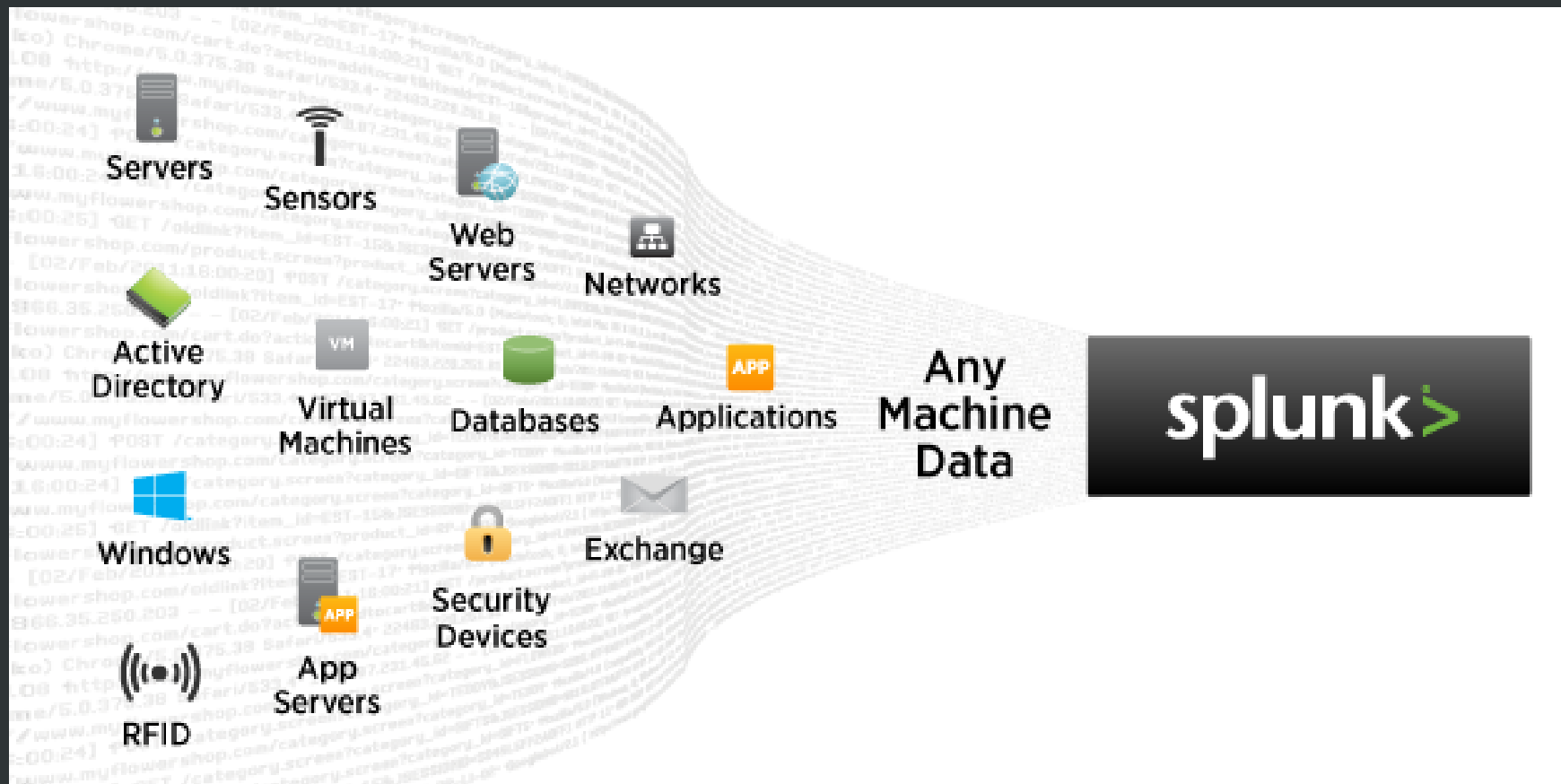
Instalace

- Zdrarma 60-ti denní Enterprise licence, poté přechod na omezenou Free verzi
- Snadná a rychlá instalace
- Po spuštění přístup přes webové rozhraní
- Přenositelnost na všechna zařízení



Vložení dat

- Jakákoli data – nestructurovaná, různé zroje
- Lokální x vzdálená



Data+

- Fields – označení, jaká data co znamenají
 - Defaultní – host, sourcetype
 - Vlastní – definované regulárními výrazy
- Přidání dodatečných dat, která budou dobře vypadat na reportech (př. tabulku číslo produktu - název)



Prohledávání dat

splunk > Search Administrator | App | Manager | Alerts | Jobs | Logout

Summary Search Status Dashboards & Views Searches & Reports Help About

Search Smart Mode

sourcetype=access_* Yesterday

9,277 matching events Save Create

Hide Zoom out Zoom to selection Deselect Linear scale 1 bar = 1 hour

9,277 events during Monday, December 3, 2012

Export Options prev 1 2 3 4 5 6 7 8 9 10 next 10 per page

#	Time	Host	Source	Event
1	12/3/12 11:59:34.000 PM	178.19.3.39	Sampledata2.zip:/apache3.splunk.com/access_combined.log	GET /flower_store/category.screen?category_id=CANDY HTTP/1.1" 200 10567 "http://mystore.splunk.com/flower_store/cart.do?action=purchase&itemId=EST-14&JSESSIONID=SD5SL10FF8ADFF3" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070223 CentOS/1.5.0.10-0.1.e14.centos Firefox/1.5.0.10" 3187 1245 host=127.0.0.1 sourcetype=access_combined_wcookie source=Sampledata2.zip:/apache3.splunk.com/access_combined.log category_id=CANDY action=purchase clientip=178.19.3.39
2	12/3/12 11:59:34.000 PM	178.19.3.39	Sampledata2.zip:/apache2.splunk.com/access_combined.log	GET /flower_store/category.screen?category_id=CANDY HTTP/1.1" 200 10567 "http://mystore.splunk.com/flower_store/cart.do?action=purchase&itemId=EST-14&JSESSIONID=SD5SL10FF8ADFF3" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070223 CentOS/1.5.0.10-0.1.e14.centos Firefox/1.5.0.10" 842 96 host=127.0.0.1 sourcetype=access_combined_wcookie source=Sampledata2.zip:/apache2.splunk.com/access_combined.log category_id=CANDY action=purchase clientip=178.19.3.39
3	12/3/12 11:59:34.000 PM	178.19.3.39	Sampledata2.zip:/apache2.splunk.com/access_combined.log	GET /flower_store/images/cat3.gif HTTP/1.1" 200 5024 "http://mystore.splunk.com/flower_store/item.screen?item_id=EST-14&JSESSIONID=SD5SL10FF8ADFF3" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070223 CentOS/1.5.0.10-0.1.e14.centos Firefox/1.5.0.10" 3966 3244 host=127.0.0.1 sourcetype=access_combined_wcookie source=Sampledata2.zip:/apache2.splunk.com/access_combined.log clientip=178.19.3.39
4	12/3/12 11:59:15.000 PM	10.192.1.46	Sampledata2.zip:/apache1.splunk.com/access_combined.log	POST /flower_store/order.do HTTP/1.1" 200 13849 "http://mystore.splunk.com/flower_store/enter_order_information.screen&JSESSIONID=SD5SL10FF8ADFF3" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070223 CentOS/1.5.0.10-0.1.e14.centos Firefox/1.5.0.10" 1463 2971 host=127.0.0.1 sourcetype=access_combined_wcookie source=Sampledata2.zip:/apache1.splunk.com/access_combined.log clientip=10.192.1.46
5	12/3/12 11:59:15.000 PM	10.192.1.46	Sampledata2.zip:/apache3.splunk.com/access_combined.log	GET /flower_store/category.screen?category_id=PLANTS HTTP/1.1" 200 10567 "http://mystore.splunk.com/flower_store/cart.do?action=purchase&itemId=EST-27&JSESSIONID=SD5SL10FF8ADFF3" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.0.10) Gecko/20070223 CentOS/1.5.0.10-0.1.e14.centos Firefox/1.5.0.10" 3352 1920 host=127.0.0.1 sourcetype=access_combined_wcookie source=Sampledata2.zip:/apache3.splunk.com/access_combined.log category_id=PLANTS action=purchase

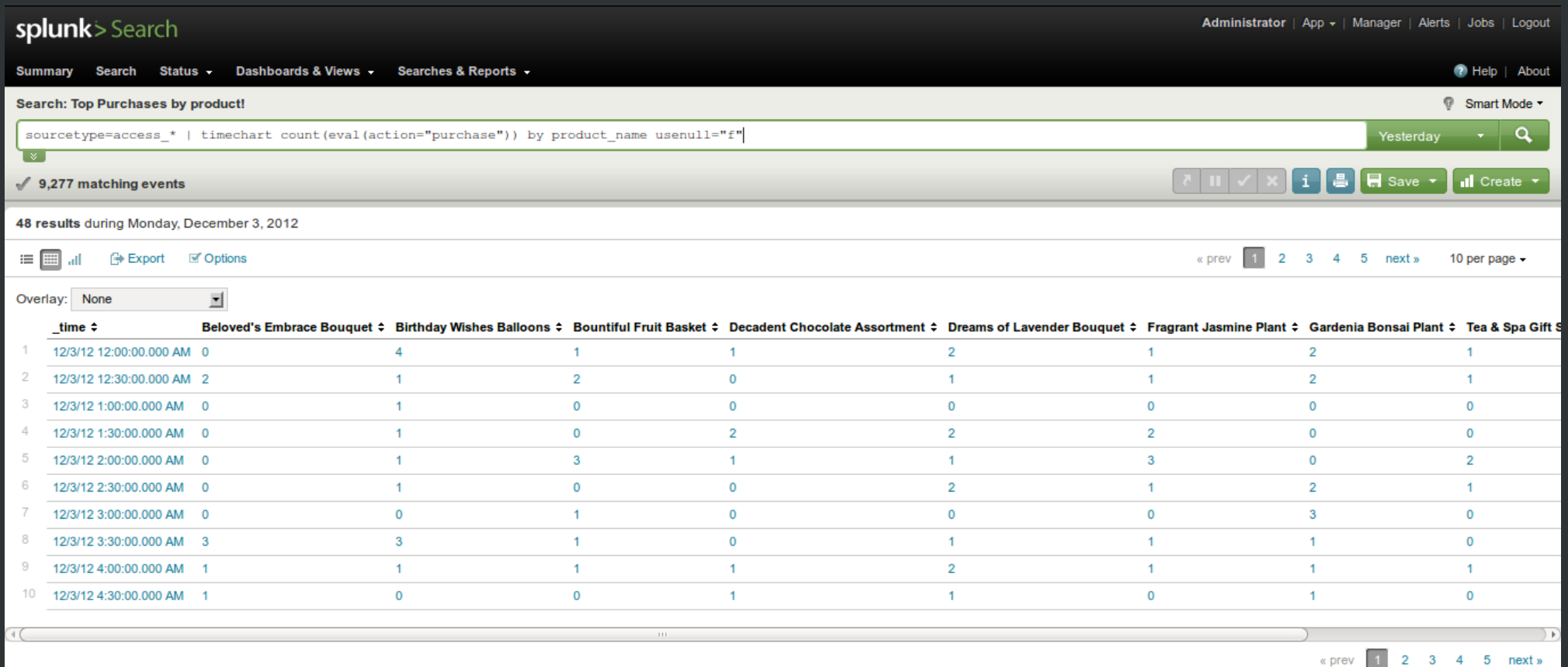
Vyhledávací jazyk

- CLI
- Fieldy
- Pipeline
- Subserch
- Funkce
- Regulární výrazy



Př: Přístupy dle produktů

```
sourcetype=access_* | timechart count(eval(action="purchase")) by product_name usenull="f"
```



Prezentace výsledků

- Reporty
 - Zobrazení výsledků vyhledávání – grafy
- Dashboardy
 - Sdružování reportů
 - Export: PDF, e-mail



Př: přístupy dle produktů

splunk Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary Search Status Dashboards & Views Searches & Reports

Help About

Report: Top purchases by Product -report!

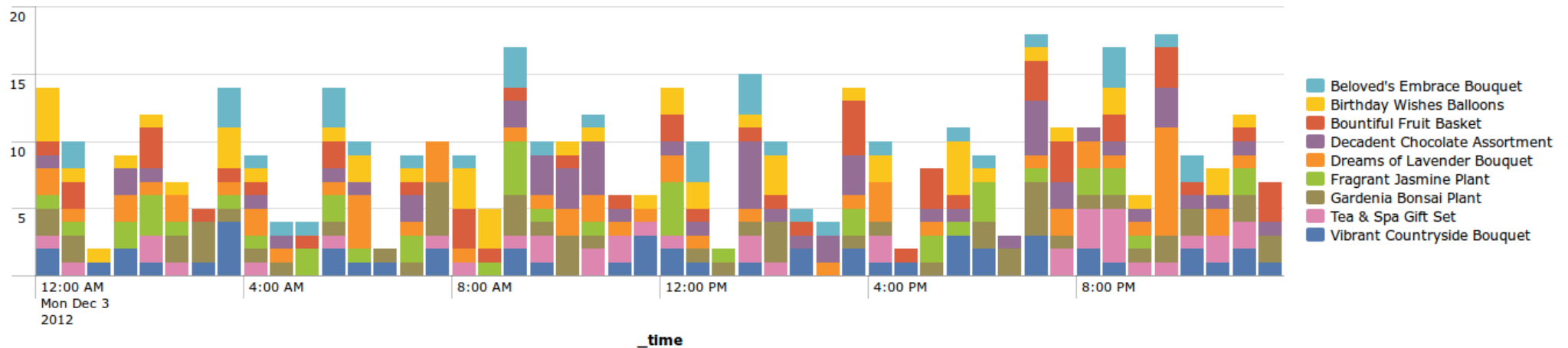
9,277 matching events



Save results Share results... View previous jobs View events Generate PDF

Chart

Top purchases by Product



Table

Overlay: None Enable Preview [Export](#)

« prev 1 2 3 4 5 next » 10 per page

_time	Beloved's Embrace Bouquet	Birthday Wishes Balloons	Bountiful Fruit Basket	Decadent Chocolate Assortment	Dreams of Lavender Bouquet	Fragrant Jasmine Plant	Gardenia Bonsai Plant	Tea & Spa Gift Set
12/3/12 12:00:00.000 AM	0	4	1	1	2	1	2	1
12/3/12 12:30:00.000 AM	2	1	2	0	1	1	2	1
12/3/12 1:00:00.000 AM	0	1	0	0	0	0	0	0
12/3/12 1:30:00.000 AM	0	1	0	2	2	2	0	0
12/3/12 2:00:00.000 AM	0	1	3	1	1	3	0	2
12/3/12 2:30:00.000 AM	0	1	0	0	2	1	2	1

Výstrahy

- Definování zajímavých (nebezpečných) událostí
- Vygenerování výstrahy
- Reakce na výstrahu
 - Poslání e-mailu
 - Spuštění skriptu



Spolupráce

- Cisco
 - Zabezpečení webu, emailu, řešení spamu
- Microsoft
 - Zabezpečení, řešení problémů
- F5
 - Real-time prohledávání a analýza dat



Splunk Apps

- Stovky doplňků, rozšíření, usnadnění..
- Poskytují uživatelský komfort pro různé role a případy užití
- Sledování systému – Windows, Linux
- Cisco security suite
- Splunk on Splunk
- Google maps pro zobrazení výsledků na mapě



Reference

- Enterprise licenci má přes 4 400 společností
- Ve více než 80 zemích
- University of Texas, Austin
 - Více než 50 000 studentů, přes 120 000 zařízení
- American University of Sharjah



Proč právě Splunk?

- Snadná instalace i používání
- Přístup ke všem datům z jednoho místa v reálném čase
- Automatické upozornění na podezřelé události
- Pro všechny uživatele – CLI i klikací
- Spuštění na rozdílných HW
- Dokáže zpracovat desítky terabytů dat denně
- Bezpečnost



- Děkuji za pozornost

