

Как мы создали SPAE — SaaS для администраторов интернет серверов



С чего всё началось?

Однажды, два админа, с достаточным опытом администрирования зоопарков серверов, задумались над тем, что для каждого серверного окружения приходится настраивать, или исторически они уже есть, свои nagios'и, mrtg, cacti, zabbix'и, pessus'и etc... Хотя настройка графиков, службы мониторинга сервисов и безопасности является тривиальной задачей, но все равно эта задача занимает время, требует размножения сущностей и постройки новых зависимостей. Логично пришла идея сделать «для себя» инструмент, который максимально помогал бы в рутинном администрировании. Но перед тем как «придумывать новый велосипед» нужно разложить проблему, которую он будет решать на составляющие.

В чем собственно проблема?

1. У меня/клиента только один сервер. Но чтобы его мониторить надо еще один.

А кто будет мониторить сервер который мониторит этот сервер? :) Выход есть! Гугл поможет найти пачку буржуйских сервисов. Перепробовали штук 15 и не нашли того, который работал бы как нам хотелось бы и имел достаточный функционал.

2. Для того, чтобы поставить сервер на мониторинг нужно его прописать как минимум в нескольких конфигах.

На самом деле не сложно п раз запустить vi config.cfg и зарелоадить софт, но, если, софт нужно установить или обновлять, то это создает дополнительную головную боль.

3. Все инструменты в разных интерфейсах.

Приведу пример браузера среднестатистического админа: Первый таб — nagios, второй — cacti/mrtg. Плюс для проверки безопасности еще какойто софт. Это три разных интерфейса, но они связаны одной сущностью.

4. Хочу получать нотификации через реальные SMS.

Почтовые шлюзы операторов или часто имеют большую задержку или просто их нет. Надо полюбовно строить взаимоотношения с операторами. Либо телефон к серверу прикручивать, либо работать через какую нить sms-кантору, разобравшись с её самописным API.

5. Забываю проводить аудиты безопасности сервера.

Таких вебсервисов существует очень мало и работают они не всегда качественно. Зато есть удобный и бесплатный pessus. Хотя и не автоматизирован и без нормального web интерфейса.

What Admin Want?

Базируясь на собственном опыте и желаниях, появился список функционала и особенностей:

- Максимально упростить добавление сервера в систему мониторинга. Достаточно установить с портов net-snmpd и мышкой в putty закопипастить сгенерированный конфиг.
- Инвентаризация — Единое место хранения информации о том что это за система и на каком железе живет.
- Мониторинг доступности сервисов и метрик: HTTP, PING, SMTP, SSH, POP3, IMAP, DNS, CPU Usage, Disk Spae.
- Нотификации по email, реальным(моментальным) sms, icq. Ежедневный сумарный отчет.
- Графики использования ресурсов — Interface, CPU Usage, LoadAvarage, Memory, Disks
- Безопасность — внешняя проверка сервера на все известные уязвимости — frontend для nessus'a

Разработка.

Свободных рук программистов небыло, потому пришлось научиться программировать и написать самому. Под web-frontent была выбрана Java, в качестве ajax framework'a ZKoss. AppServer — Tomcat. Web связка — Apache+Nginx. Backend — nagios, для графиков rrdtool, для безопасности — nessus, все это связано ~ 20 демонами и скриптами на C, Shell/AWK, Python. Через 6 месяцев мир увидила альфа-версия.

Что получилось.

Мониторинг:

Availability Monitoring Settings

Notification Contacts

ON	email	support@shalb.com	Edit
ON	icq	130231442	Edit
OFF	sms	380672348417	Edit
ON	email	380672348417@sms.ky	Edit
ON	icq	256742606	Edit
OFF	sms	380632441621	Edit

Add Notification Contact

realtor

ON	Disk:/mnt/ramdisk	normal	Edit
ON	Disk:/mnt/sataraid1	normal	Edit
ON	Disk:/boot	normal	Edit
ON	HTTP	normal	Edit
ON	Disk:/	normal	Edit
ON	CPU Usage	normal	Edit
ON	SSH	normal	Edit
ON	FTP	normal	Edit
ON	SMTP	normal	Edit
ON	PING	soft	Edit

Add New Service

Service Details

Server	Service	Status	Last Check	Status Information
realtor	SSH	OK	2010-02-16 14:03:42.0	SSH OK - OpenSSH_5.2 (protocol 2.0)
realtor	SMTP	OK	2010-02-16 14:01:37.0	SMTP OK - 0,013 sec. response time
realtor	HTTP	OK	2010-02-16 14:04:13.0	HTTP OK HTTP/1.1 200 OK - 75479 bytes in 0,176 seconds
realtor	PING	OK	2010-02-16 14:04:13.0	PING OK - Packet loss = 0%, RTA = 2.19 ms
realtor	FTP	OK	2010-02-16 14:01:04.0	FTP OK - 0,006 second response time on port 21 [220 (vsFTPd 2.2.0)]
realtor	Disk:/mnt/sataraid1	OK	2010-02-16 14:01:54.0	OK : /mnt/sataraid1: 66%used(311667MB/468674MB) : < 75 %
realtor	Disk:/mnt/ramdisk	OK	2010-02-16 14:04:11.0	OK : /mnt/ramdisk: 1%used(0MB/15MB) : < 75 %
realtor	Disk:/boot	OK	2010-02-16 14:01:18.0	OK : /boot: 90%used(174MB/194MB) : < 90 %
realtor	Disk:/	OK	2010-02-16 14:04:13.0	OK : /: 40%used(53743MB/133275MB) : < 75 %
realtor	CPU Usage	OK	2010-02-16 14:04:08.0	8 CPU, average load 9.4% < 70% : OK
joinup	SSH	OK	2010-02-16 14:03:42.0	SSH OK - OpenSSH_5.1p1 SSH2 (protocol 2.0)
joinup	SMTP	OK	2010-02-16 14:04:41.0	SMTP OK - 0,020 sec. response time
joinup	PING	OK	2010-02-16 14:01:21.0	PING OK - Packet loss = 0%, RTA = 2.34 ms
joinup	Disk:/var	OK	2010-02-16 14:01:53.0	OK : /var: 5%used(2913MB/59503MB) : < 75 %
joinup	HTTP	OK	2010-02-16 14:01:11.0	HTTP OK HTTP/1.1 200 OK - 15351 bytes in 0,228 seconds
joinup	FTP	OK	2010-02-16 14:05:11.0	FTP OK - 0,016 second response time on port 21 [220 ProFTPD 1.3.2 Server (joinup FTP-server. Access restricted) [77.120.117.28]]

Monitoring

Graphs

Security

Inventory

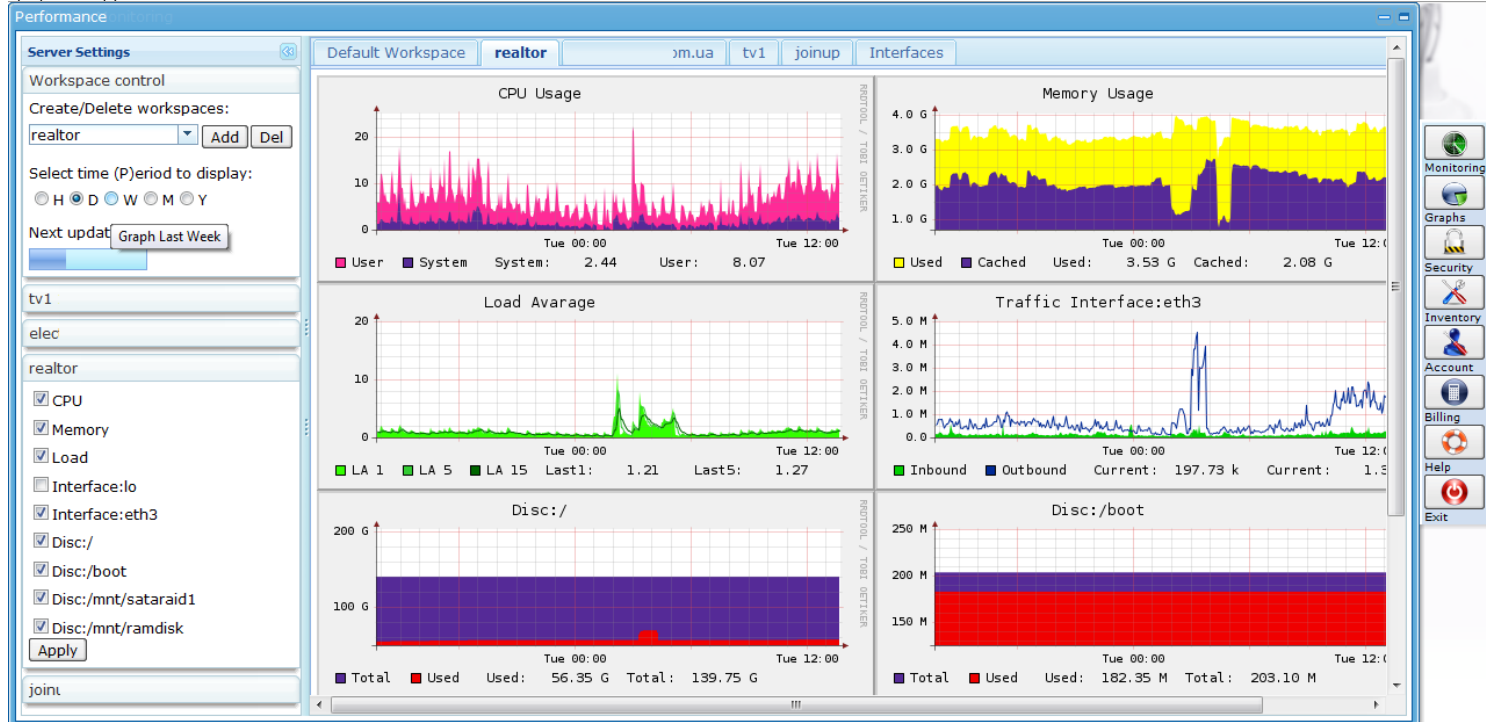
Account

Billing

Help

Exit

# Графики загрузки:



## Интерфейс безопасности:

Security

Server Security

My Reports

Critical: 6 Notice: 16 Warning: 0

Generate!

Select Servers To Report

☒ realtor

☒ joinup

☒ tv1

Select Risk Factor to Include

☐ Notice

☒ Medium

☒ Critical

Select Services to Include

☒ ftp (21-tcp)

☒ general-icmp

☒ general-tcp

☐ general-udp

Server IP	Critical Level	Service
194.1.	Critical	unknown (8086/tcp)
62.145	Critical	http (80/tcp)
62.145	Critical	http (80/tcp)
62.145	Critical	http (80/tcp)
62.145	Critical	http (80/tcp)
<b>Description:</b> The remote web server uses a version of PHP that is affected by multiple flaws. According to its banner, the version of PHP installed on the remote host is older than 5.2.4. Such versions may be affected by various issues, including but not limited to several overflows. See also: <a href="http://www.php.net/releases/5_2_4.php">http://www.php.net/releases/5_2_4.php</a> Solution: Upgrade to PHP version 5.2.4 or later. Risk factor: High / CVSS Base Score: 7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P) CVE: CVE-2007-2872, CVE-2007-3378, CVE-2007-3806 BID: 24661, 24261, 24922, 25498 Other references: OSVDB:36083, OSVDB:36085, OSVDB:36869		
62.145	Critical	general/tcp
62.145	Medium	smtp (25/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
194.1.	Medium	http (80/tcp)
62.145	Medium	http (80/tcp)
62.145	Medium	https (443/tcp)
62.145	Medium	https (443/tcp)
77.125	Medium	http (80/tcp)
77.125	Medium	unknown (7780/tcp)
77.125	Medium	unknown (7780/tcp)
77.125	Medium	unknown (7780/tcp)
77.125	Medium	http (80/tcp)

The Security interface displays a list of detected vulnerabilities. The left sidebar contains controls for generating reports, selecting servers to report on (realtor, joinup, tv1), selecting risk factors to include (Medium, Critical), and selecting services to include (ftp, general-icmp, general-tcp, general-udp). The main table lists the Server IP, Critical Level, and Service for each vulnerability. A detailed description for the first vulnerability is provided, mentioning a PHP version issue and providing references.

## Инвентаризация:

Servers Inventory

IP Address	Hostname	OS	Type	Hardware Info	Software Info
6[REDACTED]	realtor	Linux	Web	8x GenuineIntel: Intel(R) Xeon(R) CPU E5520 @ 2.27GHz Memory: 3916MB Storage:/' (130.15137GB) Storage:/boot' (0.18847656GB) Storage:/mnt/sataraid1' (457.68848GB) Storage:/var/log' (457.68848GB) Storage:/mnt/ramdisk' (0.0146484375GB) Storage:/var/backup' (457.68848GB)	System: Linux [REDACTED] 2.6.30.10-105.fc11.x86_64 #1 SMP Thu Dec 24 16:41:51 UTC 2009 x86_64
[REDACTED]	joinup	Linux	Mail	2x Intel(R) Core(TM)2 Duo CPU E7500 @ 2.93GHz Memory: 3987MB Storage:/' (1.9316406GB) Storage:/dev' (0.0GB) Storage:/var' (58.1084GB) Storage:/cache' (9.683594GB) Storage:/usr' (29.050781GB) Storage:/home' (77.481445GB) Storage:/store' (104.68652GB)	System: FreeBSD [REDACTED] 7.2-RELEASE-p3 FreeBSD 7.2-RELEASE-p3 #0: Fri Sep 4 18:31:29 EEST 2009 [REDACTED]/usr/src/sys/i386/compile/joinup i386
[REDACTED]	[REDACTED]	BSD	Web	1x VIA C3 Samuel 2 Memory: 471MB Storage:/' (0.48339844GB) Storage:/dev' (0.0GB) Storage:/tmp' (0.48339844GB) Storage:/usr' (68.947266GB) Storage:/var' (1.4042969GB)	System: FreeBSD [REDACTED] 6.2-RC1 FreeBSD 6.2-RC1 #0: Thu Nov 16 05:01:36 UTC 2006 root@opus.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC i386
[REDACTED]	tv1	Linux	Web	16x GenuineIntel: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz Memory: 31913MB Storage:/' (1647.9521GB) Storage:/boot' (0.3779297GB)	System: Linux tv1 2.6.30.10-105.2.4.fc11.x86_64 #1 SMP Tue Jan 19 22:46:59 UTC 2010 x86_64

Selected Server

Add Server

Apply Changes

Delete Server

Server	Host	Port	Status	Time	Details
joinup	Disk:/var		OK	2010-02-16 12:41:20.0 12:41:53.0	OK : /var: 5%used(2912MB/59503MB) : < 75 %
joinup	HTTP		OK	2010-02-16 12:41:11.0	HTTP OK HTTP/1.1 200 OK - 15861 bytes in 0,236 seconds
joinup	FTP		OK	2010-02-16 12:40:11.0	FTP OK - 0,009 second response time on port 21 [220 ProFTPD 1.3.2 Server (joinup FTP-server. Access restricted) [77.120.117.28]]

Поганять демку можна:

user: demo@shalb.com  
password: shalb  
[spae.shalb.com/](http://spae.shalb.com/)

Промо страница: [shalb.com/ru/spae/spae\\_features/](http://shalb.com/ru/spae/spae_features/)

#### Бизнес.

Так как было просто глупо тратить столько времени без варианта заработать, дописалась регистрация и биллинг. Сделали анализ цен хоть как-то похожих проектов (mon.tor.us, host-tracker), посчитали себестоимость услуги для мониторинга одного сервера, построили ценовую политику и вышло 5\$ в месяц за мониторинг одного IP.

#### Кто клиент.

Целевые клиенты SPAE — владельцы, администраторы серверов, VPS'ов у которых от одного до пяти серверов. Мы не ориентируемся на Гуру администраторов и на администраторов больших систем серверов. У этих людей уже всё давно есть. Сервис просто решает часть проблем связанных с администрированием и безопасностью серверов.

#### Настоящее.

Сейчас система мониторит 80 серверов в 5ти датацентрах.  
Запущена партнерская программа с датацентром Воля, который дает 20% скидки на наш сервис.  
Начали рефакторинг кода уже с настоящими опытными Java программистами. Ловим баги, планируем маркетинговую кампанию.

#### Будущее:

Кастомная настройка мониторинга сервисов (по портам/продвинутый http мониторинг)  
Кастомные OID для графиков (disk IO включительно)  
Многоязычный интерфейс.  
Му IPS — интеграция в интерфейс управления/нотификация snort'a.  
WebServices API.  
OpenSource standalone версия — как только код будет не стыдно показать коммюнити.

Спасибо.

- [мониторинг](#)
- [сервер](#)
- [сервис](#)
- [spae](#)
- [мой бизнес](#)
- [saas](#)
- [я пиарюсь](#)

+14  
16 февраля 2010, 15:38  
20  
[voa](#)