

Использование свободного ПО в инфраструктуре облачных услуг

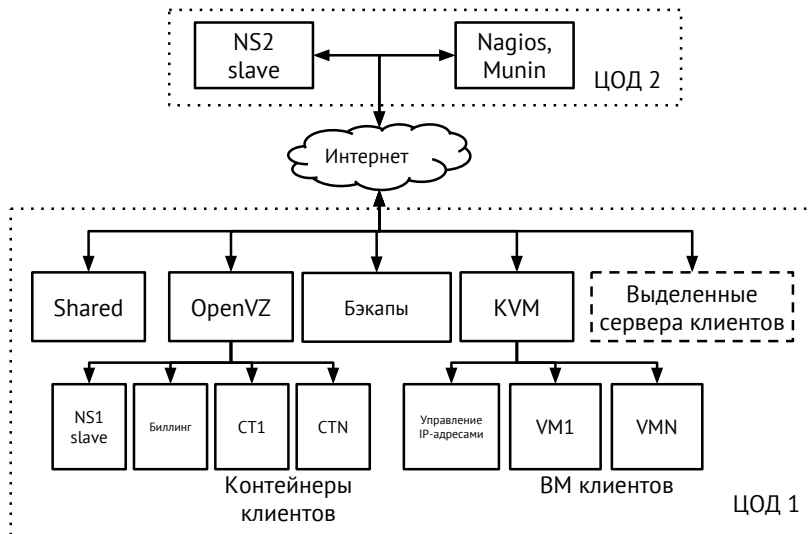
Умеров Амет

Разработка виртуальной инфраструктуры для реализации облачных услуг

Требования:

- устранение единых точек отказа
- защита от несанкционированного доступа и DDoS-атак
- **использование свободного ПО**
- документирование инфраструктуры
- автоматизация инфраструктуры

Общая схема инфраструктуры



Серверная операционная система

CentOS 7 (GPL)

Преимущества:

- поддержка 6-10 лет
- свободно распространяемая ОС
- большое количество документации
- имеется опыт работы с дистрибутивом

Мониторинг

Nagios

Nagios®


Host **	Service **	Status **	Last Check **	Duration **
node-19.domain.tld	cinder-api	OK	12-30-2013 20:16:07	0d 0h 16m 12s
	cinder-scheduler	OK	12-30-2013 20:16:39	0d 0h 15m 40s
	cpu	WARNING	12-30-2013 20:17:10	0d 0h 15m 9s
	glance-api	OK	12-30-2013 20:17:42	0d 0h 14m 37s
	glance-registry	OK	12-30-2013 20:18:13	0d 0h 14m 6s
	horizon	OK	12-30-2013 20:18:45	0d 0h 13m 34s
	kernel	OK	12-30-2013 20:19:17	0d 0h 13m 2s
	keystone	OK	12-30-2013 20:19:48	0d 0h 12m 31s
	libs	OK	12-30-2013 20:20:20	0d 0h 11m 59s
	load	OK	12-30-2013 20:20:51	0d 0h 11m 28s
	memcached	OK	12-30-2013 20:21:23	0d 0h 10m 56s
	memory	WARNING	12-30-2013 20:21:54	0d 0h 0m 25s
	nova-api	OK	12-30-2013 20:12:26	0d 0h 9m 53s
	nova-scheduler	OK	12-30-2013 20:12:58	0d 0h 9m 21s
	procs	OK	12-30-2013 20:14:11	0d 0h 8m 50s
	swap	OK	12-30-2013 20:14:01	0d 0h 8m 18s
	user	OK	12-30-2013 20:14:32	0d 0h 7m 47s

Мониторинг

Nagios > Icinga2 (GPLv2)

Nagios®

Host ★★	Service ★★	Status ★★	Last Check ★★	Duration ★★
node-19.domain.tld	cinder-api	OK	12-30-2013 20:16:07	0d 0h 16m 12s
	cinder-scheduler	OK	12-30-2013 20:16:39	0d 0h 15m 40s
	cpu	WARNING	12-30-2013 20:17:10	0d 0h 15m 9s
	glance-api	OK	12-30-2013 20:17:42	0d 0h 14m 37s
	glance-registry	OK	12-30-2013 20:18:13	0d 0h 14m 6s
	horizon	OK	12-30-2013 20:18:45	0d 0h 13m 34s
	kernel	OK	12-30-2013 20:19:17	0d 0h 13m 2s
	keystone	OK	12-30-2013 20:19:48	0d 0h 12m 31s
	libs	OK	12-30-2013 20:20:20	0d 0h 11m 59s
	load	OK	12-30-2013 20:20:51	0d 0h 11m 28s
	memcached	OK	12-30-2013 20:21:23	0d 0h 10m 56s
	memory	WARNING	12-30-2013 20:21:54	0d 0h 0m 25s
	nova-api	OK	12-30-2013 20:12:26	0d 0h 9m 53s
	nova-scheduler	OK	12-30-2013 20:12:58	0d 0h 9m 21s
	procs	OK	12-30-2013 20:14:11	0d 0h 8m 50s
	swap	OK	12-30-2013 20:14:01	0d 0h 8m 18s
	user	OK	12-30-2013 20:14:32	0d 0h 7m 47s

 **icinga**

Current Incidents Overdue Muted + ▾

Search ...

Dashboard

Problems 19

Overview

History

Reporting

Documentation

System

Configuration

icingaadmin

Logout

Service Problems

CRITICAL
1m 9s
Soft 2/5

test-random-3: service-flapping-1
test-random-3 (checked by vagrant-centos7)
service-flapping-1 unchanged

CRITICAL
1m 33s
Soft 3/5

test-random-2: service-flapping-4
test-random-2 (checked by vagrant-centos7)
service-flapping-4 unchanged

CRITICAL
2m 42s
Soft 4/5

test-random-9: service-flapping-4
test-random-9 (checked by vagrant-centos7)
service-flapping-4 unchanged

UNKNOWN
Sep 24

test-unreachable-1: service-unknown-1
test-unreachable-1 (checked by vagrant-cent
service-unknown-1

UNKNOWN
Sep 24

test-unreachable-10: service-unknown-1
test-unreachable-10 (checked by vagrant-cent
service-unknown-1

UNKNOWN
Sep 24

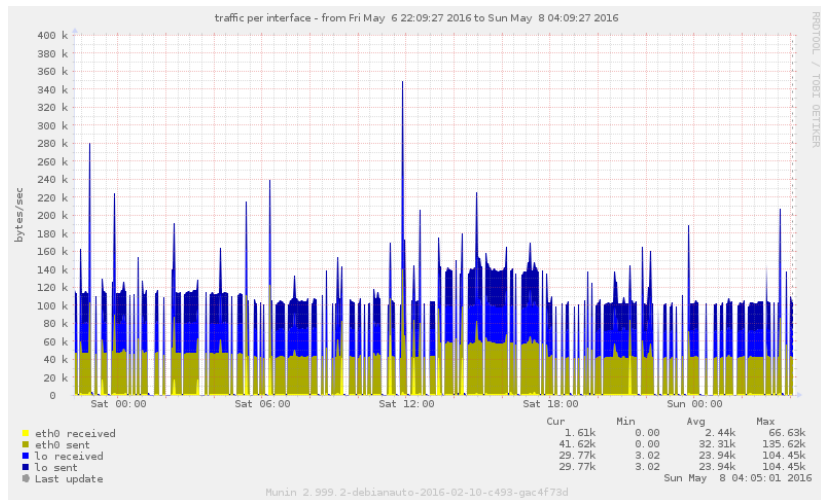
test-unreachable-2: service-unknown-1
test-unreachable-2 (checked by vagrant-cent
service-unknown-1

UNKNOWN
Sep 24

test-unreachable-3: service-unknown-1
test-unreachable-3 (checked by vagrant-cent
service-unknown-1

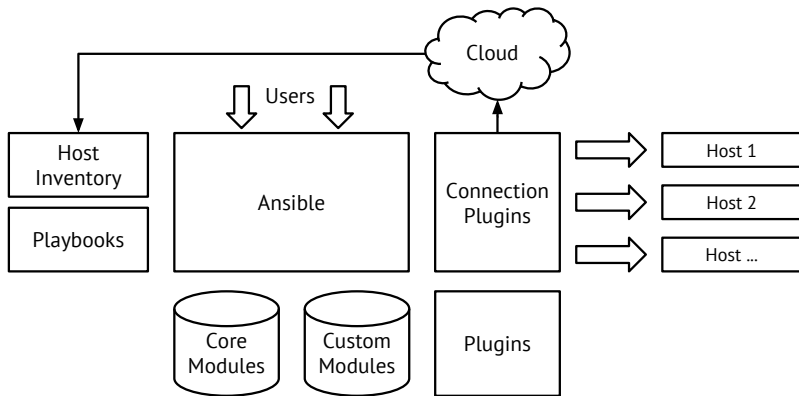
Метрики

Munin (GPL)



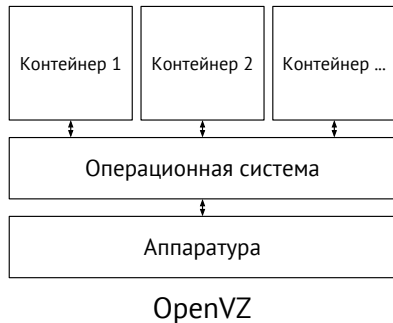
Автоматизация управления

Ansible (GPL)



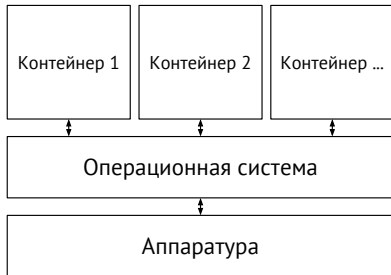
Виртуализация

OpenVZ (GPLv2)

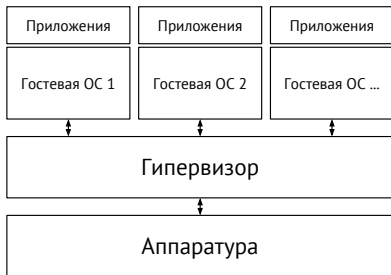


Виртуализация

OpenVZ (GPLv2) + KVM (GPL/LGPL)



OpenVZ



KVM

Защита от вредоносков

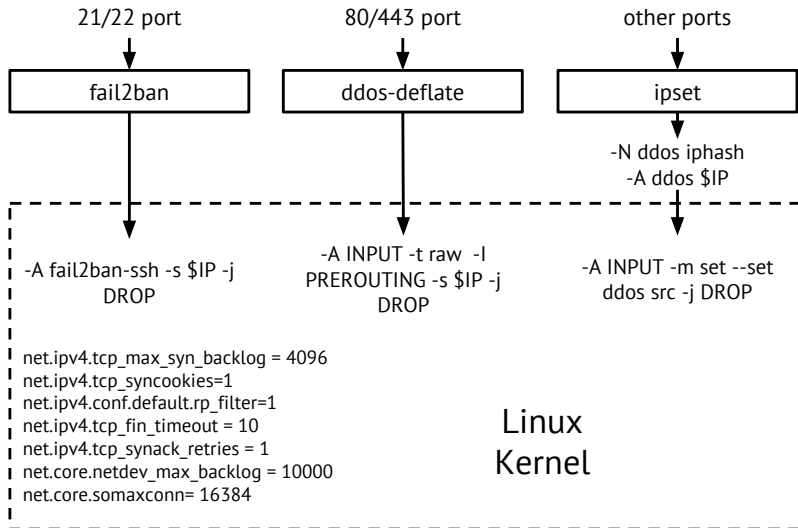
Linux Malware Detect (GPL)

Возможности:

- обнаружение вредоносков по хэш-сумме MD5
- отправка потенциально опасных файлов на сервис rfxn.com для внесения в базу сигнатур
- использование exclude-файлов
- удаление инфицированных base64 и gzip вставок
- перемещение зараженных файлов в карантин
- поиск по сигнатурам ClamAV



Защита сети

ddos-deflate (Artistic License) + IPTables/fail2ban/ipset (GPL)





Панели управления для клиентов

Vesta Control Panel (GPLv3)

 VESTA Packages IP Graphs Statistics Log Updates Firewall File Manager Server  admin Log out

USER	WEB	DNS	MAIL	DB	CRON	BACKUP
users: 2	domains: 1	domains: 1	domains: 1	databases: 1	jobs: 7	backups: 2
suspended: 0	aliases: 1	records: 12	accounts: 1	suspended: 0	suspended: 0	
	suspended: 0	suspended: 0	suspended: 0			

 26 Jan 2016

☐ toggle all sort by: DATE ↓ apply to selected >

demo.vestacp.com

www.demo.vestacp.com

77 . 247 . 243 . 30

Bandwidth	9 mb	Web Template:	default	Proxy Support:	yes
		SSL Support:	yes	Proxy Template:	force-https
Disk:	3 mb	Web Statistics:	awstats	Additional FTP:	admin_2

Сравнение с закрытыми аналогами

Стоимость лицензий и обслуживания

Open Source	Closed Source
CentOS 7	RHEL 7 – \$900/год за 1 сервер
Nagios Munin	Sensu – \$600/год за 50 серверов Opsview – \$935/год за 50 серверов
OpenVZ KVM	Virtuozzo – \$6200/год за 100 контейнеров vCenter Server – \$1750/год за 1 CPU
Maldet	Virusdie – \$20/год + \$2/год за сайт

- RHEL 7 (10 серверов) – \$9 000/год
- Virtuozzo (100 контейнеров x 10 серверов) – \$62 000/год
- vSphere Server (4 CPU x 10 серверов) – \$70 000/год
- Sensu/Opsview (30-50 серверов) – \$600-935/год
- Virusdie (2000 сайтов x 10 серверов) – \$40 000/год

Итого: **\$262 600/год**

Проекты в Open Source

- openvz-tutorial (CC BY-SA 4.0):
github.com/Amet13/openvz-tutorial
- virtuoizzo-tutorial (CC BY-SA 4.0):
github.com/Amet13/virtuoizzo-tutorial
- ddos-deflate (Artistic License 2.0):
github.com/Amet13/ddos-deflate
- ansible-vz-wordpress (GNU GPLv3):
github.com/Amet13/ansible-vz-wordpress
- icinga2-plugins-extra (GNU GPLv3):
github.com/Amet13/icinga2-plugins-extra
- **bachelor-diploma (CC BY-SA 4.0):**
github.com/Amet13/bachelor-diploma