Installed to last

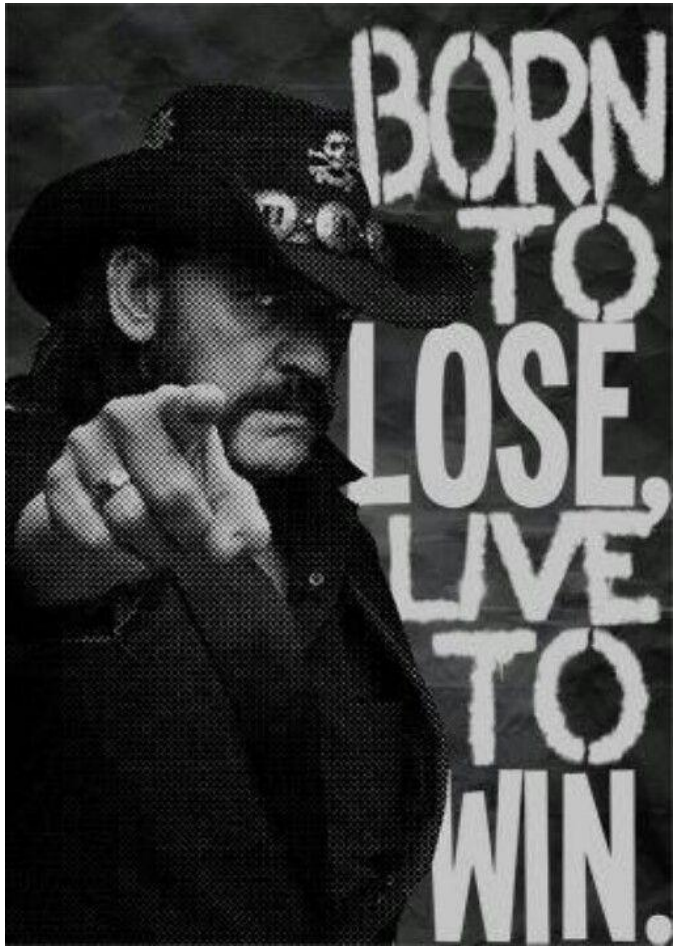
@jedux, @godlike64, @sysarmy

Abstract

"(GNU/Linux) Instalado para durar"

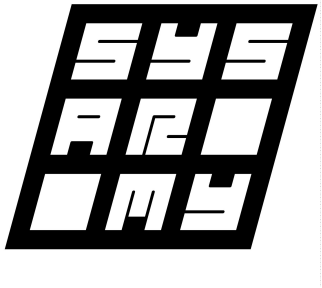
Abstract:

El dinamismo de la industria a veces genera situaciones de instalación de servidores que no son las óptimas para durar años en producción. Durante esta charla revisaremos un check list básico de tareas y configuraciones que nos ayudarán a que ese servidor instalado pueda transcurrir su largo ciclo de vida con la menor sobrecarga administrativa posible. (selección de OS, selección de paquetes, hardening, configuraciones de hardware, etc).



About godlike

redhat.



About jedux

SYSARMY

QUE ES SYSARMY

Es la comunidad Argentina de sistemas, nuclea a lxs profesionales del sector para favorecer el contacto y el intercambio de conocimiento

EL SOPORTE DE QUIENES DAN SOPORTE

- IRC
- /HELP
- ADMINFEST, ADMINBIRRAS, EOY 7 de Diciembre!
- NERDEAR.LA
- ENCUESTA DE SUELDOS

NERDEAR.LA


Taking Over & Managing
Large Messy Systems
Lisa 2018
Nashville, TN, USA
usenix
LISA18

There are Bodies Buried Everywhere

- Always messy
- Always bad configurations
- No/broken backups
- Often crashing
- Often overloaded

- 3-year-old server lists
- People usually gone
- Dead RAID disks
- High-Availability is Low

What we find

- Not what CEOs & CTOs think
- Mountain of Tech Debt

- One server, many services
- Many instances – Tomcat, DBs
- Root Linux/DB users for everything

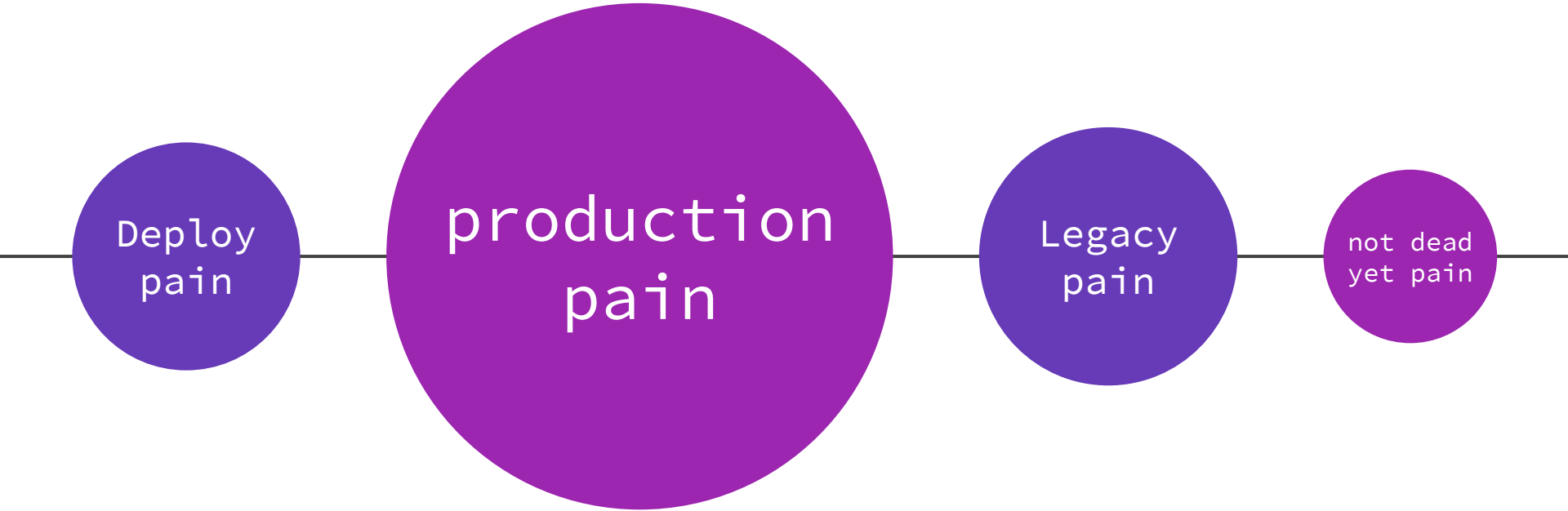
- Zero updates of anything
- Redhat Ver 6-9 with Linux Kernel 2.2

Amazed at what we find

- 3 Apaches Installed
  - RPM, Source, Random Tarball
- 2 Apaches Running
- 1 Apache Actually Used
  - The Random Tarball one …
  - Started from ssh by random user

Amazing Apaches

Ciclo de vida de un server.



- Hardware

- Relación costo / servicio / calidad
- Redundancia
  - PSU
  - Ethernet
  - RAID
    - Software vs Hardware
  - HA
- Costo => Inversión => less pain

WD Green


Western Digital
www.westerndigital.com
1.0TB
SATA / 32MB Cache
WD10EADS
S/N : WCAV5C677993
MDL : WD10EADS – 11M2B2
WWN:50014EE2AF16A78A
DATE: 21 APR 2010
DCM : DARNHT2CHB
DCX : 7029MCT27
LBA : 1953525168
5VDC : 0.70A
12VDC : 0.55A
R/N : 701640
WD Caviar Green

NO


OSI


WD
3.0TB
SATA / 64MB Cache
WD30EFRX
NASware™ 3.0
Western Digital
www.westerndigital.com
3.0TB
SATA / 64MB Cache
WD30EZRX
S/N : WCAWZ1153745
MDL : WD30EZRX – 00MMMB0
DATE : 03 AUG 2011
DCM : HARCNV2AAB
Western Digital
www.westerndigital.com
3.0TB
SATA / 64MB Cache
WD30EZRX
S/N : WCAWZ1165968
MDL : WD30EZRX – 00MMMB0
DATE : 03 AUG 2011
DCM : HARCNV2AAB
Western Digital
www.westerndigital.com
3.0TB
SATA / 64MB Cache
WD30EZRX
S/N : WCAWZ1057290
MDL : WD30EZRX – 00MMMB0
DATE : 17 JUL 2011
DCM : HBNCM12AAB


3.0TB
3.0TB
3.0TB
3.0TB
3.0TB
3.0TB

- Selección del OS

- Ciclo de vida/actualizaciones
  - Ubuntu LTS: 5 años
  - RHEL: 10 años
- Nivel de soporte/documentación.
- Comunidad
- EOL (End of Life):
  - No más actualizaciones
  - No más soporte

- Selección de Paquetes

- Objetivo: dejar el sistema andando por años, mantenimiento mínimo.
- Backporting.
- Priorizar paquetes provistos por el vendor.
  - QA, testing, seguridad, actualizaciones
- Paquetes de terceros
  - Origen? Actualizaciones?
- Containers
  - Origen? Actualizaciones? Seguridad?
- ~~Armar paquete custom? Compilar código?~~

- OS configuration - Network Bonding

- Server físico o hypervisor donde corre la VM
  - BONDING
  - LACP
- Service ip different from server ip
- DNS
- Hardcodear todo /etc/hosts

- OS configuration - auto update security patches

- “Update early. Update often.”
    - Auto security updates or die
- Agendar reinicios periódicos para actualizaciones de kernel.
- Asignar ventanas de mantenimiento para aplicación de actualizaciones.

- OS hardening

- Autenticación centralizada
  - sudo para administradores. Root password en vault seguro.
- MAC: SELinux / AppArmor
- SSH
  - Ideal: acceso sólo por keys
  - **No exponer puerto 22 públicamente**
- PoLP: no chmod 777
  - Se puede enjaular? → chroot
  - Corre como usuario raso? → crear usuario específico para el servicio
  - Necesita permisos de root para algo? → `man capabilities`
- SSL para qué?

- OS configuration management

- Todo lo que se pueda automatizar, se debe automatizar.
  - Puppet / Ansible / Saltstack / Chef
- No importa el configuration management, importa que esté.
- Y que sea el mismo para todos los equipos.
- Fuerza a estandarizar las instalaciones.

SALVO: que nuestro configuration management sea un rudimentario experimento(?) #EsPregunta

- monitoring

- Server Monitoring
  - Basics: Uptime, Raid Status, Mem, CPU, Disk Space, Inodes
  - Services: apache, smtp, etc.
  - Nagios / Zabbix / etc.
- Monitoreo de logs
  - ELK
- Local email relay (root!, md monitoring, cronjobs)

- Documentación

- Owners / Stakeholders
  - Roles no personas.
- Propósito
  - Qué servicio brinda al negocio?
- Técnica:
  - Como se instaló
  - Qué servicios tiene.
- Procedimientos varios
  - Cómo ejecutar upgrades?
  - Cómo reiniciar?
  - Cómo hacer failover?

- Backups!

- Hope for the best, plan for the worst.
- Planear backups
- **Hacer backups**
  - **no en el mismo servidor**
  - **idealmente no en el mismo edificio**
- ***Probar backups***
- DR?

RAID NO ES BACKUP.

RED HAT®
VIRTUALIZATION

TECHNOLOGY DETAIL

BEST PRACTICES FOR RED HAT VIRTUALIZATION 4

Guidance, recommendations, and considerations for design and deployment

FULLY PREPARED ENVIRONMENT

After reviewing the installation documentation, be sure to have the environment completely ready for deployment. This may sound like an obvious recommendation, but many deployments are delayed because of items such as incorrect network configuration, waiting on server setup, or lack of storage provisioning. Additionally, other network-based services, like DNS, will play a major part. Commonly overlooked steps include:

- Not having fully qualified domain names (FQDN) for hosts and Red Hat Virtualization Manager, including full resolution in DNS (forward and reverse).
- Not having all of the underlying storage provisioned and configured properly for the storage domains.
- Not having the underlying network prepared correctly, including switch and virtual LAN (VLAN) configuration.
- Not having the right kind of hardware for the hypervisors (e.g., no remote power control).
- Not using the latest available versions of the software.

- Not having fully up-to-date hardware, firmware, BIOS, etc.
- Misconfigured remote management/out-of-band (OOB)/power management.
- Attempting to set up the environment in the wrong order (e.g., storage prior to networking).
- Not having proper file system layout (e.g., VM thinpool when using Red Hat Virtualization Hypervisor).
- Not having proper /var size requirements for hosted-engine deployment.
- Not having correct software channels subscribed or properly registered with Red Hat Content Delivery Network (CDN) or Red Hat Satellite.
- Not properly testing before going into production.
- Missing other configuration items that lengthen or frustrate the deployment process.

ENVIRONMENT

This is an often-overlooked area that bears emphasis. The environment in which Red Hat Virtualization is to be deployed needs to comparable to the workloads it will support. That is, if the workloads are mission-critical, then the overall environment should be mission-critical.

Things to consider in a mission-critical environment include:

- Redundant Ethernet switches for both data and storage.
- Redundant fibre channel (FC) switches.
- Redundant power to all components.
- Redundant power in the datacenter.
- Redundant network providers to the datacenter.
- Redundant network services (e.g., DNS, LDAP).

Finally, document absolutely everything, including:

- How are hosts deployed in your environment?
- How are VMs provisioned in your environment?
- How does application x get deployed in production?
- How does application y get updated in production?
- How does a developer get a new test environment for a week?
- How does that test environment get cleaned up?
- Where are IP addresses, DNS names, VLANs, and other network information documented?
- What are the security standards for Red Hat Enterprise Linux® VMs?
- What are the security standards for Red Hat Enterprise Linux virtualization hosts?

Essentially, any system administrator, engineer, architect, developer, or manager should be able to access the documentation (online or otherwise) and understand how to get things done. Especially when things go wrong.

¿Preguntas?

Contact

@jedux
@godlike64

@sysarmy
sysarmy.com.ar/help

LISA18 Talk:
https://www.youtube.com/watch?v=oD1knEp2c9I

RH Doc
https://www.redhat.com/cms/managed-files/vi-best-practice-rhv-technology-detail-f7659kc-201706-en.pdf