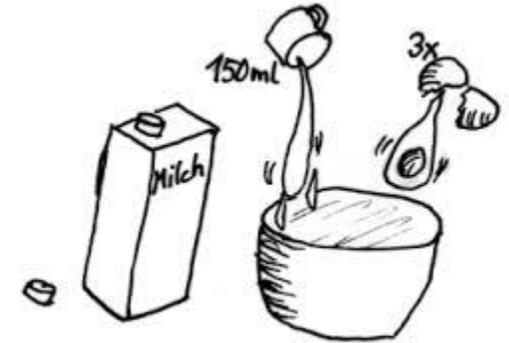


Konfigurationsmanagement und Sicherheit



Über mich

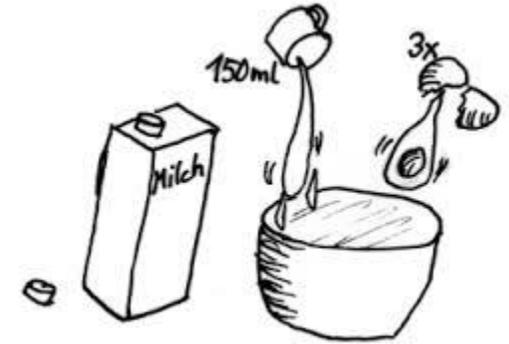
- Seit Ende der 90-er im IT-Bereich tätig
- Web- und Java Entwicklung
- Nebenher Betreuung von Server- und Netzwerkinfrastrukturen
- 2010 Wechsel in Infrastrukturbereich
- 2012 Umstellung des RZ-Betriebes auf DevOps
- Seither Regelbetrieb + externe Kundenprojekte



Setup

- Kleines Team
- Berufsanfänger
- KEINE Securityexperten
- Unbelastet, kein konventioneller Systembetrieb

- RZ als Infrastructure As A Service
- ~ 300 VMs
- Interne, produktive Systeme
- Kundensysteme
- 1st-, 2nd- und 3rd-Level Support



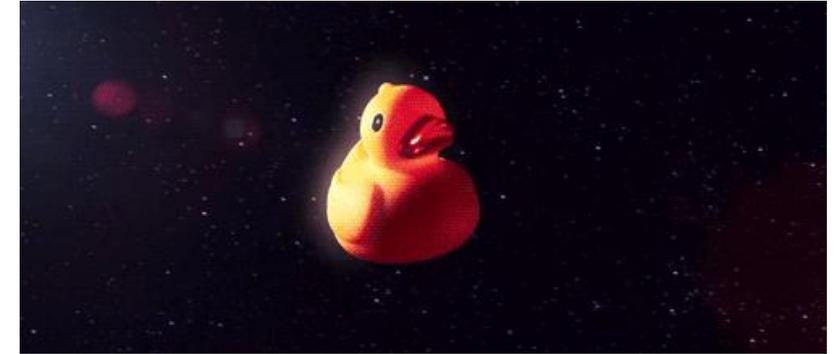
Ein wenig Puppet: Grundlagen

- Configuration Management Tool
- KEIN Security- oder Auditingtool
- Puppetmaster -> nur authentifizierte und Zertifizierte Clients haben Zugriff
- Auf Ressourcen (File, User, Cron,) basierend
- Deklarierendes Sprachkonstrukt

```
class openssh::service (Boolean $service_ensure) {  
  service { 'sshd':  
    ensure    => $service_ensure,  
    enable    => true,  
    hasrestart => true,  
    hasstatus => true,  
    subscribe => Class['openssh::config',  
                    |'openssh::install']  
  }  
}
```


Ein wenig Puppet: Best Practices for Security

- Backup von Files auf Puppet Master
 - Kein grep auf Passwörter
 - Ressourcenschonend
- `show_diff => false`,
 - - Verwendung externer Module
 - - Eigenverantwortung der Kollegen notwendig
- Verwendung von Puppet Resources statt exec-Anweisungen



```
[0root@~:~ 0^2 17:16]# ls -la /var/log/puppetlabs/puppet/*201707*
-rw-----. 1 root root 1539 Jul  1 22:14 /var/log/puppetlabs/puppet/puppet-client.log-20170701.gz
-rw-----. 1 root root 1522 Jul  2 22:14 /var/log/puppetlabs/puppet/puppet-client.log-20170702.gz
-rw-----. 1 root root 1888 Jul  3 22:14 /var/log/puppetlabs/puppet/puppet-client.log-20170703.gz
[0root@~:~ 0^3 17:17]#
```

Ein wenig Puppet: Best Practices for Security

- Regelmäßige Runs einmal die Stunde
- Überwachung durch Monitoringsystem
 - Zuweisung korrektes Environment
 - Error Log leer
 - Puppet status (Last run + fehlerfrei)

- „fail“-Anweisung für default-Zweige

```
case ($::ops_os) {  
  $::os_name_centos6 : {  
    # ...  
  }  
  $::os_name_centos7 : {  
    # ...  
  }  
  $::os_name_opensuse42 : {  
    # ...  
  }  
  default : {  
    fail("${module_name}: Operating system \"${::os[name]}\" is not yet supported!")  
  }  
}
```

VM Initialisierung

- Templating von Minimalinstallation, Vermeidung unnötiger:
 - Pakete
 - Services
 - Ports
- Initialisierung mittels Script:
 - Filesystemlayout
 - Repositorys --> nur definierte Softwarepakete verwendbar
 - Upgrade System --> System bei Übergabe auf aktuellstem Stand
 - Installation Puppet
- Housekeeping mittels Script:
 - Remove from puppet
 - Remove from monitoring
 - Finden und löschen v. Firewallregeln
 - ...

Filehandling: /etc-files

- Setzen von Fileberechtigungen:
 - /etc/passwd
 - /etc/shadow
 - /etc/gshadow
 - /etc/group

```
if $::ops_hardening_level == '1' {  
    $passwd_mode = '644'  
    $group_mode = '644'  
    $shadow_mode = '000'  
    $gshadow_mode = '000'
```

```
'/etc/passwd':  
    mode => $ops::hardening::passwd_mode,;  
  
'/etc/group':  
    mode => $ops::hardening::group_mode,;  
  
'/etc/shadow':  
    mode => $ops::hardening::shadow_mode,;  
  
'/etc/gshadow':  
    mode => $ops::hardening::gshadow_mode
```

```
[2root@rcl-centos701:etc 1^40 18:55]# chmod 777 passwd shadow gshadow group  
[0root@rcl-centos701:etc 1^41 18:55]# ls -la passwd shadow gshadow group  
-rwxrwxrwx. 1 root root 1435 Jul  4 18:05 group  
-rwxrwxrwx. 1 root root 1257 Jul  4 18:05 gshadow  
-rwxrwxrwx. 1 root root 1587 Jul  4 18:25 passwd  
-rwxrwxrwx. 1 root root 1404 Jul  4 18:25 shadow  
[0root@rcl-centos701:etc 1^42 18:55]# puppet agent -t --tags ops  
Info: Using configured environment 'dev'  
Info: Retrieving pluginfacts  
Info: Retrieving plugin  
Info: Loading facts  
Info: Caching catalog for rcl-centos701.ops.ethalon.local  
Info: Applying configuration version '1499187366'  
Notice: /Stage[init]/Ops::Etc_files/File[/etc/passwd]/mode: mode changed '0777' to '0644'  
Notice: /Stage[init]/Ops::Etc_files/File[/etc/group]/mode: mode changed '0777' to '0644'  
Notice: /Stage[init]/Ops::Etc_files/File[/etc/shadow]/mode: mode changed '0777' to '0000'  
Notice: /Stage[init]/Ops::Etc_files/File[/etc/gshadow]/mode: mode changed '0777' to '0000'  
Info: Stage[init]: Unscheduling all events on Stage[init]  
Notice: Applied catalog in 3.13 seconds  
[2root@rcl-centos701:etc 1^43 18:56]#
```

Filehandling: /etc-files

- Schreiben von Dateiinhalten

- cramfs
- freevxfs
- jffs
- hfs, hfsplus
- squashfs
- Udf

```
$disable_cramfs = 'yes'  
$disable_freevxfs = 'yes'  
$disable_jffs2 = 'yes'  
$disable_hfs = 'yes'  
$disable_hfsplus = 'yes'  
$disable_squashfs = 'yes'  
$disable_udf = 'yes'
```

```
'/etc/modprobe.d/CIS-Hardening.conf':  
  content => template('ops/etc/modprobe.d.CIS-Hardening.conf.erb'),;
```

- Puppet:

- Komfortables Verwalten von Dateien, Links, Verzeichnissen, ...
- Verwaltung incl. Backup der Dateien mittels MD5-Summe
- Verwalten der Berechtigungen

Filehandling: /etc-files

```
[2root@rcl-centos701:etc 1^48 19:08]# vi /etc/modprobe.d/CIS-Hardening.conf
[0root@rcl-centos701:etc 1^49 19:09]# grep false /etc/modprobe.d/CIS-Hardening.conf
install hfsplus /bin/false
install squashfs /bin/false
[0root@rcl-centos701:etc 1^50 19:09]# puppet agent --tags ops
Info: Using configured environment 'dev'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for rcl-centos701.ops.ethalon.local
Info: Applying configuration version '1499188197'
Notice: /Stage[init]/Ops::Etc_files/File[/etc/modprobe.d/CIS-Hardening.conf]/content:
--- /etc/modprobe.d/CIS-Hardening.conf 2017-07-04 19:09:35.803852809 +0200
+++ /tmp/puppet-file20170704-5952-ocvbhj 2017-07-04 19:10:06.679993478 +0200
@@ -5,7 +5,7 @@
+install freevxfs /bin/true
+install jffs2 /bin/true
+install hfs /bin/true
-install hfsplus /bin/false
-install squashfs /bin/false
+install hfsplus /bin/true
+install squashfs /bin/true
install udf /bin/true

Info: Computing checksum on file /etc/modprobe.d/CIS-Hardening.conf
Info: /Stage[init]/Ops::Etc_files/File[/etc/modprobe.d/CIS-Hardening.conf]: Filebucketed /etc/modprobe.d/CIS-Hardenin
Notice: /Stage[init]/Ops::Etc_files/File[/etc/modprobe.d/CIS-Hardening.conf]/content:

Notice: /Stage[init]/Ops::Etc_files/File[/etc/modprobe.d/CIS-Hardening.conf]/content: content changed '{md5}f36eaff40
Info: Stage[init]: Unscheduling all events on Stage[init]
Notice: Applied catalog in 3.46 seconds
[2root@rcl-centos701:etc 1^51 19:10]#
```

Verzeichnishandling: sudo

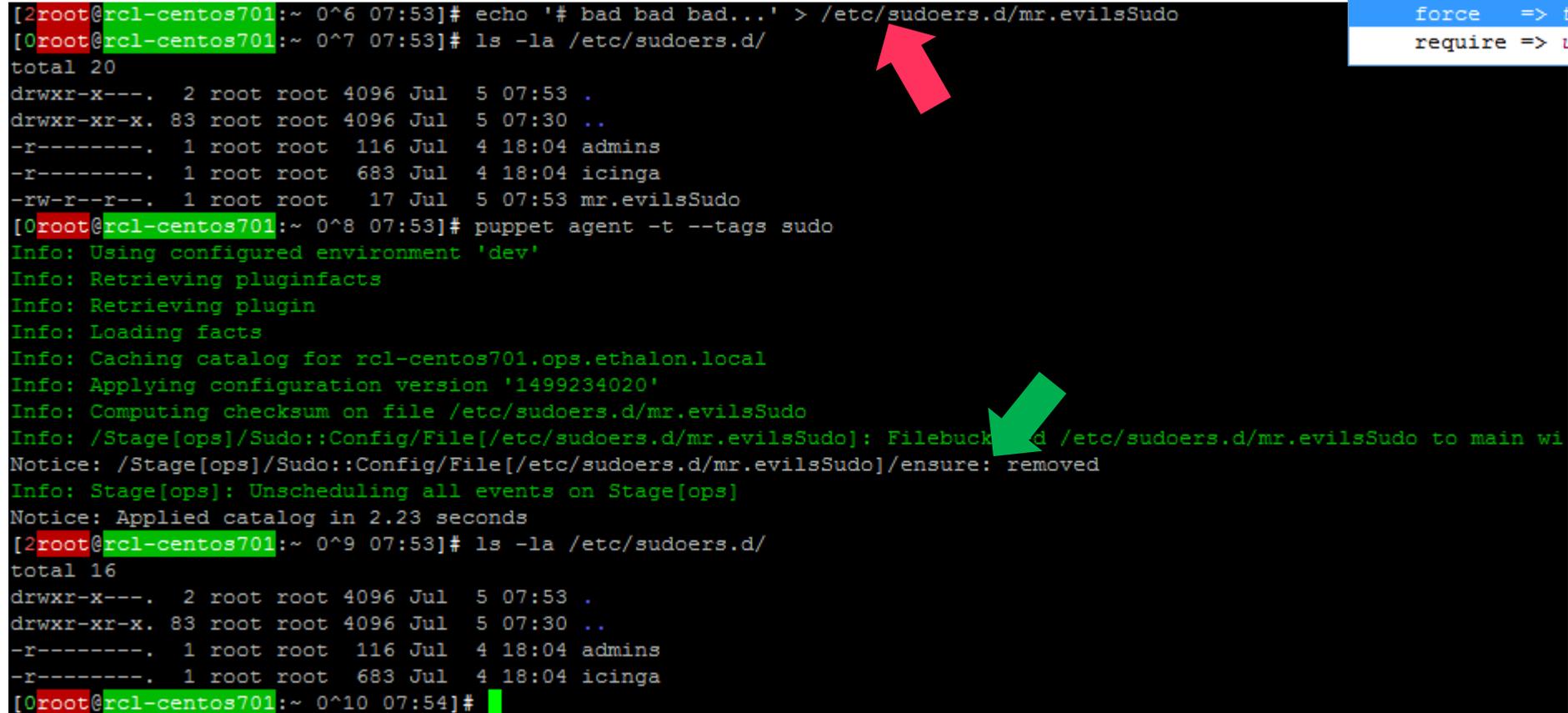
- Eskalieren von Berechtigungen ausschließlich mittels Passworteingabe
- Ausgelagerte Konfiguration (/etc/xxxx.d/...)
- Puppet:
 - Verwaltung von Verzeichnissen analog zu Dateien
 - Berechtigungen
 - Inhalte (Dateien, weitere Unterverzeichnisse)
 - Zusätzlich - Bereinigen von Verzeichnissen:
 - Rekursiv
 - Purge
 - Force



Verzeichnishandling: sudo

```
'/etc/sudoers.d':  
ensure => directory,  
mode   => '0750',  
purge  => true,  
recurse => true,  
force  => true,  
require => undef;
```

```
[2root@rcl-centos701:~ 0^6 07:53]# echo '# bad bad bad...' > /etc/sudoers.d/mr.evilsSudo  
[0root@rcl-centos701:~ 0^7 07:53]# ls -la /etc/sudoers.d/  
total 20  
drwxr-x---. 2 root root 4096 Jul  5 07:53 .  
drwxr-xr-x. 83 root root 4096 Jul  5 07:30 ..  
-r-----. 1 root root  116 Jul  4 18:04 admins  
-r-----. 1 root root  683 Jul  4 18:04 icinga  
-rw-r--r--. 1 root root   17 Jul  5 07:53 mr.evilsSudo  
[0root@rcl-centos701:~ 0^8 07:53]# puppet agent -t --tags sudo  
Info: Using configured environment 'dev'  
Info: Retrieving pluginfacts  
Info: Retrieving plugin  
Info: Loading facts  
Info: Caching catalog for rcl-centos701.ops.ethalon.local  
Info: Applying configuration version '1499234020'  
Info: Computing checksum on file /etc/sudoers.d/mr.evilsSudo  
Info: /Stage[ops]/Sudo::Config/File[/etc/sudoers.d/mr.evilsSudo]: Filebucket => d /etc/sudoers.d/mr.evilsSudo to main wi  
Notice: /Stage[ops]/Sudo::Config/File[/etc/sudoers.d/mr.evilsSudo]/ensure: removed  
Info: Stage[ops]: Unsheduling all events on Stage[ops]  
Notice: Applied catalog in 2.23 seconds  
[2root@rcl-centos701:~ 0^9 07:53]# ls -la /etc/sudoers.d/  
total 16  
drwxr-x---. 2 root root 4096 Jul  5 07:53 .  
drwxr-xr-x. 83 root root 4096 Jul  5 07:30 ..  
-r-----. 1 root root  116 Jul  4 18:04 admins  
-r-----. 1 root root  683 Jul  4 18:04 icinga  
[0root@rcl-centos701:~ 0^10 07:54]#
```



Pakete/Services: unwanted packages/services

- Entfernen unerwünschter Services:

- NetworkManager-wait-online,
- NetworkManager, chargen-*,
- daytime-*, echo-*, tcpmux-server,
- avahi-*, cups, telnet, snmp

- Entfernen unerwünschter Pakete:

- net-snmp, nis, rsh, telnet,
- telnet-server, talk, talk-server, tftp,
- tftp-server, ypbind, ypserv, xinetd,

- Puppet:

- Verwendung von Arrays
- Packages werden NICHT gepurged!
- Services werden gepurged (in Arbeit)

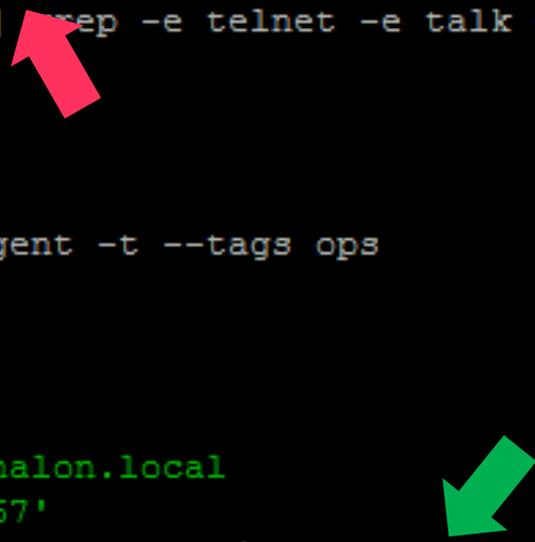
```
$unwanted_packages = [  
  'telnet-server',  
  #...  
  'net-snmp']  
$unwanted_services = [  
  'NetworkManager-wait-online',  
  #...  
  'snmpd']
```

```
service { [$::ops::hardening::unwanted_services]:  
  ensure => false,  
  enable => false,  
}
```

```
# unwanted Packages  
package { [$::ops::hardening::unwanted_packages,]: ensure => absent, }
```

Package/Services: unwanted packages/services

```
[2root@rcl-centos701:etc 1^62 19:52]# yum install -qy telnet-server talk-server rsh > /dev/null 2>&1
[0root@rcl-centos701:etc 1^63 19:52]# rpm -qa | grep -e telnet -e talk -e rsh
telnet-0.17-60.el7.x86_64
telnet-server-0.17-60.el7.x86_64
rsh-0.17-76.el7_1.1.x86_64
talk-server-0.17-46.el7.x86_64
[0root@rcl-centos701:etc 1^64 19:52]# puppet agent -t --tags ops
Info: Using configured environment 'dev'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for rcl-centos701.ops.ethalon.local
Info: Applying configuration version '1499190767'
Notice: /Stage[init]/Ops::Packages/Package[telnet-server]/ensure: removed
Notice: /Stage[init]/Ops::Packages/Package[rsh]/ensure: removed
Notice: /Stage[init]/Ops::Packages/Package[talk-server]/ensure: removed
Info: Stage[init]: Unsheduling all events on Stage[init]
Notice: Applied catalog in 3.44 seconds
[2root@rcl-centos701:etc 1^65 19:53]# rpm -qa | grep -e telnet -e talk -e rsh
telnet-0.17-60.el7.x86_64
[0root@rcl-centos701:etc 1^66 19:53]#
```



Hiera: Trennung von Code und Konfiguration

- Swappiness

- Serversystem – Swappen vermeiden
- Konfiguration eventuell individuell vom jeweiligen System abhängig

```
class ops::sysctl (String $swapamount, Boolean $deactivate_IPv6) {  
  # Configure Swappiness on Linux  
  sysctl { 'vm.swappiness':  
    ensure => present,  
    value  => $swapamount,  
    comment => 'Set Swappiness',  
    apply  => true  
  }  
}
```

- IPv6 Stack für interne Systeme deaktivieren

- Puppet:

- Trennung von Code und Konfiguration
- Konfiguration folgt Vererbungshierarchie

```
:hierarchy:  
- "10_fqdn/%{::fqdn}"  
- "20_domain/domain_%{::domain}"  
- "30_host_environment/host_environment_%{::ops_host_environment}"  
- "40_environment/environment_%{::environment}"  
- common
```

MOS (Multi OS Support): Cron

- Unterschiedliche Pakete/Paketnamen
 - RedHat: crontabs, crone, crone-noanacron
 - SuSE: cronie, cron
- Unterschiedliche Servicenamen
 - RedHat: crond
 - SuSE: cron



```
case ($::ops_os) {
  $::os_name_centos6 : {
    $mos_packages = ['cronie-noanacron', 'crontabs', 'cronie']
    $mos_rm_anacron = true
    $mos_service_name = 'crond'
  }
  $::os_name_centos7 : {
    $mos_packages = ['cronie-noanacron', 'crontabs', 'cronie']
    $mos_rm_anacron = true
    $mos_service_name = 'crond'
  }
  $::os_name_opensuse42 : {
    $mos_packages = ['cronie', 'cron']
    $mos_rm_anacron = false
    $mos_service_name = 'cron'
  }
}
```

Service: Cron

- Handling v. daily, hourly, monthly, weekly, cron.d
- Managing:
 - Anlegen: /etc/at.allow, /etc/cron.allow, /etc/crontab
 - Löschen: /etc/at.deny, /etc/cron.deny, /etc/anacrontab

- **cronie-anacron**

- Serverbetrieb -> nicht notwendig
- Deinstallieren ohne Abhängigkeiten
- Deinstallation vor cronie Installation

```
package { 'cronie-anacron':  
  ensure      => absent,  
  provider    => rpm,  
  uninstall_options => '--nodeps',  
  before      => Package[$::cronie::install::mos_packages],  
}
```

- **Puppet:**

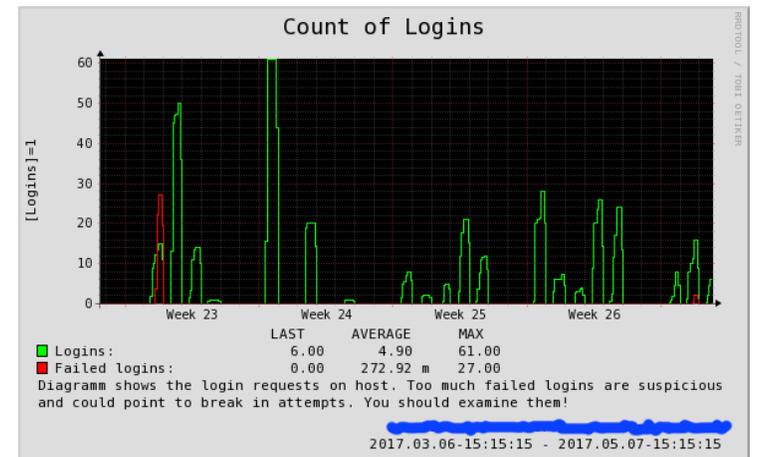
- Neustart des Service config-Änderungen

```
service { $::cronie::params::mos_service_name:  
  ensure  => true,  
  enable  => true,  
  subscribe => Class[$::cronie::config]  
}
```

audit-Daemon

- install.pp
 - package – installieren des auditd-Packages
 - cron – Anlegen des Cronjobs für Generierung des aureports
 - files – Anlegen von Scripts und Unitfiles
 - exec - Audit daemon neu laden
- config.pp
 - Anlegen der Rules
- icinga.pp
 - Anlegen des checks für
 - den aureport

```
class audit_daemon {
    $aureport_log_file_path = '...'
    class { '::audit_daemon::params': } ->
    class { '::audit_daemon::hardening': } ->
    class { '::audit_daemon::install': } ->
    class { '::audit_daemon::config': } ->
    class { '::audit_daemon::service': } ->
    class { '::audit_daemon::cleanup': } ->
    class { '::audit_daemon::icinga': }
}
```



```
::icinga2_agent_ops::add_service_vars { $module_name:
    procs => {
        $module_name => {
            cmd_name => 'auditd',
            warn_nb => "${app_proc_running_w_low}:${app_proc_running_w_high}",
            crit_nb => "${app_proc_running_c_low}:${app_proc_running_c_high}",
            user => 'root',
            notify => false,
```

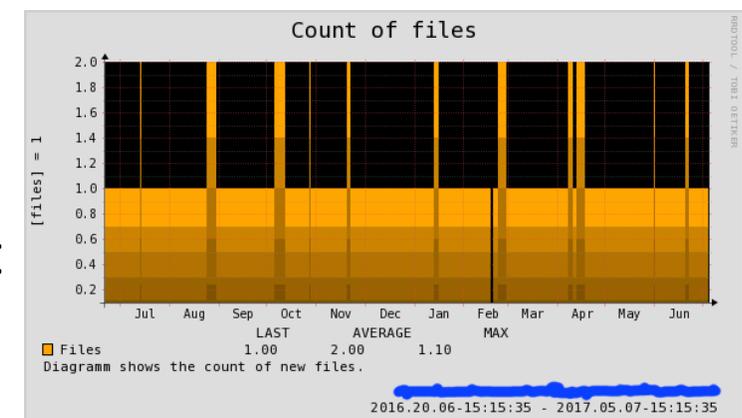
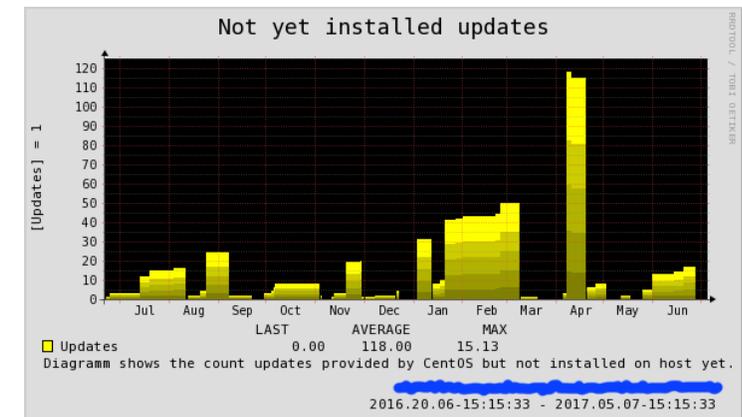
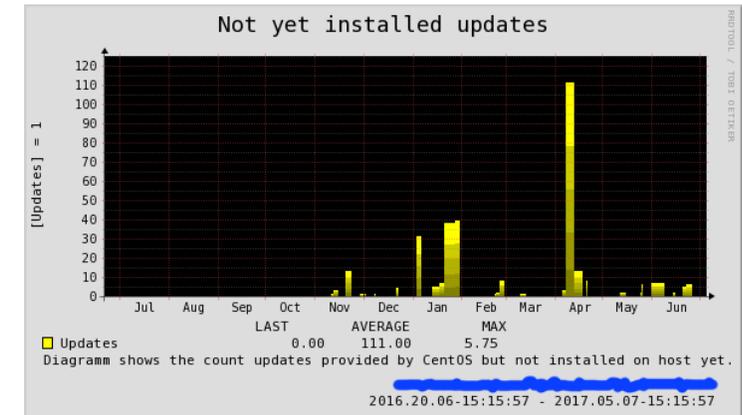
sshd

- Ausschließlich Public Key Authentication
- Ausschließlich named User
 - root Zugriff via sudo-Eskalation
- Kein root-Login
- Chiphren und Kex-Algorithmen beschränkt
 - putty + WinScp-Version aktualisieren
 - Anpassung der Chiphren entsprechend Empfehlungen der Pen-Tester
- Strict mode
- LoginGraceTime
- ...



Update Prozess

- Gesteuert via Cron
 - Dev: Aktualisierung alle 10 Minuten
 - Test: Aktualisierung jeden Tag zu fester Zeit
 - Live: Aktualisierung manuell
- Monitoring
 - Anzahl offener Updates
 - Anzahl neu zu startender Prozesse
- Kernel
 - Ausschließlich und einzig aktueller Kernel installiert
 - Anzahl der Kernel im Monitoring



User: Verwalten von Usern

- User (+ Gruppen) verwalten:
 - Benutzernamen + UID einmalig in gesamter Umgebung (--> NFS-Shares)
 - Primäre Gruppe
 - Optional: Passworthash
 - Homeverzeichnis
 - .ssh-Verzeichnis
 - Berechtigungen: 0700
 - authorized_keys, Berechtigungen 0600
 - Startumgebung
 - Rot hinterlegter Username bei root-Zugriff
 - Farbige Cursors für live (rot), test/qs (gelb), dev/private (grün)

```
'xxxx-user':  
  email      => 'xxxx-user@it-informatik.de',  
  groups     => [  
    'admins',  
    #...  
    'git_grp_eth-tms-jobs'],  
  group_name => 'ops',  
  password_hash => '$6$2/M9pXLZ...pL/',  
  rsa_key     => 'AAAAB3NzaC1...dkEhns=',  
  uid        => 1001;
```

```
user { $user_name:  
  ensure      => $ensure,  
  gid         => $group_name,  
  home        => $home,  
  groups      => $groups,  
  password    => $password_hash,  
  membership  => inclusive,  
  managehome  => $managehome,  
  shell       => $shell,  
  uid         => $uid,  
  purge_ssh_keys => true, # NOTE: Purge keys not managed  
  require     => Group[$groups],  
}
```

- ~ 130 Zeilen Code incl. Kommentar --> Überschaubare Logik

User: Hardening

- FAIL: Kein User, wenn OS unbekannt
- Unterschiedliche Root-Passwörter auf verschiedenen Systemen
- Technische Nutzer – sofern möglich – ohne loginshell
- „Unbekannte“ public Keys werden ohne Rückfrage gelöscht
- „Unbekannte“ Personen/Gruppen werden ohne Rückfrage beseitigt ;-(
)

```
resources { 'user':  
  purge => $user_enable_purge,  
  noop  => $user_enable_noop,  
  unless_system_user => $user_unless_system_user  
}
```

```
resources { 'group':  
  purge => $group_enable_purge,  
  require => Resources['user'], # NOTE: Don't rem  
  noop => $group_enable_noop,  
}
```

```
purge_ssh_keys => true, # NOTE: Purge keys not mana
```

User: Hardenings

```
[0root@rcl-centos701:~ 0^14 16:55]# sudo -iu mr.evil
sudo: unknown user: mr.evil
sudo: unable to initialize policy plugin
[1root@rcl-centos701:~ 0^15 16:55]# useradd -c 'evil user' mr.evil -g admins
[0root@rcl-centos701:~ 0^16 16:55]# sudo -iu mr.evil
[mr.evil@rcl-centos701 ~]$ logout
[0root@rcl-centos701:~ 0^17 16:55]# puppet agent -t --tags groups_users
Info: Using configured environment 'dev'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for rcl-centos701.ops.ethalon.local
Info: Applying configuration version '1499266575'
Notice: /Stage[apps]/Groups_users::Cleanup/User[mr.evil]/ensure: removed
Info: Stage[apps]: Unscheduling all events on Stage[apps]
Notice: Applied catalog in 2.00 seconds
[2root@rcl-centos701:~ 0^18 16:56]# sudo -iu mr.evil
sudo: unknown user: mr.evil
sudo: unable to initialize policy plugin
[1root@rcl-centos701:~ 0^19 16:56]#
```

```
[1root@rcl-centos701:~ 0^19 16:56]# vi /home/rclaus/.ssh/authorized_keys
[0root@rcl-centos701:~ 0^20 17:04]# puppet agent -t --tags groups_users
Info: Using configured environment 'dev'
Info: Retrieving pluginfacts
Info: Retrieving plugin
Info: Loading facts
Info: Caching catalog for rcl-centos701.ops.ethalon.local
Info: Applying configuration version '1499267086'
Notice: /Stage[init]/Groups_users::Human_users/Groups_users::Manage_user[rclaus]/Ssh_authorized_key[rclaus (ronald.claus@irgendwo.de)]/ensure: removed
Info: Computing checksum on file /home/rclaus/.ssh/authorized_keys
Info: Groups_users::Manage_user[rclaus]: Unscheduling all events on Groups_users::Manage_user[rclaus]
Notice: Applied catalog in 2.04 seconds
[2root@rcl-centos701:~ 0^21 17:04]#
```

Out of Scope...

- Automatisierung
 - Vermeidung von Routine- und somit Konfigurationsfehlern
 - Replizier- und somit Skalierbarkeit
- Übernahme der Module ins Monitoring
 - Jedes Modul weiß, wie es gern überwacht wäre
 - Wichtige Checks (→ auditReport) werden nicht „vergessen“

Top

- PenTest
 - “Was soll ich hier finden – Alle Updates regelmäßig eingespielt, Kernel auf aktuellstem Stand...”
 - Issues fixed in weniger als einer Woche
- Heartbleet: Fix aller Systeme am selben Tag
- Drown: Fix aller Systeme am selben Tag
- Sämtliche interne Kommunikation verschlüsselt

Nächste Schritte

- SELinux: per default aktiv
- Firewall: Per Default inaktiv
- Evaluierung Purgen der Ressourcen
 - Cron
 - Service
 - Public_key
 - Ssh_key
- Public Key Authentifizierung f. techn. User an Befehle binden
- Sudo-Eskalation auf konkrete Befehle binden

Gehen wir es an....

