

Bezpečnost v Red Hat Enterprise Linuxu

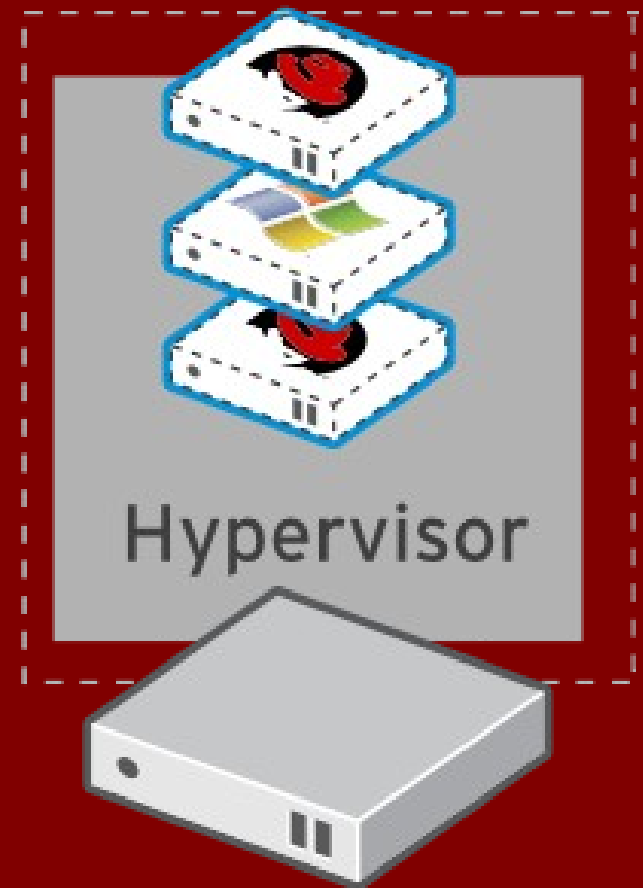
Radek Langkramer, konsultant

Agenda

- kompletní stack
 - virtualizace
 - platforma
 - update a identity management
- RHEL technologie
 - SELinux
- SSSD a ti druzí
- errata
- životní cyklus

Virtualizace: Red Hat Enterprise Virtualization

- baremetal hypervisor X RHEL
- live migration
- maintenance režim
- system scheduler
- power saver
- high availability
- thin provisioning
- ksm
- mnoho dalších funkcí...



Platforma: RHEL

bezpečný



výkonný



moderní



zelený

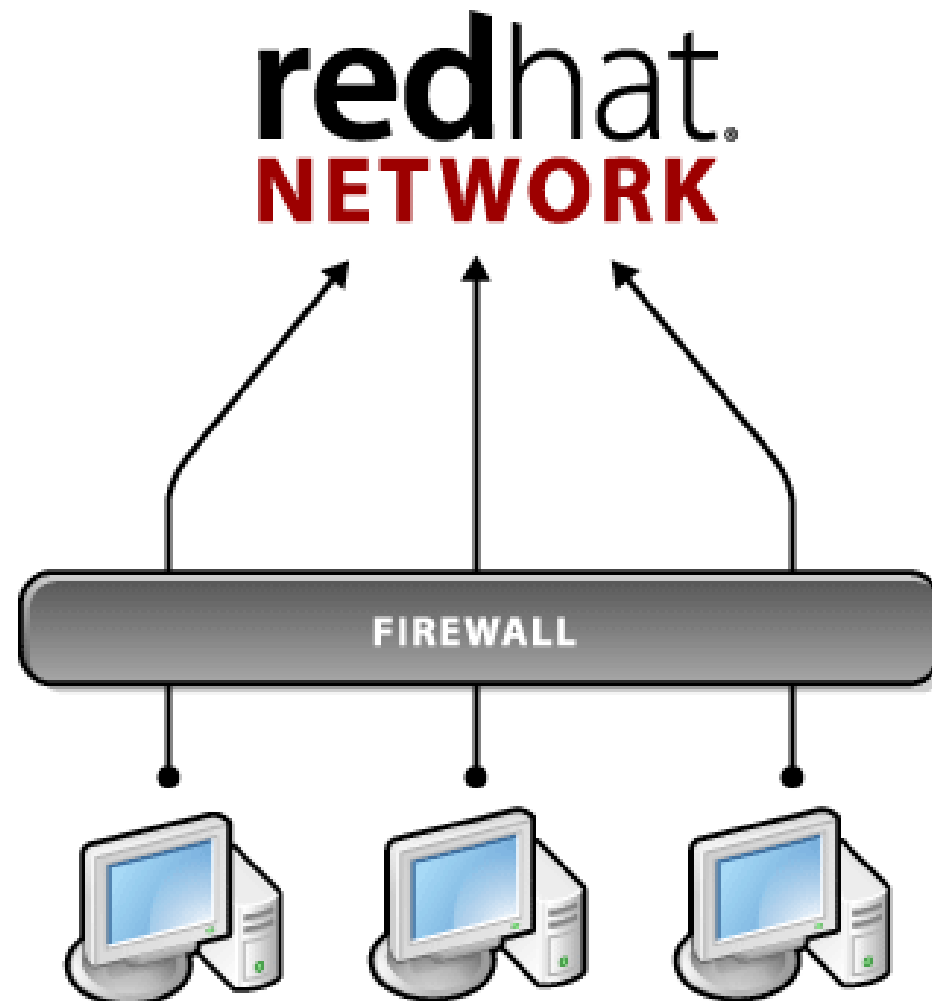


enterprise

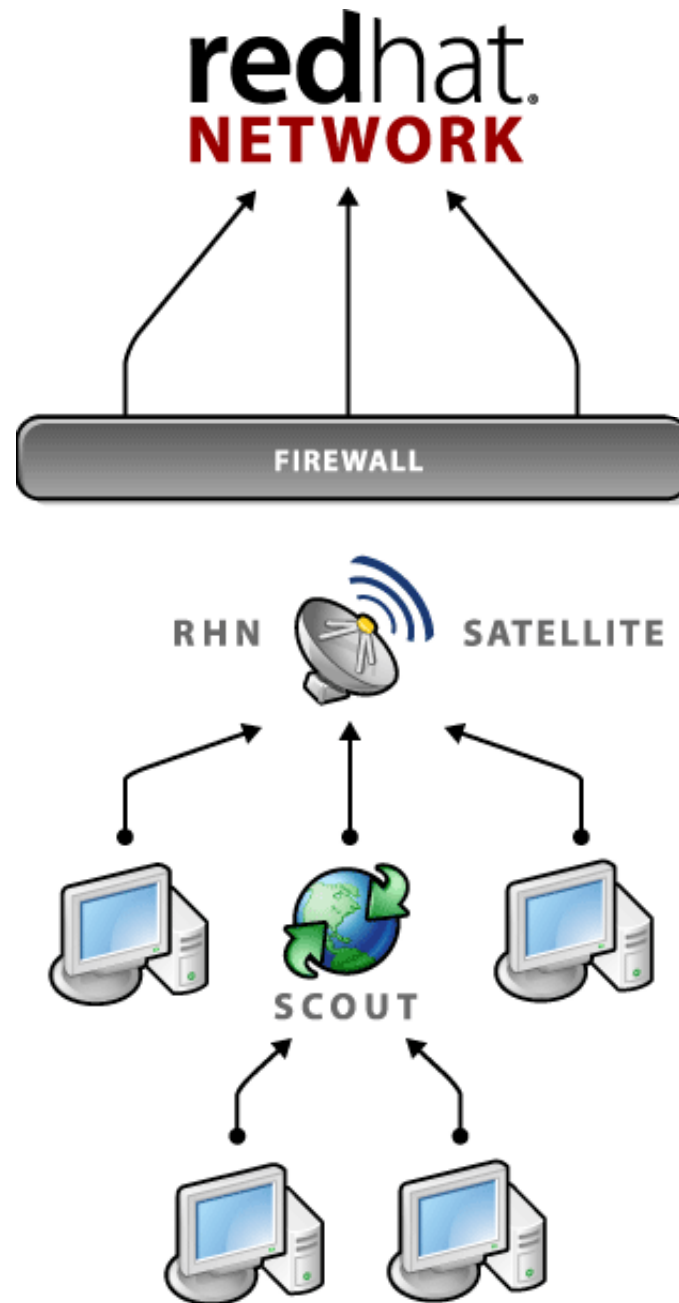


10. listopadu, 2010

Management: Red Hat Network Satellite

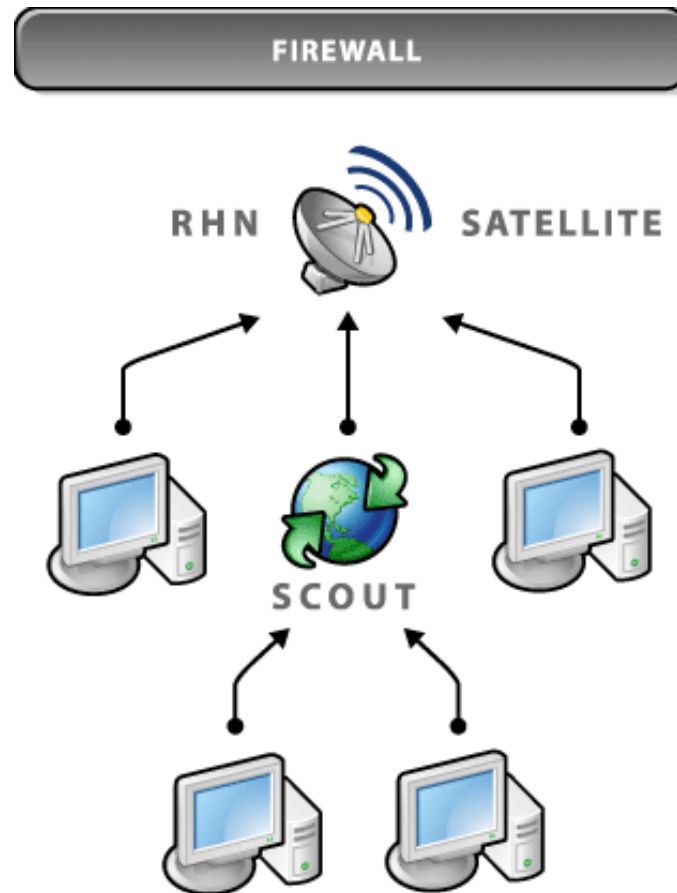


Management: Red Hat Network Satellite

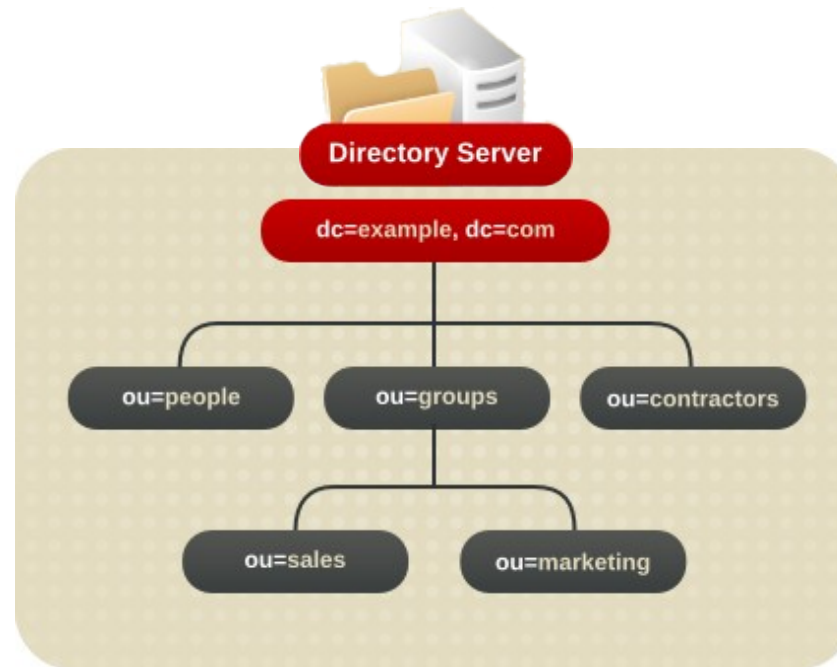


Management: Red Hat Network Satellite

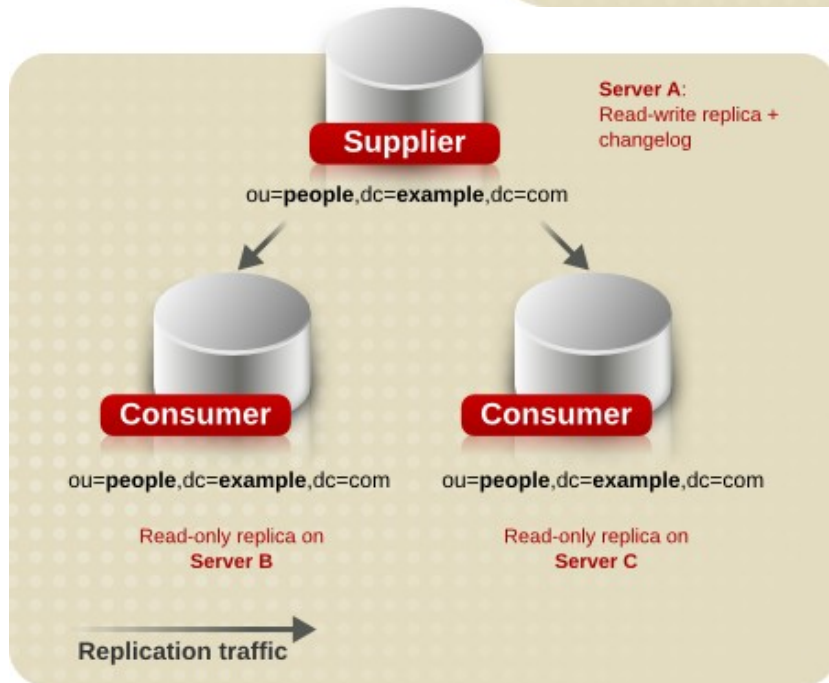
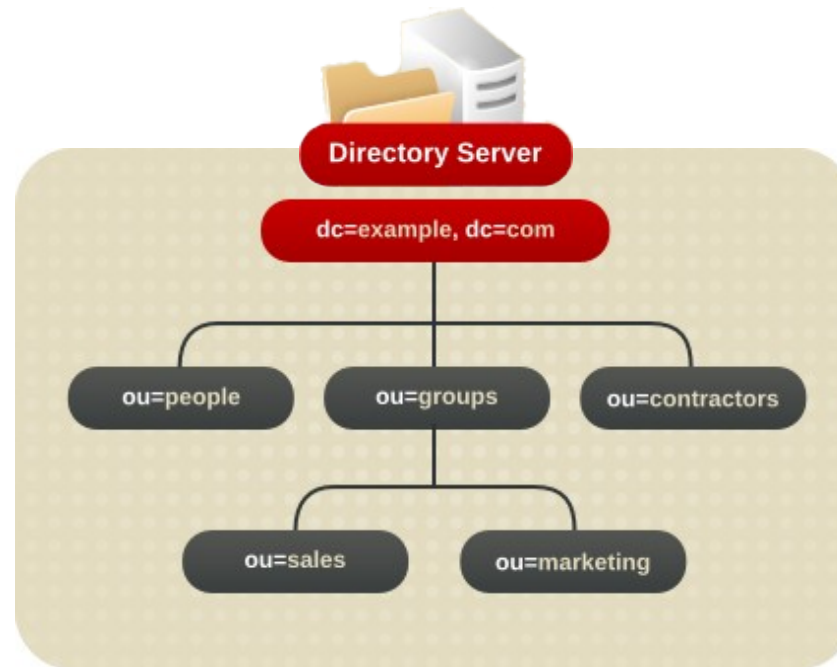
Disconnected mode



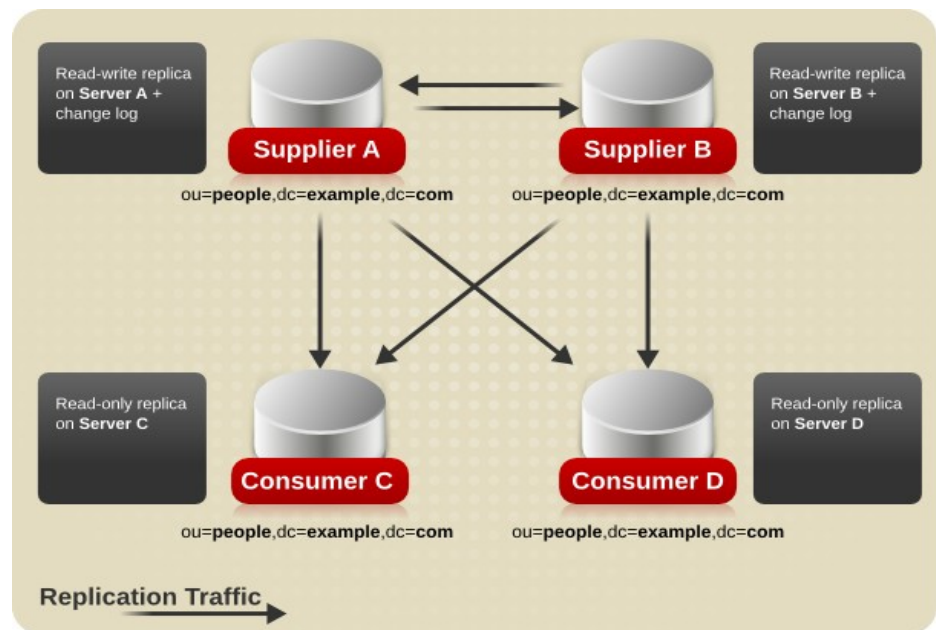
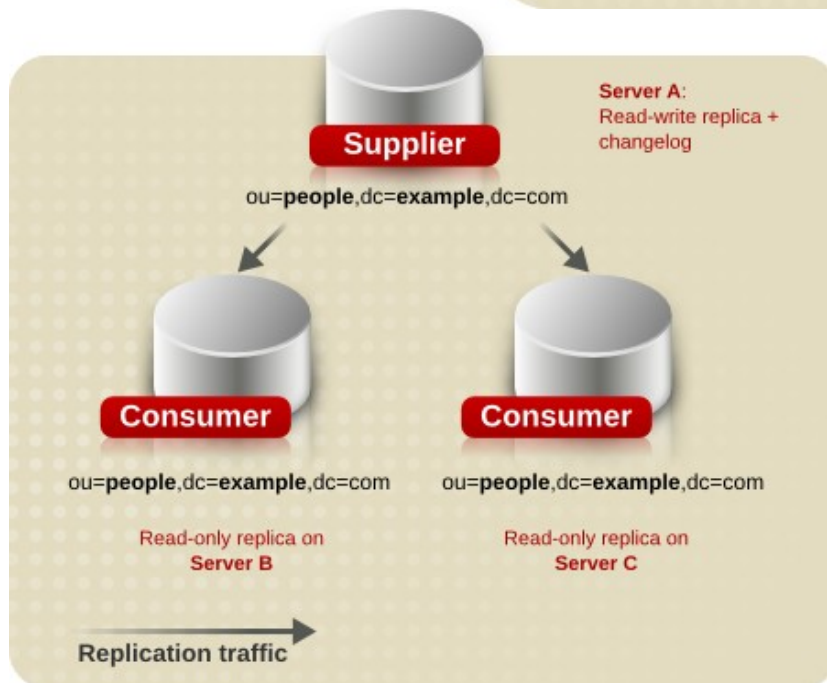
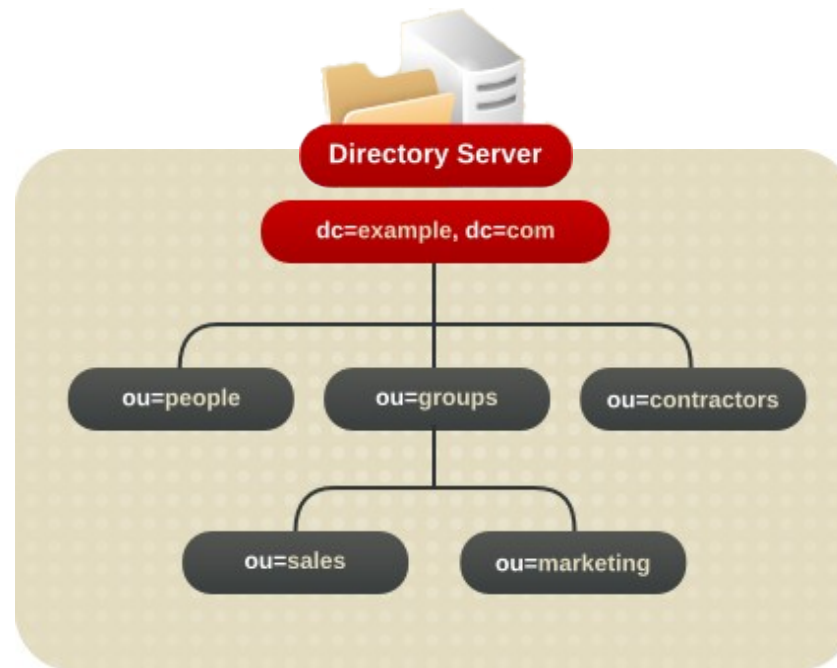
Identity management: Red Hat Directory Server



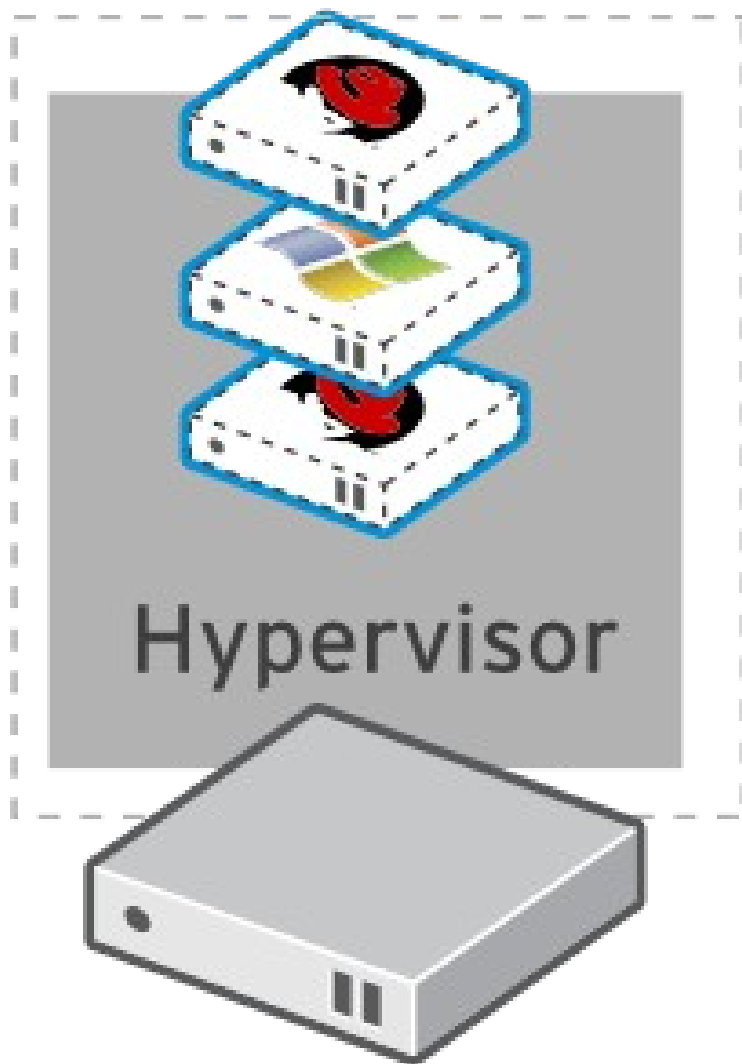
Identity management: Red Hat Directory Server



Identity management: Red Hat Directory Server



Kompletní prostředí



10. listopadu, 2010

Platforma: RHEL

bezpečný



výkonný



moderní



zelený



enterprise



10. listopadu, 2010

access control - řízení přístupu

- DAC - Discretionary access control
 - UNIXová práva jsou příliš široce definovaná
 - vlastník může vše
 - User, Group, Others
 - rwx
- POSIXová ACL
 - rwx
 - chybí append, modify
 - špatná přenositelnost
- MAC - Mandatory access control
 - nastavuje bezp. administrátor
 - platnost do změny politiky
 - SELinux



<http://www.nsa.gov/>

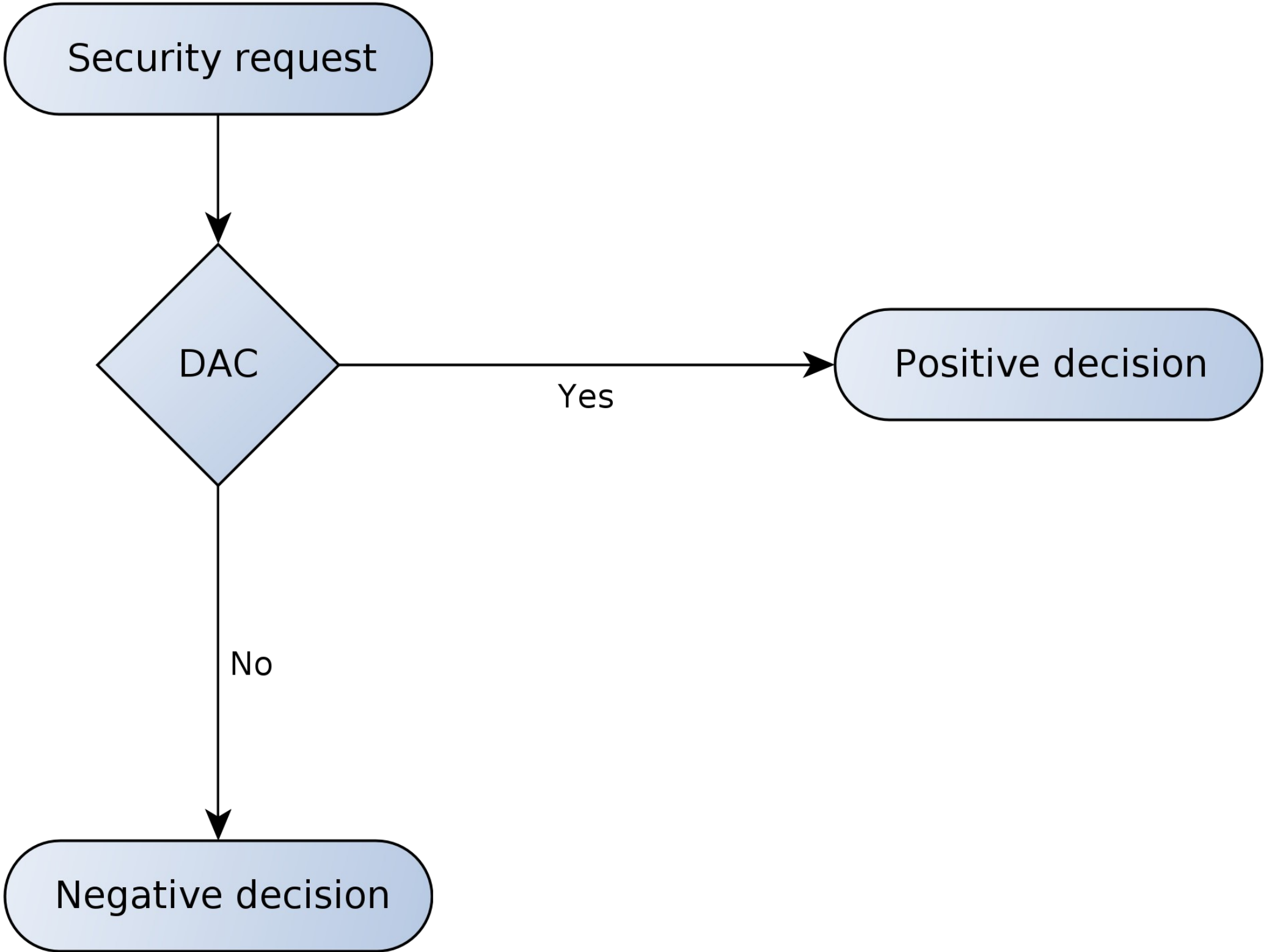
- vládní organizace USA
- 1950
- speciální pravomoce
- „Velké ucho“
- databanka tajných informací
- utajení a zabezpečení
- linux v jejich službách

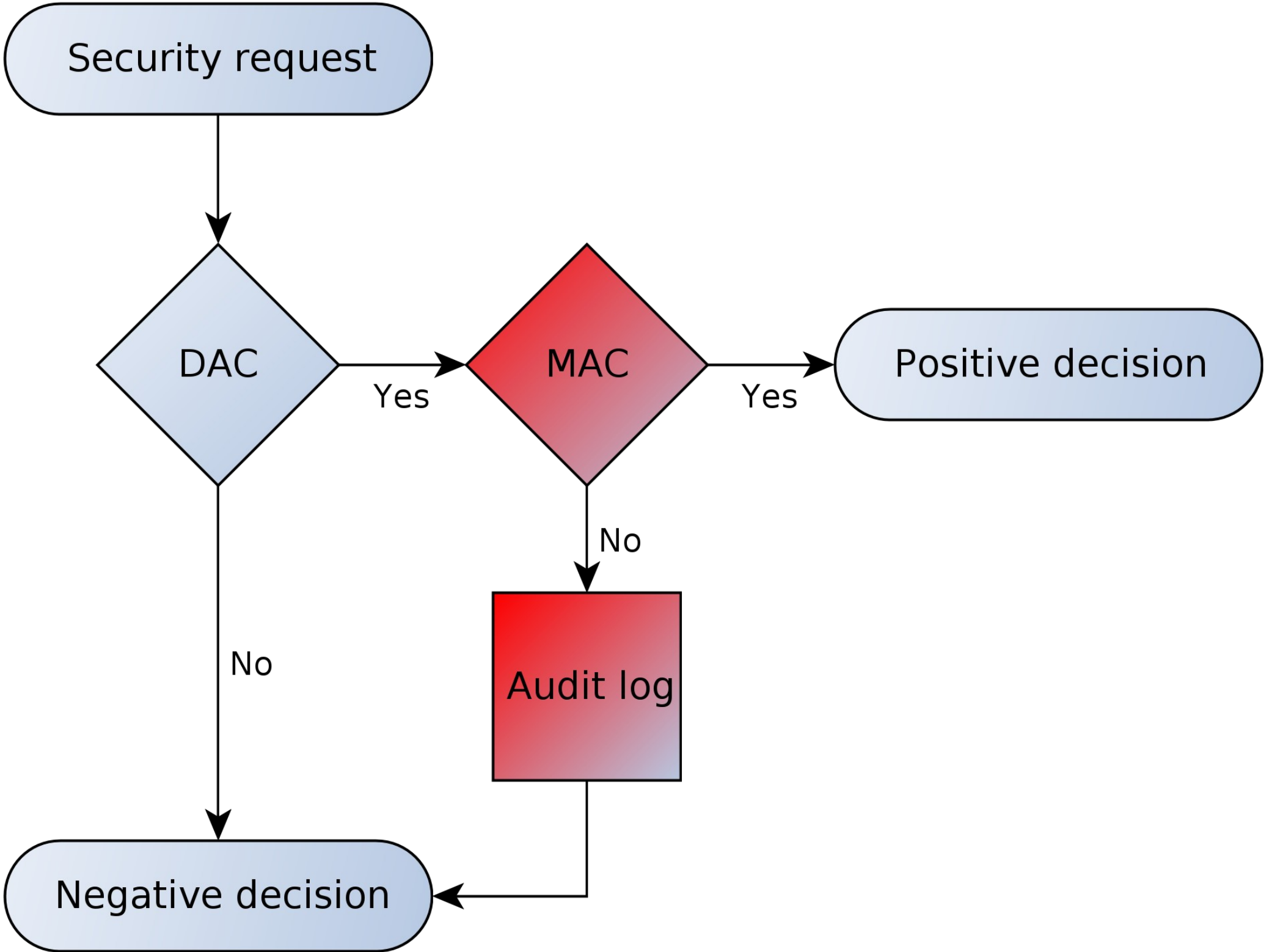


SELinux

- implementuje MAC do Linuxu
- GNU General Public Licence
- od 2.6 ve vanilla kernelu
- přímo ovládá systémová volání
 - file
 - directory
 - process
 - port
- bezpečnost na základě politik
- kontrola superuživatele
- RHEL 4, 5, 6

RBAC - „role based access control“ řeší, kdo (míněno uživatel, člověk) smí co dělat,
TE - „Type enforcement“ stará se o to, který proces smí dělat nějakou činnost
MLS - „multi level security“ určuje, jakým způsobem smí proudit v systému data.





security

System Security Services Daemon (SSSD)

identity a authentication management
RHDS, AD, LDAP, 389, Kerberos a LDAP
lokální kešování

Enterprise Security Client

smartcard, tokeny

cryptosetup a luks

backup passphrase - aneb nic
není ztraceno

sVirt

nejen virtuální
bezpečnost

Netfilter

firewall v jádře
iptables

cGroups

správa prostředů



Red Hat Errata

typ:



security



bug fixes



enhancements

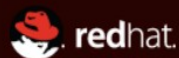
dopad:

critical

important

moderate

low



CUSTOMER PORTAL

Red Hat Network | Try OpenShift

Search

Help | Register or Log in

Advanced Search



Knowledge

Groups

Support

Downloads

Security

Subscriptions



Red Hat Enterprise Linux Server (v. 6) General Advisories

Security



Bug Fix



Enhancement



Jump to: [[all](#) | [security](#) | [bug fixes](#) | [enhancements](#)]

Type	Severity	Advisory	Synopsis	Date
	Critical	RHSA-2011:0856	Critical: java-1.6.0-openjdk security update	2011-06-08
	Moderate	RHSA-2011:0858	Moderate: xerces-j2 security update	2011-06-08
	Moderate	RHSA-2011:0859	Moderate: cyrus-imapd security update	2011-06-08
	Moderate	RHSA-2011:0862	Moderate: subversion security update	2011-06-08
		RHBA-2011:0848	openssh bug fix update	2011-06-02
		RHBA-2011:0849	sssd bug fix update	2011-06-02
	Important	RHSA-2011:0836	Important: kernel security and bug fix update	2011-06-01
		RHEA-2011:0846	libgcrypt enhancement update	2011-05-31
	Moderate	RHSA-2011:0839	Moderate: gimp security update	2011-05-31
	Moderate	RHSA-2011:0842	Moderate: systemtap security update	2011-05-31
	Moderate	RHSA-2011:0843	Moderate: postfix security update	2011-05-31

životní cyklus

Production 1 (Approximately 4 years)				Production 2 (Approximately 1 year)	Production 3 (Approximately 2 years)		Extended Life Cycle (Additional 3 years)		
Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Year 9	Year 10

některé reference v ČR





Děkuji za pozornost

Radek Lagnkramer
konzultant
langkramer@servodata.net