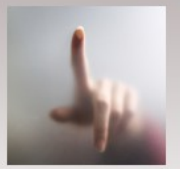
Linuxový dotykový kiosek

Miloš Wimmer

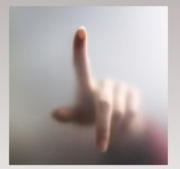
Záměr



- LF získala projekt OP VK “Modernizace didaktických metod cestou podpory systému elektronického vzdělávání (MODIM)”
- cílem je podpora pedagogů při tvorbě elektronických studijních materiálů a kurzů pro studenty
- použití moderních internetových a technických prostředků
  - nejčastěji ve formátech PDF a Flash
  - publikování na edukačním portálu MEFANET (Moodle)

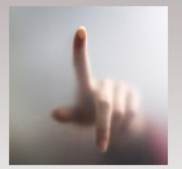
- použití velkoplošných elektronických vzdělávacích kiosků instalovaných ve veřejných prostorách LF a FN v Plzni

Požadavky na kiosky



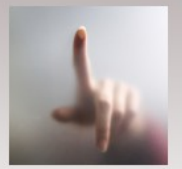
- atraktivní grafické prostředí
- řízený přístup k prezentovaným dokumentům i k jiným cílům v Internetu
  - ověřování uživatelů proti CAS UK
- podpora formátů prezentovaných dokumentů (PDF, flash)
- statistiky přístupů
- umístění do počítačových sítí LF a FN
- rozumná správa
- stabilita

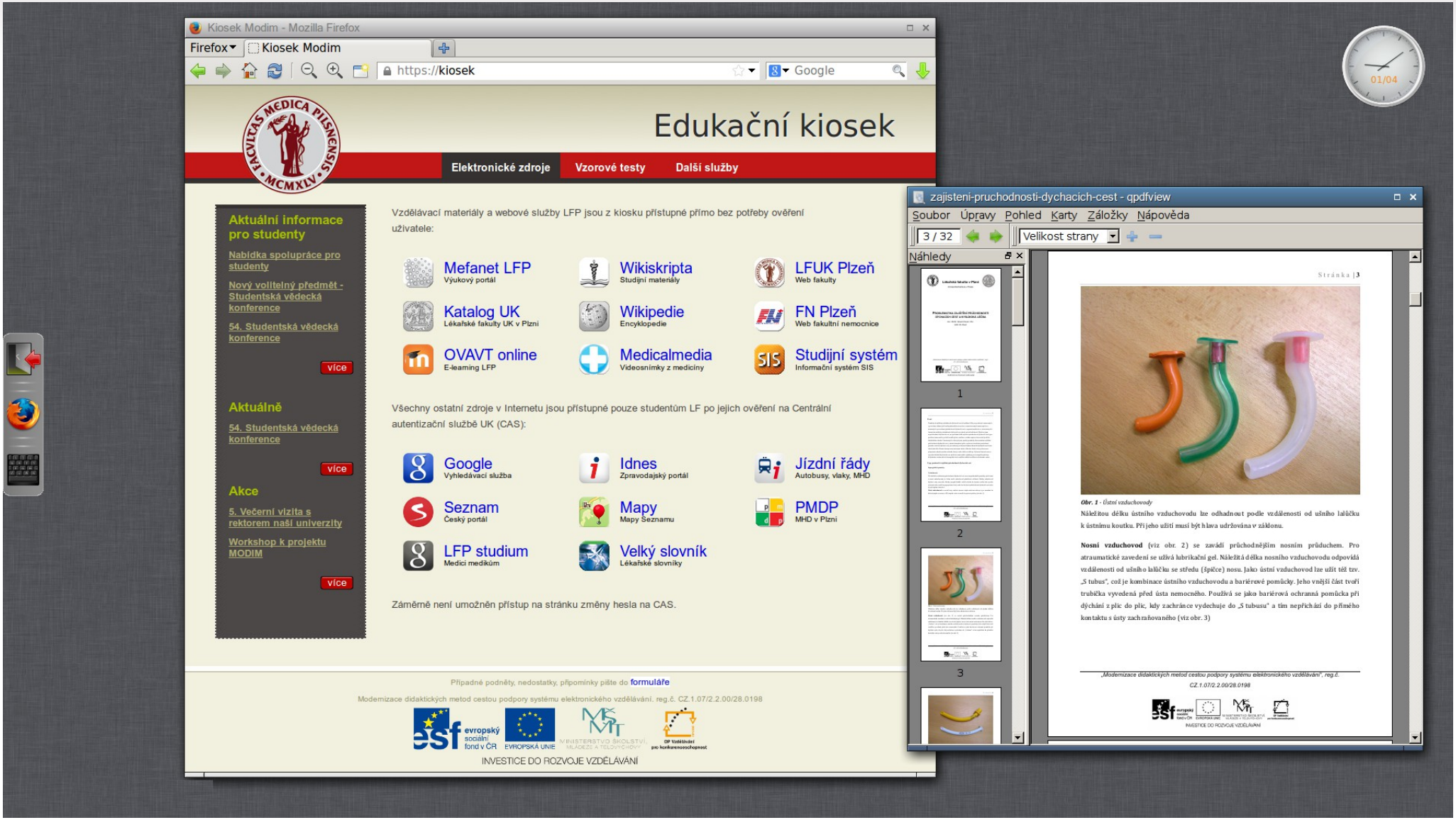
Moje požadavky na kiosky



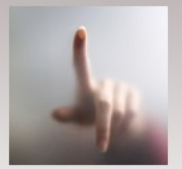
- nerozbitný systém
- co nejmenší závislost na infrastruktuře okolních sítí LF a FN
- zajištění bezpečného prostředí pro uživatele
  - integrita dat na lokálním disku
  - přenos dat sítí
  - systém ověřování uživatelů
- centralizovaná a automatizovaná správa
- všechny kiosky budou mít identický obraz disku
- otevřený systém

Ukázka kiosku, komponenty





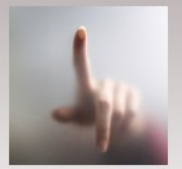
Ukázka kiosku, komponenty



- velká plocha, práce s několika současně otevřenými dokumenty
  - desktopové prostředí oken, ale s ovládáním tabletu
- zaměření na cíl,

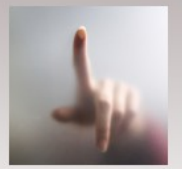
  uživatel má k dispoci jen aplikace, které potřebuje
  - WWW prohlížeč s podporou flashe
  - PDF prohlížeč
  - virtuální klávesnice
  - animovaný spouštěcí panel
- srozumitelné grafické prostředí

Ukázka kiosku, komponenty



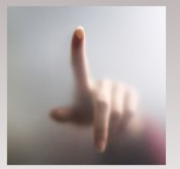
- přístup k vyjmenovaným cílům bez ověření
- přístup k ostatním cílům s ověřením (CAS)
- automatické odhlašování
- zobrazování zpráviček při neaktivitě

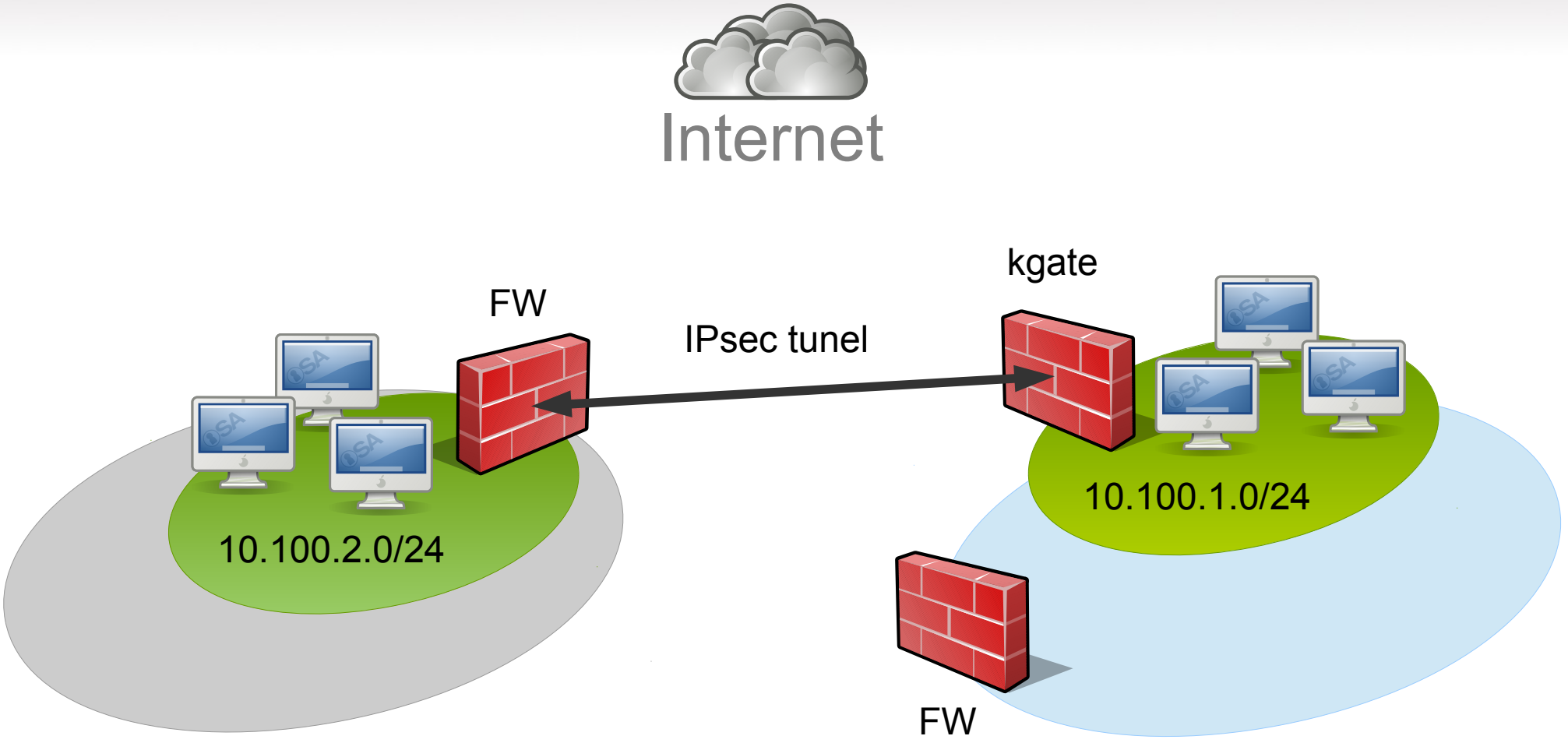
Koncepce, infrastruktura



- kiosky
  - jsou v izolovaných L2 sítích uvnitř sítí LF a FN
  - nemají přímou konektivitu do Internetu ani do sítí LF a FN
  - veškeré síťové služby jim poskytuje řídící server kgate umístěný na veřejném segmentu sítě LF
  - řízený přístup k cílům na webu jim poskytuje aplikační proxy server na kgate

Topologie

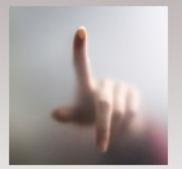




síť FN

síť LF UK

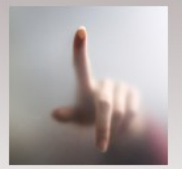
Popis hardwaru kiosku



- Elo TouchSystems ET4200L
- 42” dotykový LED panel, 1920x1080 bodů
- PC integrované do těla monitoru v podobě vyjímatelného kovového šuplíku
- integrované reproduktory

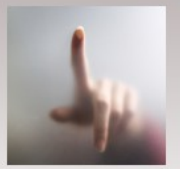
  - instalace na stěnu
  - doplněno zajištěním proti demontáži a přístupu k portům

Popis hardwaru kiosku



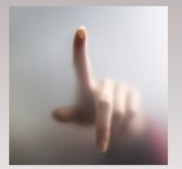
- Konfigurace PC
  - CPU Intel Core Duo / 3 GHz
  - 2 GB RAM
  - disk 160 GB
  - eth Gb
  - akcelerovaná grafická karta Intel
  - USB porty

Systém kiosku



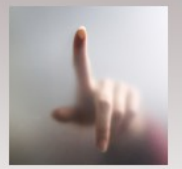
- Linux nebo Android?
- Debian amd64
  - otevřený systém
  - široké možnosti, varianty komponent
  - pro mne známé prostředí
  - je nejlepší ;-)
  - distribuce Testing obsahovala poslední verze několika důležitých komponent
- celý hardware kiosku je přímo podporován distribučním jádrem 3.x

Grafické prostředí



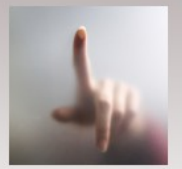
- GNOME, Xfce, KDE, MATE nebo ...?
- minimalistické X-prostředí
  - standardní xserver-xorg
  - openbox startovaný z xinitrc (definice pracovní plochy)
- kompozitní window manager - xcompmgr (stíny)
- animovaný spouštěcí panel - cairo-dock
- virtuální klávesnice - florence
- neviditelná myš - xcursor-transparent

Grafické prostředí



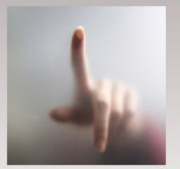
- dialogové boxy - zenity
- automatické odhlašování, spouštění screensaveru - xautolock
- screensaver - xscreensaver s modulem gslideshow (efektní prolínání obrazovek)

Grafické prostředí



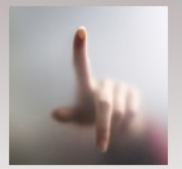
- prohlížeč Firefox
- výhoda velkého množství rozšiřujících doplňků
  - Grab and Drag
    - ovládání obsahu okna prstem stylem “chytni a táhni”
    - dynamická gesta “švihnutím”
  - Personal Menu
    - zpřístupní jen určené položky menu
  - Public Fox
    - znemožní uživateli provádět změny konfigurace i přístup k 'about:config'

Grafické prostředí



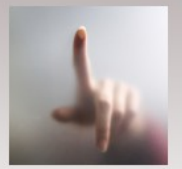
- prohlížeč PDF - qpdfview
  - mnohem lepší zpracování PDF než prohlížeč PDF integrovaný ve Firefoxu
  - ovládání obsahu okna prstem stylem “chytni a táhni”

Rozdělení disku



- systém na pevném disku nebo na NFS?
- /dev/sda1 ..... 10 GB (použito 1.4 GB)
  - systémový filesystém xfs / , připojený jako read-only
- /dev/sda2 ..... 2 GB
  - swap
- /dev/sda3 ..... 10 GB (použito 100 MB)
  - filesystém xfs používaný pro zápisy do /tmp, /var/log, /var/tmp, /home/kiosk
- /dev/sda4 ..... zbytek (použito 1.8 GB)
  - servisní (alternativní) systémový filesystém xfs
  - není připojený, používá se jen při updatech hlavního systému

Souborový systém

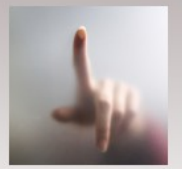


- Kiosky obsahují identický obraz všech oddílů
  - včetně UUID disků (kvůli grubu)
- systémový /dev/sda1 je připojený jako read-only
- rozdílná systémová nastavení

  `/etc/hostname /etc/hosts /etc/resolv.conf ...`
  - se získávají z DHCP serveru
  - při bootu se zapisují do souborů v tmpfs v RAM
  - překrývají originální soubory na read-only filesystému /

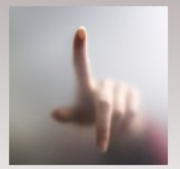
```
mount --bind /run/kiosk/etc/hostname /etc/hostname
```

Souborový systém



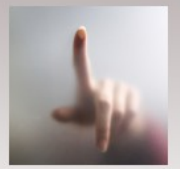
- pro zápisy je určen oddíl /dev/sda3
  - na něm se vytváří filesystém xfs při každém startu kiosku
  - příslušné adresáře /tmp , /var/log , ... , a domovský adresář uživatele kiosk, pod kterým běží GUI, jsou připojeny stejným způsobem `mount --bind`
- adresářová struktura /home/kiosk (s konfigurací sytémového prostředí a GUI)
  - vytváří se při každém přihlášení uživatele znovu
  - rozbalení archivu z read-only filesystému
  - zaručení čistého výchozího prostředí

Souborový systém



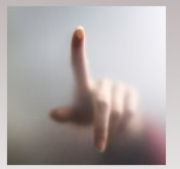
```
root@k1:~# mount
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,relatime,size=10240k,nr_inodes=247009,mode=755)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
/dev/disk/by-uuid/fadd27f2-309a-48fb-baea-5560547cadc9 on / type xfs (ro,noatime,attr2,inode64,noquota)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k)
pstore on /sys/fs/pstore type pstore (rw,relatime)
tmpfs on /run/shm type tmpfs (rw,nosuid,nodev,noexec,relatime,size=817700k)
tmpfs on /etc/hostname type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /etc/hosts type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /etc/resolv.conf type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /etc/ntp.conf type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /etc/udev/rules.d type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /var/lib/dhcp type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /var/lib/ntp type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /var/lib/quota type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
tmpfs on /var/spool type tmpfs (rw,nosuid,noexec,relatime,size=199140k,mode=755)
/dev/sda3 on /opt/rw type xfs (rw,noatime,attr2,inode64,usrquota)
rpc_pipefs on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
kgate:/usr/local/share/gallery on /usr/local/share/gallery type nfs
(ro,nosuid,nodev,relatime,vers=3,rsize=4096,wsize=4096,namlen=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,mountaddr=10.100.1.1,mountvers=3,moun
tport=56395,mountproto=udp,local_lock=none,addr=10.100.1.1)
/dev/sda3 on /tmp type xfs (rw,noatime,attr2,inode64,usrquota)
/dev/sda3 on /var/log type xfs (rw,noatime,attr2,inode64,usrquota)
/dev/sda3 on /var/tmp type xfs (rw,noatime,attr2,inode64,usrquota)
/dev/sda3 on /home/kiosk type xfs (rw,noatime,attr2,inode64,usrquota)
```

Řízený přístup kiosků k cílům



- přístup řídit na úrovni FW/iptables nebo proxy serveru?
- provádí se na úrovni aplikačního proxy serveru squid
- vyjmenované vzdělávací cíle a cíle v sítích LF a FN jsou přístupné přímo, bez ověření
- ostatní cíle jsou dostupné jen po ověření proti CAS UK (LDAP)
  - jméno / heslo
  - případně čipová karta ISIC
- všechny přístupy jsou logovány

Řídící server kgate



- Debian amd64
- funguje jako firewall pro obě sítě kiosků
- 2 síťová rozhraní
- kioskům poskytuje kompletní síťové služby
  - konektivitu do Internetu
  - DHCP (na vyjmenované MAC adresy), DNS, NTP, NFS
  - centrální syslog - rsyslog
  - domovský web server s navigací na nejvýznamnější cíle
  - aplikační proxy server s ověřováním - squid
  - IPsec tunel pro spojení se sítí kiosků ve FN - racoon

Zabezpečené spojení kiosku a kgate

- uživatelé se na kiosku mohou ověřovat
- jejich jméno/heslo je přenášeno sítí mezi kioskem a proxy serverem na kgate, který provádí jejich ověření proti CAS UK v Praze
- nutnost zabezpečeného přenosu dat mezi WWW prohlížečem na kiosku a aplikačním proxy serverem
- ... ale Firefox https komunikaci s proxy serverem nepodporuje a k dispozici není ani doplněk

Zabezpečené spojení kiosku a kgate

- vytvoření šifrovaného tunelu mezi kioskem a kgate
  - stunnel
  - na straně kiosku je v konfiguraci Firefoxu nastaven proxy server na místní začátek stunnelu http://localhost:3128
  - na straně kgate je konec jeho stunnelu propojen se vstupním portem proxy serveru
  - funguje, ale v logu proxy serveru jsou všechny přístupy logovány se zdrojovou adresou kgate (zdrojová adresa po výstupu z stunnelu)

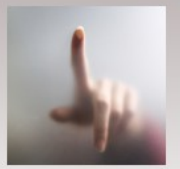
```
24/Mar/2014:07:30:23 +0100     19 127.0.0.1 TCP_MISS/301 949 GET
http://www.wikiskripta.eu/ - HIER_DIRECT/www.wikiskripta.eu
text/html
```

Zabezpečené spojení kiosku a kgate

- proxy server squid v distribuci Debianu nepodporuje šifrovaný přístup klientů přes https
  - ale ve zdrojovém kódu podpora je
- kompilace squidu s direktivami pro https přístup
- jeho použití namísto distribučního balíčku
- šifrovaný stunnel od kiosku je pak zakončen přímo na vstupním https portu squidu
  - funguje a v logu proxy serveru jsou všechny přístupy logovány se skutečnou zdrojovou adresou kiosku

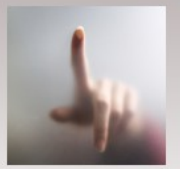
```
24/Mar/2014:07:35:49 +0100     19 10.100.1.102 TCP_MISS/301
949 GET http://www.wikiskripta.eu/ -
HIER_DIRECT/www.wikiskripta.eu text/html
```

Propojení sítí kiosků v LF a ve FN



- segment kiosků LF 10.100.1.0/24
- segment kiosků FN 10.100.2.0/24
- segment kiosků FN připojen na vyhrazené síťové rozhraní firewallu FN
- IPsec tunel mezi kgate a firewallem FN
  - ve FN používaná technologie
- kgate pracuje s oběma segmenty stejným způsobem
- na segmentu FN běží virtuální stroj
  - přes něj se vysílají WoL pakety pro startování koisků
  - běží na něm DHCP relay na kgate pro kiosky

Centralizovaná správa kiosků



- kiosky lze ovládat z řídícího serveru kgate příkazem

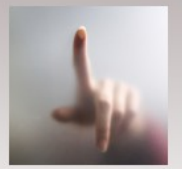
```
kadm -c {boot|halt|reboot|start|stop|restart|status} {-n}
{kiosk|all} [kiosk kiosk ...]
```

  který spouští odpovídající příkaz na určeném kiosku přes NRPE

  - boot přes WoL (povoleno v jejich BIOSu)

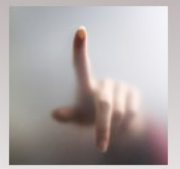
```
# kadm -c status k1

k1 up:  2:56;  session: 00:11:52;  xscreensaver: 00:00:00;
load: 0.04;  temp: +53.1°C;  version: 1396456389.1392161302
```

Dohled nad infrastrukturou



- dohledový systém Icinga /nagios
- sleduje síťové i interní služby a systémové hodnoty všech kiosků i serveru kgate
  - sledování přímo i přes NRPE
  - vlastní pluginy

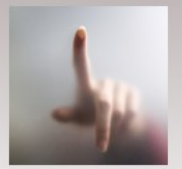
Dohled nad infrastrukturou



- služby sledované na kiosku

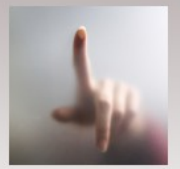
Host	Service	Status	Last Check	Duration	Attempt	Status Information	
k1.kiosk.lfp.cuni.cz	DISK /	OK	25-03-2014 09:47:05	0d 3h 18m 6s	1/4	DISK OK - free space: / 8141 MB (85% inode=99%):	
	DISK /opt/rw	OK	25-03-2014 09:48:24	0d 3h 16m 47s	1/4	DISK OK - free space: /opt/rw 10144 MB (99% inode=99%):	
	INTERFACE eth0	OK	25-03-2014 09:49:43	0d 3h 15m 28s	1/4	eth0:UP OK	
	LOAD	OK	25-03-2014 09:46:30	0d 3h 18m 41s	1/4	OK - load average: 0.00, 0.01, 0.05	
	MEM	OK	25-03-2014 09:49:49	0d 3h 15m 22s	1/4	MEMORY OK - total/used: 1991392/641604 KB	
	NTP	OK	25-03-2014 09:49:08	0d 3h 16m 3s	1/4	NTP OK: Offset -3.218650818e-06 secs	
	PING	OK	25-03-2014 09:46:27	0d 3h 18m 44s	1/4	PING OK - Packet loss = 0%, RTA = 0.30 ms	
	PROCESS firefox	OK	25-03-2014 09:49:22	0d 3h 15m 49s	1/4	PROCS OK: 1 process with command name 'firefox'	
	PROXY	OK	25-03-2014 09:48:23	0d 3h 16m 48s	1/4	HTTP OK: HTTP/1.1 200 OK - 9204 bytes in 0.025 second response time	
	SESSION	OK	25-03-2014 09:46:33	0d 3h 18m 38s	1/4	OK - session time: 03:16:06	
	TEMPERATURE	OK	25-03-2014 09:49:52	0d 3h 15m 19s	1/4	OK - temperature: +52.9°C	
	UPTIME	OK	25-03-2014 09:46:36	0d 3h 18m 35s	1/4	OK : up 0 days, 03:16:21	
	XSCREENSAVER	OK	25-03-2014 09:46:29	0d 3h 18m 42s	1/4	OK - xscreensaver time: 03:10:55	

Zprávičky do screensaveru



- LF provozuje aplikační server, do kterého jsou (pro web) zadávany aktuální zprávičky v kategoriích
  - akce, aktulality, informace pro studenty, novinky portálu Mefanet
- na kgate je z cronu spouštěn skript, který
  - z databáze aplikace získá aktuální data
  - vloží je do html šablony příslušné kategorie
  - ve virtuálním prostředí X serveru spustí cutycapt, který jádrem WebKitu vykreslí html stránku do grafického souboru
  - zkonvertuje ho do formátu png a ořízne ho na velikost plného rozlišení zobrazovače 1920x1080 bodů
  - výsledný obrázek zapíše do sdíleného adresáře, který je kioskům dostupný přes NFS

Zprávičky do screensaveru



- na kiosku běží xscreensaver
- upravený modul gslideshow sekvenčně zobrazuje obrázky všech kategorií dostupných na sdíleném NFS filesystému
- plně automatizovaný proces
- aktuální informace udržují kiosek “živý”

aktuality

1. místo v projektu Fakulta roku v oboru Lékařství a farmacie

Naše fakulta **v projektu Fakultaroku.cz** pro akademický rok 2013/2014 obsadila **1. místo v oboru Lékařství a farmacie.**

Již loni jsme v této kategorii obsadili velmi hezké druhé místo, letos nás 982 hlasů "like" naprosto bezpečně vyneslo na místo první.

studenti

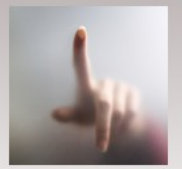
Pozvánka na přednášku zahraničního hosta prof. Dr. Chiraga C. Shetha BSc PhD

Pozvánka na přednášku zahraničního hosta prof. Dr. Chiraga C. Shetha BSc PhD, kdy: čtvrtek 27.3.2014 v 15:00 hod, Kde: děkanát LFP, téma:

1. Trends in European Disease Control and Research Skills for Health Professional

2. Candida albicans and Candida glabrata: A tale of two Candidas

Upgrade systému kiosku



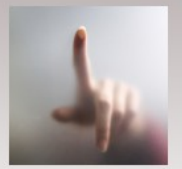
- rsync, puppet, clonezilla, tar?
- na referenčním kiosku
  - systémový filesystém sda1 přepojím na read-write
  - udělám upgrade systému
  - příkazem

    ```
    grub-reboot 1 ; reboot
    ```

    nabootuji alternativní servisní systém sda4 do shellu
  - připojím sda1, vytvořím jeho tar archiv sda1.tgz

    a pořídím jeho kontrolní součet sda1.tgz.md5sum
  - oba tyto soubory přenesu na řídící server kgate do adresáře sdíleného kioskům přes NFS

Upgrade systému kiosku

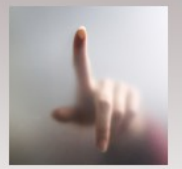


- na cílových kioscích
  - příkazem

    ```
    grub-reboot 2 ; reboot
    ```

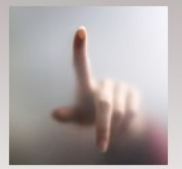
    nabootuji alternativní servisní systém sda4 do režimu upgradu, v němž se automaticky:
  - porovná nainstalovaná verze archivu sda1.tgz s verzí aktuálně dostupnou na NFS
  - při zjištění rozdílu se na lokální disk zkopíruje archiv z NFS, provede se kontrola md5sum, původní obsah sda1 je přepsán přeneseným sda1.tgz
  - a provede se reboot do upgradovaného sda1

Možnosti dalšího využití



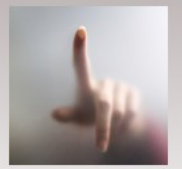
- když už jsme došli až sem...

Zkušenosti z provozu



- kiosky jsou v provozu po-pá 6:30-20:00
- bezproblémový chod
- perličky...

Moje hodnocení



- zajímavá práce
- vytvoření uceleného systému uplatněného v provozu
- veliká míra volnosti
- žádné utrpení s výběrovým řízením
- minimální nároky na administrativu
- skvělá spolupráce kolegů se zájmem o věc
- přesahy do různých směrů IT
- naučil jsem se řadu nových věcí
  - a ještě za to dostal zaplaceno ;-)
- užil jsem si to