Zákoutí implementace IdM

Svět IdM pohledem dodavatele

Není IdM jako IdM

různé produkty

různí zákazníci

různé integrace

uživatelský self-service

pokročilé funkcionality

federated identity

ČSSZ, O2 CZ, Orange SK, ISIC,

Ministerstvo zemědělství

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

IBM Security Identity Manager

DirX Identity

Organisation Manager

Licence open-source IdM

Apache License v 2.0

CDDL 1.0

MIT License

GNU Lesser ...blic License 2.1

GNU L... ...al Public License 3.0

Eclipse ...nse - v 1.0

Common Public License Version 1.0

GPLv2 with classpath exception

Všechny hlavní open-source projekty používají tento mix.

FREE SOFTWARE FOUNDATION

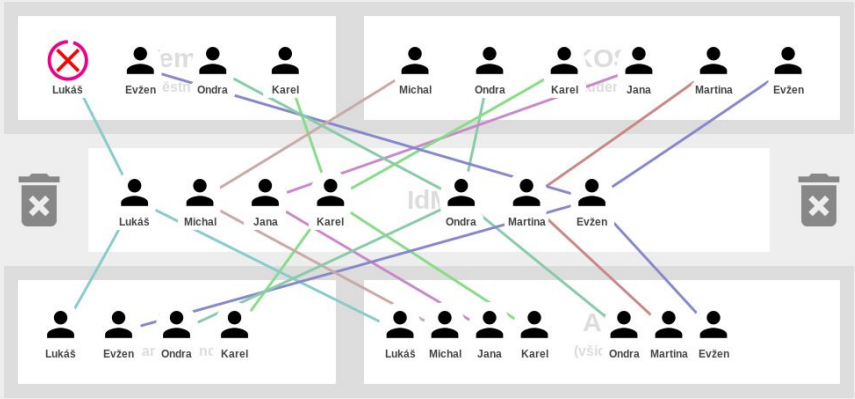
open source initiative

identitr

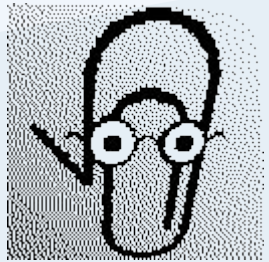
https://idm.systems/identitr/

Zahrajte si na IdM.

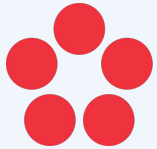
Jak dlouho zvládnete reagovat na události ve zdrojových a cílových systémech?



Správa identit má být jednoduchý problém.



Jihočeská univerzita



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

3 zdrojové systémy … 6 cílových systémů … 3 plánované systémy

70k identit, z toho 15k aktivních

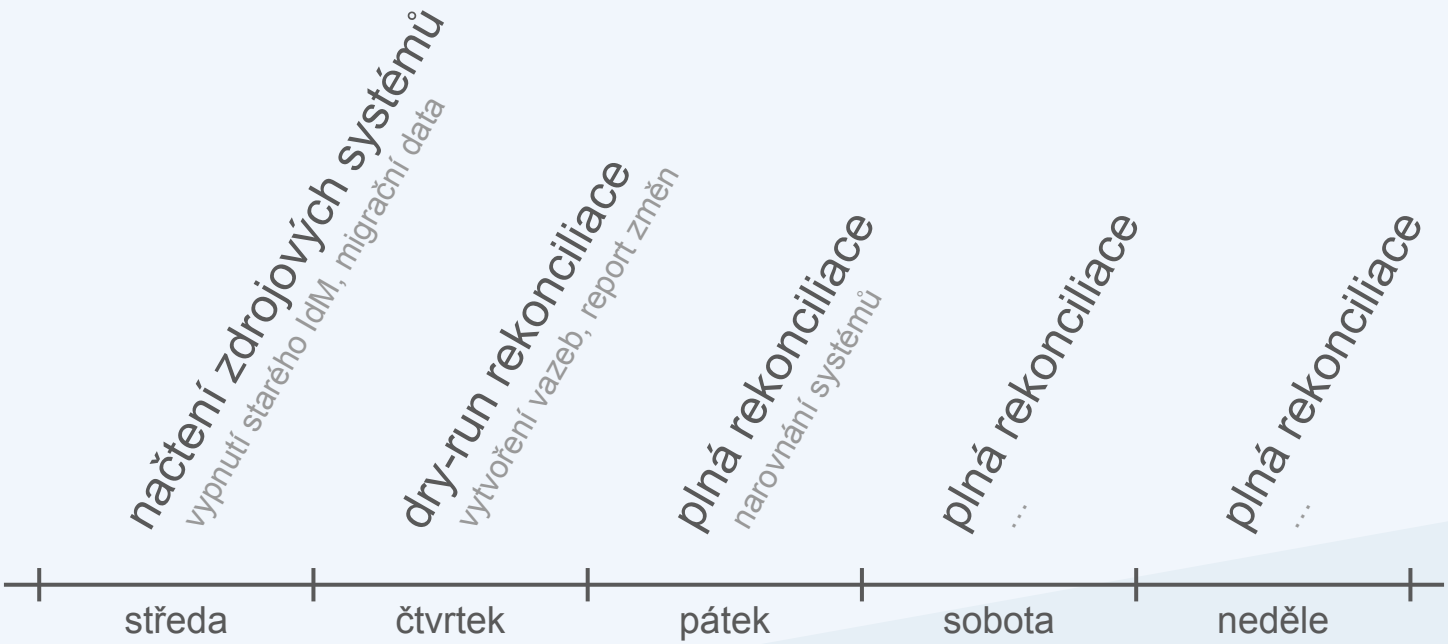
synchronizace hesel

slučování identit

osobní e-maily

Jihočeská univerzita

přechod do produkce



Jihočeská univerzita

Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

simulovaný zápis neboli dry-run

AD

14k namapovaných
33k neoprávněných
8 chybějících
150 neidentifikovaných

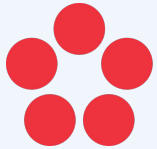
RADIUS

8k namapovaných
30 neoprávněných
3 chybějící
1 neidentifikovaný

```
...9862 [department] [ null, "M4101" ]
...9862 [company] [ null, "FZE" ]
...9862 [ldapGroups] [ [  ], [ "CN=FZEAlum,OU=IDMGroups,DC=ad,DC=jcu,DC=cz" ] ]
...b14a [mail] [ "le******@zf.jcu.cz", "le******@jcu.cz" ]
...b14a [department] [ null, "P1601" ]
...b14a [company] [ null, "FZE" ]
...b14a [mail] [ "kn******@ef.jcu.cz", "kn*****@jcu.cz" ]
...dbb5 [sn] [ "KNECHT", "Knecht" ]
...dbb5 [cn] [ "KNECHT ******", "Knecht ******" ]
...dbb5 [department] [ null, "B6208" ]
...dbb5 [company] [ null, "FEK" ]
...a2ef [userAccountControl] [ "546", "544" ]
```

Jihočeská univerzita

problémy



Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

AD – maximální délka uživatelského jména je 20 znaků

AD – sambaNTPassword je MD4 v UTF-16LE

RADIUS – single-value není tak úplně single-value

AD – speciální znaky v hesle nesmí být moc speciální

Původní IdM – diakritika v e-mailových adresách

AD – UserPasswordNotRequired

LDAP + **SQL** – referenční integrita

Univerzita J. E. Purkyně

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

4 zdrojové systémy … 4 cílové systémy

60k identit, z toho 12k aktivních

nový způsob evidence studentů

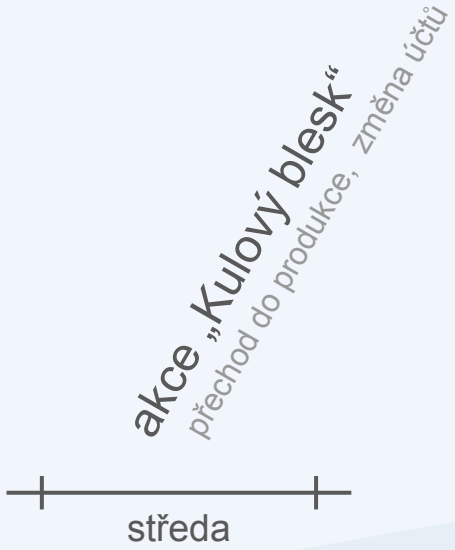
nový LDAP, nový způsob autentizace

hostovské identity, žádost o mailbox

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

Univerzita J. E. Purkyně

přechod do produkce



Univerzita J. E. Purkyně

problémy

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

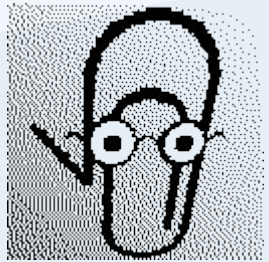
Víceméně vše vyřešeno v rámci testovacích migrací.

OpenLDAP – nestabilní při replikaci pod zatížením

UNL – chybějící objectclasses

eDirectory – datum jako INT32 (1970 ~ 2038)

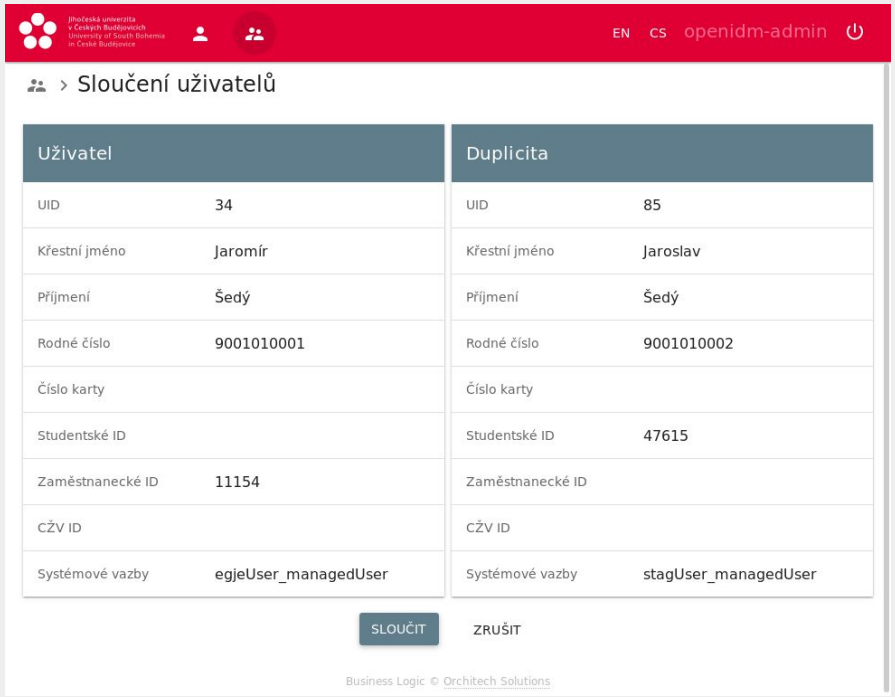
Správa identit má být jednoduchý problém.



Slučování identit I

ve zdroji jsou chyby

- zdánlivě komplexní problém
  - duplicity ve zdrojových systémech
  - duplicity mezi zdrojovými systémy
  - slučování konfliktních atributů
- jednoduchý use-case
  - dohledání duplicity a její označení
  - přenesení vazebních atributů
  - zakázaní duplikátu



Slučování identit II

zdroj fyzickou osobu neřeší

- zdrojový systém to neřeší?

  oddělený model pro zdrojové objekty

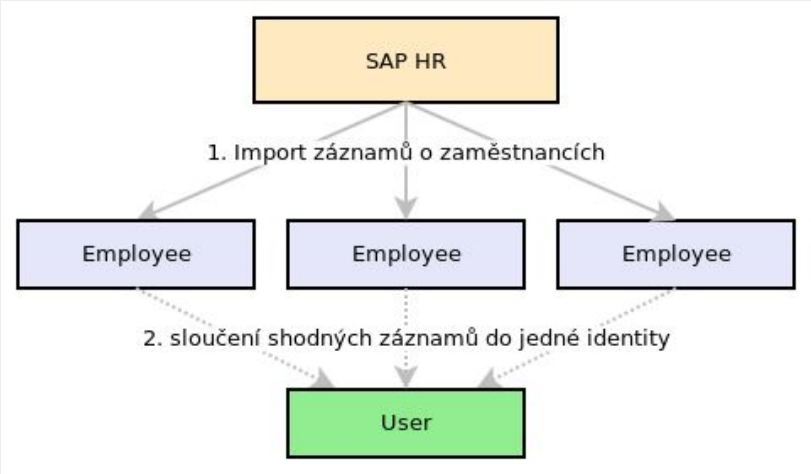
  proces párování zdrojových objektů

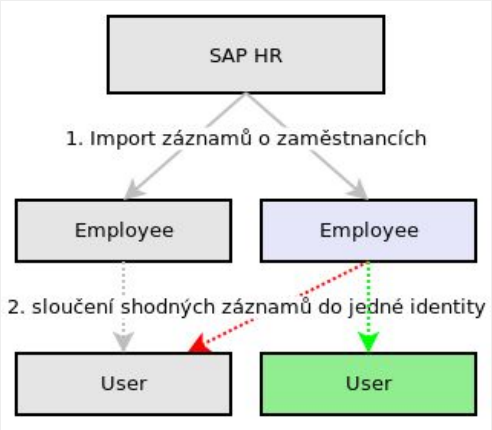
  proces mapování na identitu

- přepárování není problém

  proces nebude nikdy bezchybný

  změna vazby a zbytek plyne z IdM





Slučování identit III

slučujeme zákazníky

- správa zákazníků

  vícenásobné mapování

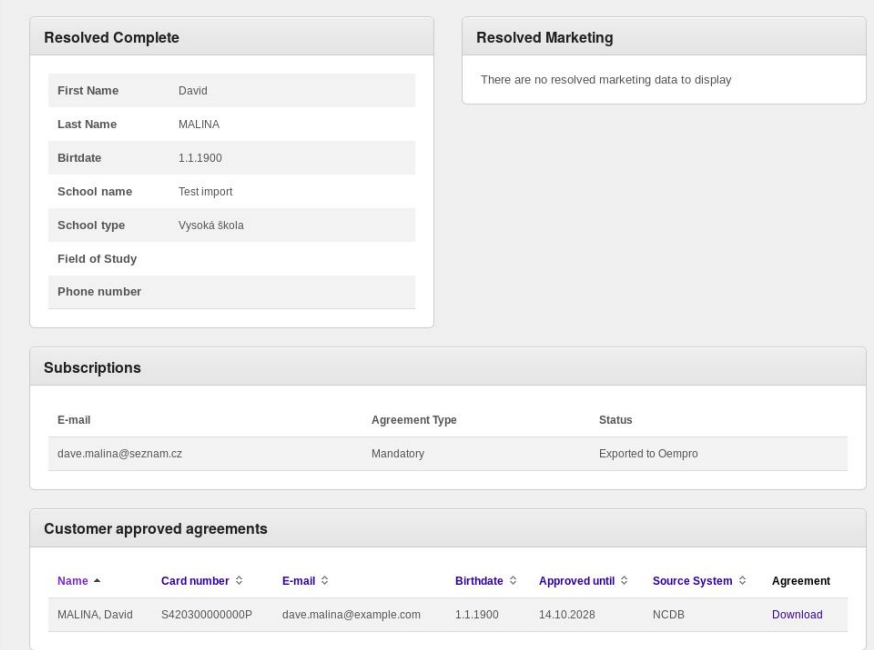
  aktualizace a zastarávání údajů

  evidence souhlasů a jejich odvolání

  marketingové využití dat

- identity provider

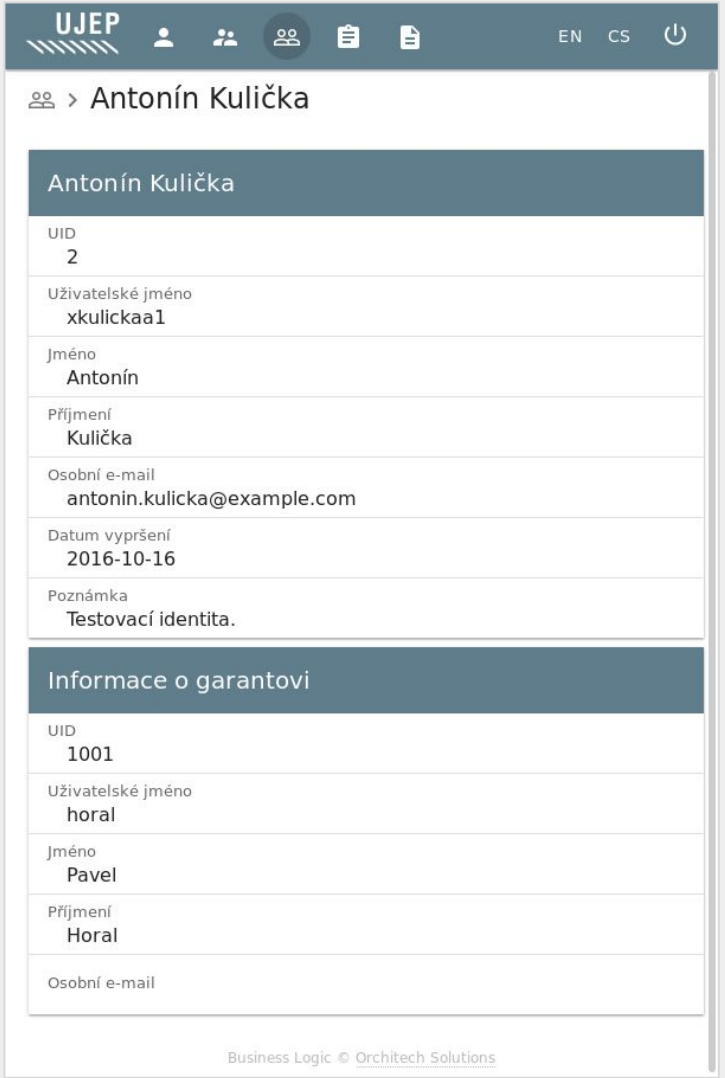
  přihlášení a namapování účtu



Hostovské identity

rychlý přístup pro hosty

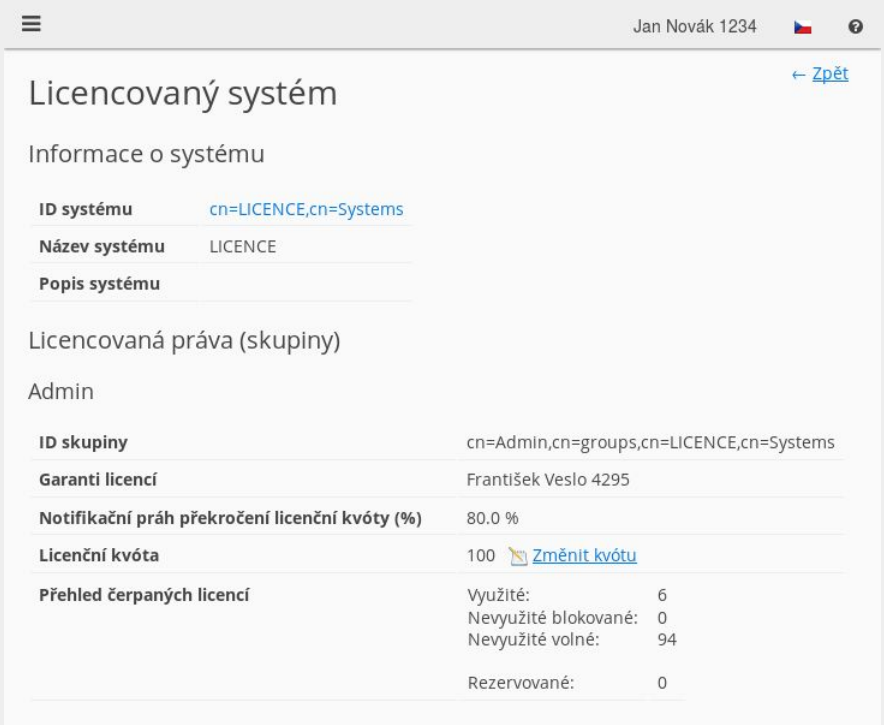
- ad-hoc identity
  - omezená platnost
  - omezená práva
- zodpovídá garant
  - proces prodloužení
  - proces převzetí



Licence

když přístupy nejsou zdarma

- omezení počtu přiřazení
  - definice licencí (účet vs. právo)
  - logika čerpání licencí
  - překročení a navázané procesy
- rezervace
  - rezervace počtu přiřazení
  - rezervace pro konkrétní účel



Další zajímavosti

všehochuť

Viditelnost a přiřaditelnost – access control naruby

Odložená synchronizace – řešení referenční integrity

Unique value cache – generujeme unikátní hodnoty

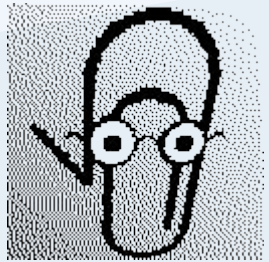
Integration profiling – kontrola počtu a délky operací

Request logging – rozšířené logování BE i FE

Nestandardní oprávnění – plnohodnotná free-text práva

Pokročilá workflow – agregace žádostí, poznámky k realizaci

Správa identit má být jednoduchý problém.



Watchdog

tady hlídám já

- jak a co kontrolovat

  počet změn objektu za danou rekonciliaci

  počet změn na objektu za daný čas (load)

- co (ne)hlídat

  inkrementální rekonciliace (LIVE SYNC)

  odvozené změny

- problémy

  kdy je UPDATE skutečně UPDATE

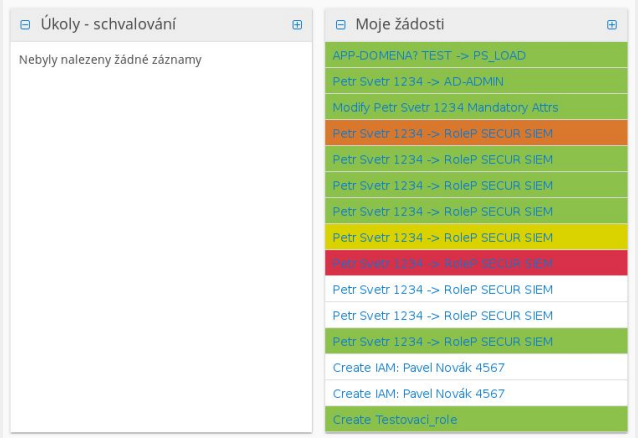
Pozorované chyby I

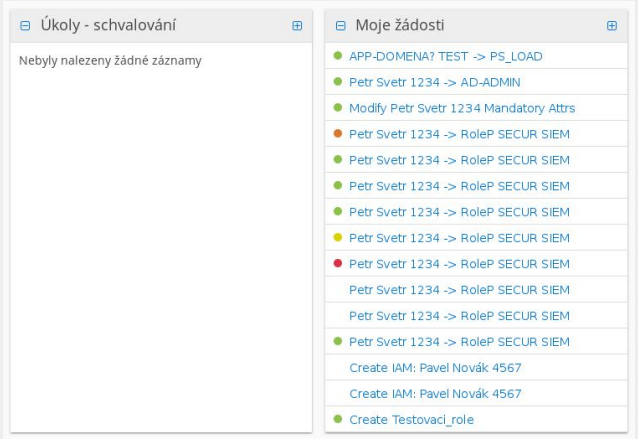
nevhodné UI požadavky

- přehnané barvičky
- nekoncepčnost
- vše na jedné obrazovce
- prohřešky proti UX

  WCAG, WAI-ARIA, …

Je nutné specifikovat konvence pro UI a neporušovat best practices.





Pozorované chyby II

projekt nepodléhá verzování

- nejasná verze projektu
  - implementace klikáním
  - ad-hoc změny
  - ruční přenos do produkce
- chyby a jejich odstraňování
  - neodstraňování starých částí
  - důvod implementační změny

Projekt by měl být v SCM a podléhat release managementu.

```
276be16 CUA mapping changes. See RM #26143.
24e53eb Next dev cycle.
64cbc96 1.0.6
be87bba Fixed incorrect version in master branch.
5e46195 LDAP contactVisible rules changed. See RM #25961.
3ae0ad0 E-mail change detection with disconnected mailboxes. See RM #25438.
c9c153e Next development cycle.
b66a9ae 1.0.4
01bbdf3 Better upgrade instructions. NOREF
a51c02b Manager can be NULL. See RM #25182
e9f94bc Notification dispatcher can handle non-existing template. NOREF
207dec0 Workaround for PostgreSQL audit record logging error. See RM #24045.
a4b29c5 Fixed MailboxSearch result size limitation. See RM #24910.
e3ac8d5 Mapping Building attr from HR export. See RM #24910.
c1a0df3 Next release cycle.
82fa206 1.0.3
fc63300 Default value for empty managers in AD. See RM #24910.
```

Pozorované chyby III

metoda pokus-omyl

- implementátor musí uklízet

  nepořádek v kódu, nekoncepčnost, chybná nebo chybějící komponentizace…

  nepochopení konceptu IdM nebo cílového systému (DN vs. ID)

  celkově velmi obtížně (::= draze a s chybami) spravovatelné řešení

Po realizaci integrace nebo funkcionality je potřeba uklidit.

```
public RoleChangesSummary getChanges(Map parameters, RoleModifications modifications) throws Exception {
    RoleChangesSummary summary = new RoleChangesSummary();
    // hashset for checked applications in added section (do not check in section of unchanged roles)
    HashSet<String> checked = new HashSet<String>();
    for (Application application : modifications.getAdded()) {
        for (MyRole role : application.getRoles()) {
            summary.addRole(role.getWorkflowName(), role.getRoleDN());
        }
        processLocalisationChanges(application, parameters, summary);
        processVipChanges(application, parameters, summary);
        checked.add(application.getApplName());
    }
    for (Application appl : modifications.getUnchanged()) {
        // check adv. settings only in applications, which has not been in added section
        if (!checked.contains(appl.getApplName())) {
            processLocalisationChanges(appl, parameters, summary);
            processVipChanges(appl, parameters, summary);
            checked.add(appl.getApplName());
        }
    }
    for (Application appl : modifications.getDeleted()) {
        for (MyRole role : appl.getRoles()) {
            summary.deleteRole(role.getWorkflowName(), role.getRoleDN());
        }
        // look if it is last role - have to delete localization and vip roles
        // only if there are not any added or unchanged roles in this appl
        if (!checked.contains(appl.getApplName())) {
            if (appl.isLocalizable() && appl.getApplLocalities() != null) {
                summary.deleteRoles(appl.getApplName(), appl.getApplLocalities());
            }
            if (appl.isVIPable() && appl.getVip().getDisplayName() == "ANO") {
                summary.deleteRole(appl.getApplName(), appl.getVip().getRoleDN());
            }
        }
    }
    return summary;
}
```

Pozorované chyby IV

kontrolujeme změnu nebo stav

- změnové vs. stavové chování

  velmi odlišný způsob implementace

  funkcionality jako reakce na události

  události spouštějící kontrolu stavu

- když událost nezpracujeme

  nekonzistentní stav

  rollback

Synchronizace by měla přenášet raději stav než změny.

Best practices

software development

- release management

  projekt, dokumentace, konfigurace
- sestavování konfigurace

  kompilace, transpilace
- zero-configuration

  okamžitý start
- unit testy

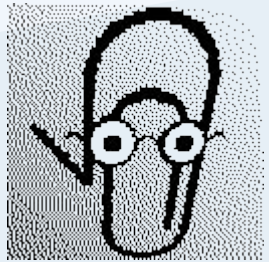
  skripty, konfigurace, UI

Continuous Integration
Continuous Delivery

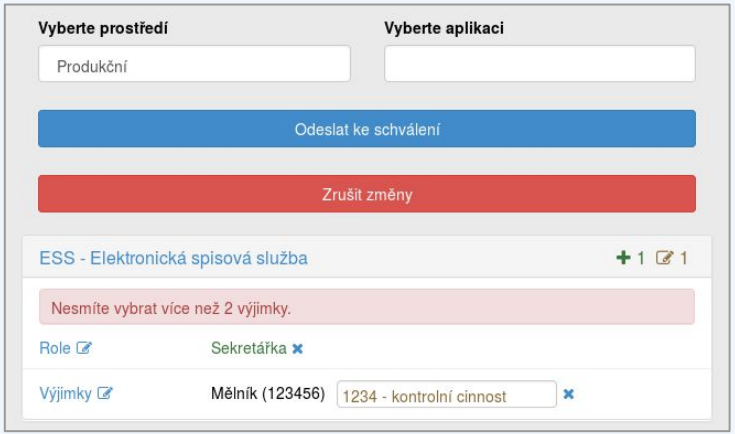
```
it("employee short", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Ab',
        surname: 'Cd',
        workforceId: 1
    })).toBe('acd');
});

it("employee long", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Karel',
        surname: 'TesterTestovitý',
        workforceId: 1
    })).toBe('ktestertestovit');
});

it("employee two names", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Hana',
        surname: 'Vorlová Görglová',
        workforceId: 1
    })).toBe('hvorlovagorglov');
});

it("student", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Petr',
        surname: 'Svetr'
    })).toBe('svetrp00');
});

it("student conflict", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Jan',
        surname: 'Novák'
    })).toBe('novakj02');
});

it("accents", function() {
    expect(generateUsername(openidmMock, {
        givenName: 'Žlababa',
        surname: 'Ňňážová'
    })).toBe('rnazoz00');
    expect(generateUsername(openidmMock, {
        givenName: 'Nikola',
        surname: 'Mojžyszková',
        workforceId: 1
    })).toBe('nmojzyszkova');
});
```

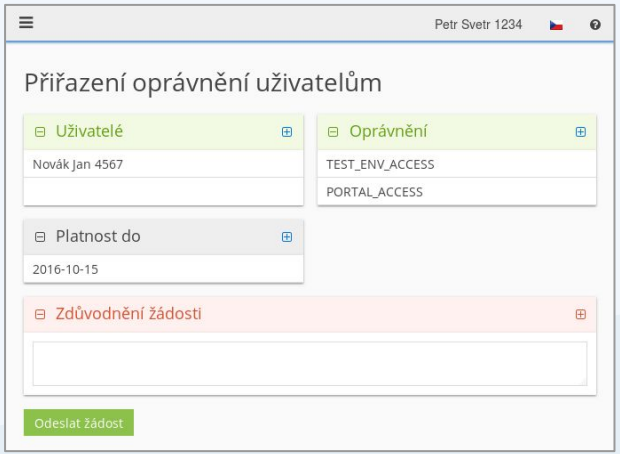
```
[14:15:26] Using gulpfile ~/Documents/repository/mze/
[14:15:26] Starting 'clean'...
[14:15:26] Finished 'clean' after 34 ms
[14:15:26] Starting 'default'...
[14:15:26] Starting 'build:vendor'...
[14:15:26] Starting 'build:conf:json'...
[14:15:26] Starting 'build:conf:other'...
[14:15:26] Starting 'build:data'...
[14:15:26] Starting 'build:doc'...
[14:15:26] Starting 'build:ui'...
[14:15:26] Starting 'build:script:js'...
[14:15:26] Starting 'build:script:other'...
[14:15:26] Finished 'default' after 56 ms
[14:15:26] Finished 'build:doc' after 43 ms
[14:15:26] Finished 'build:vendor' after 170 ms
[14:15:26] Starting 'test'...
[14:15:26] Finished 'build:ui' after 195 ms
[14:15:26] Finished 'build:conf:other' after 212 ms
.....................................

36 specs, 0 failures
Finished in 0 seconds
[14:15:26] Finished 'test' after 202 ms
[14:15:26] Finished 'build:data' after 354 ms
[14:15:26] Finished 'build:script:other' after 480 ms
[14:15:26] Finished 'build:script:js' after 533 ms
[14:15:26] Starting 'build:script'...
[14:15:26] Finished 'build:script' after 2.95 µs
[14:15:26] Finished 'build:conf:json' after 553 ms
[14:15:26] Starting 'build:conf'...
[14:15:26] Finished 'build:conf' after 1.99 µs
[14:15:26] Starting 'build'...
[14:15:26] Finished 'build' after 1.76 µs
[14:15:26] Starting 'default:build'...
[14:15:26] Finished 'default:build' after 1.68 µs
```

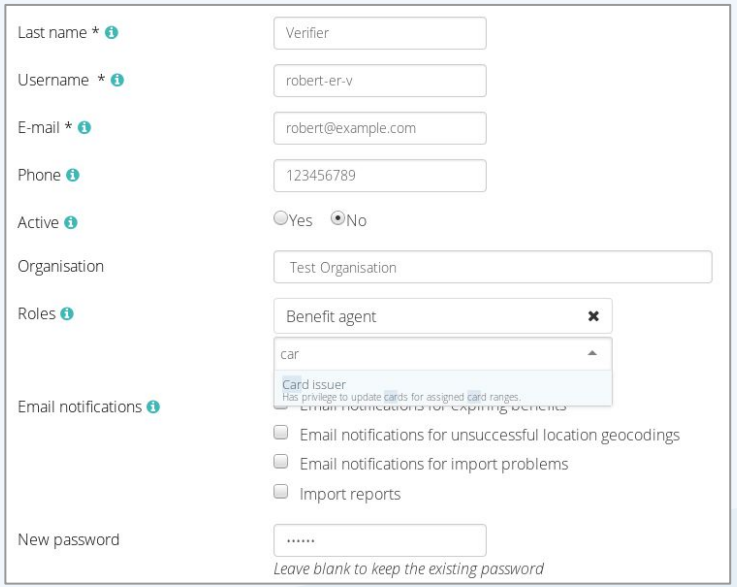
Správa identit má být jednoduchý problém.



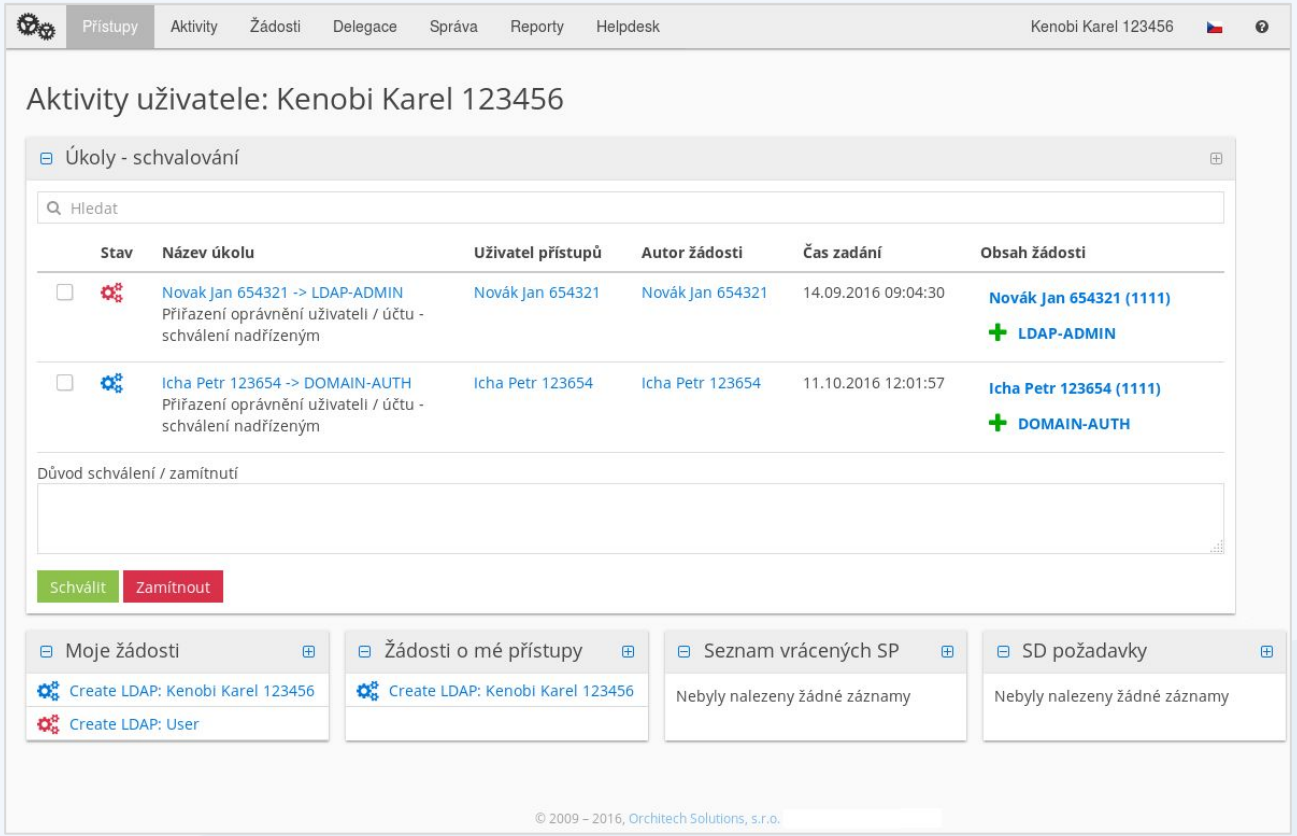
Správný návrh UI



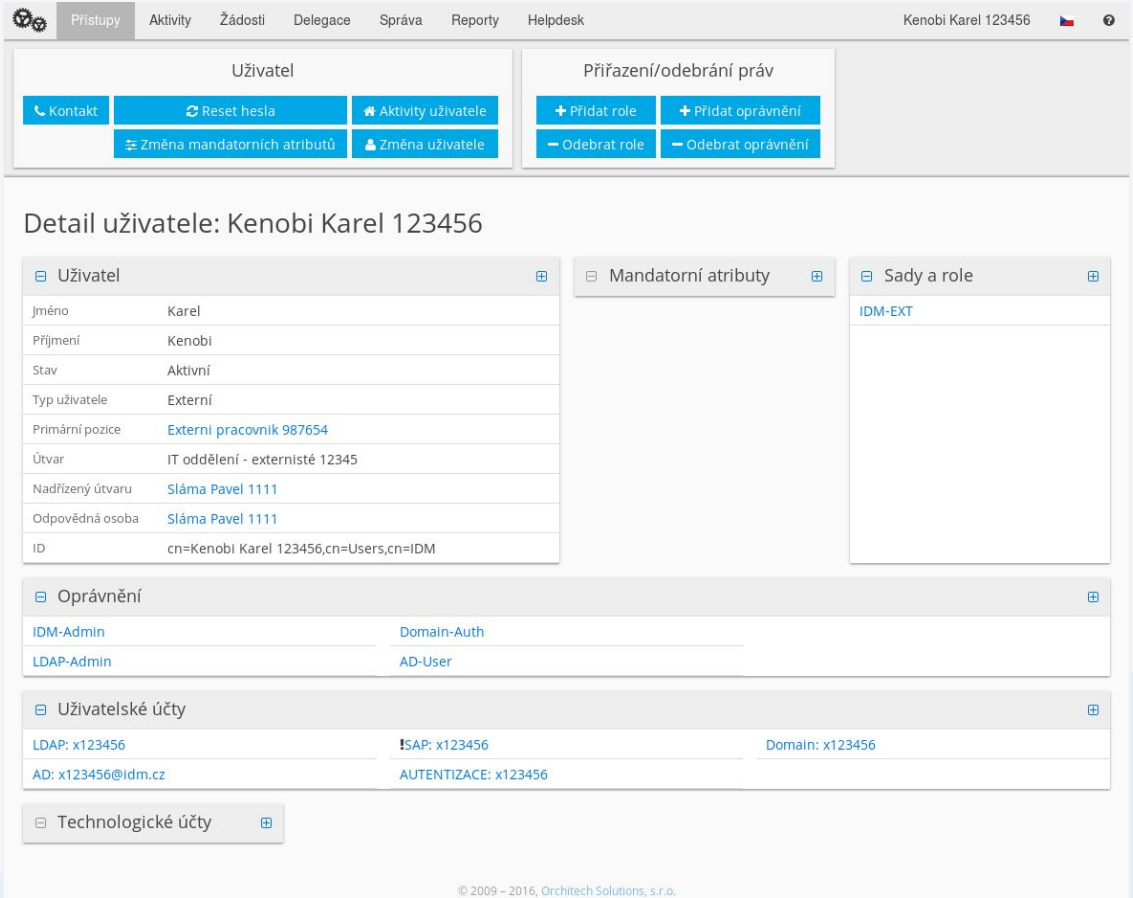




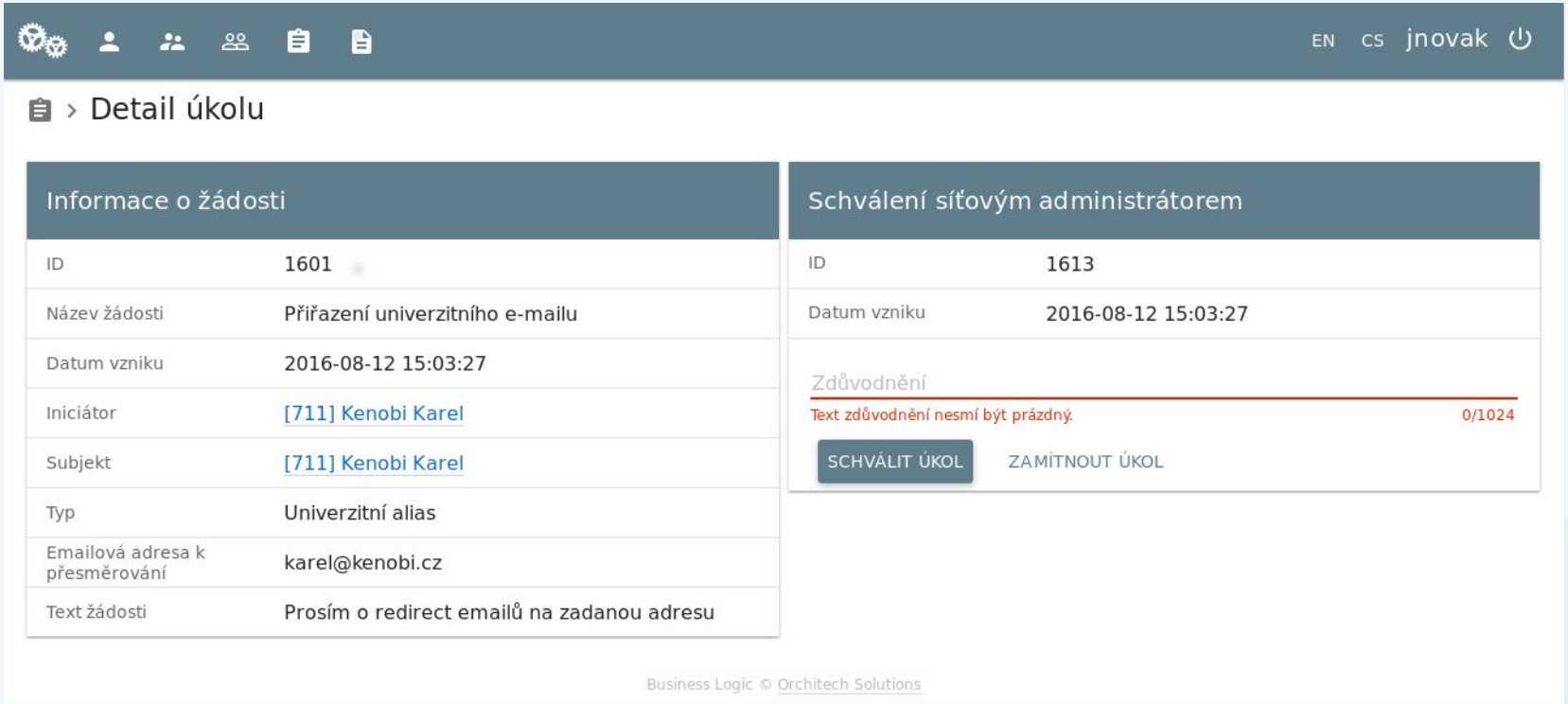
Několik ukázek UI



Několik ukázek UI



Několik ukázek UI



Děkujeme za pozornost.