stepping stone

Mit GitLab, Puppet und MediaWiki zu ISO/IEC 27001

Niklaus Hofer
Information Security

4. September 2020

Übersicht

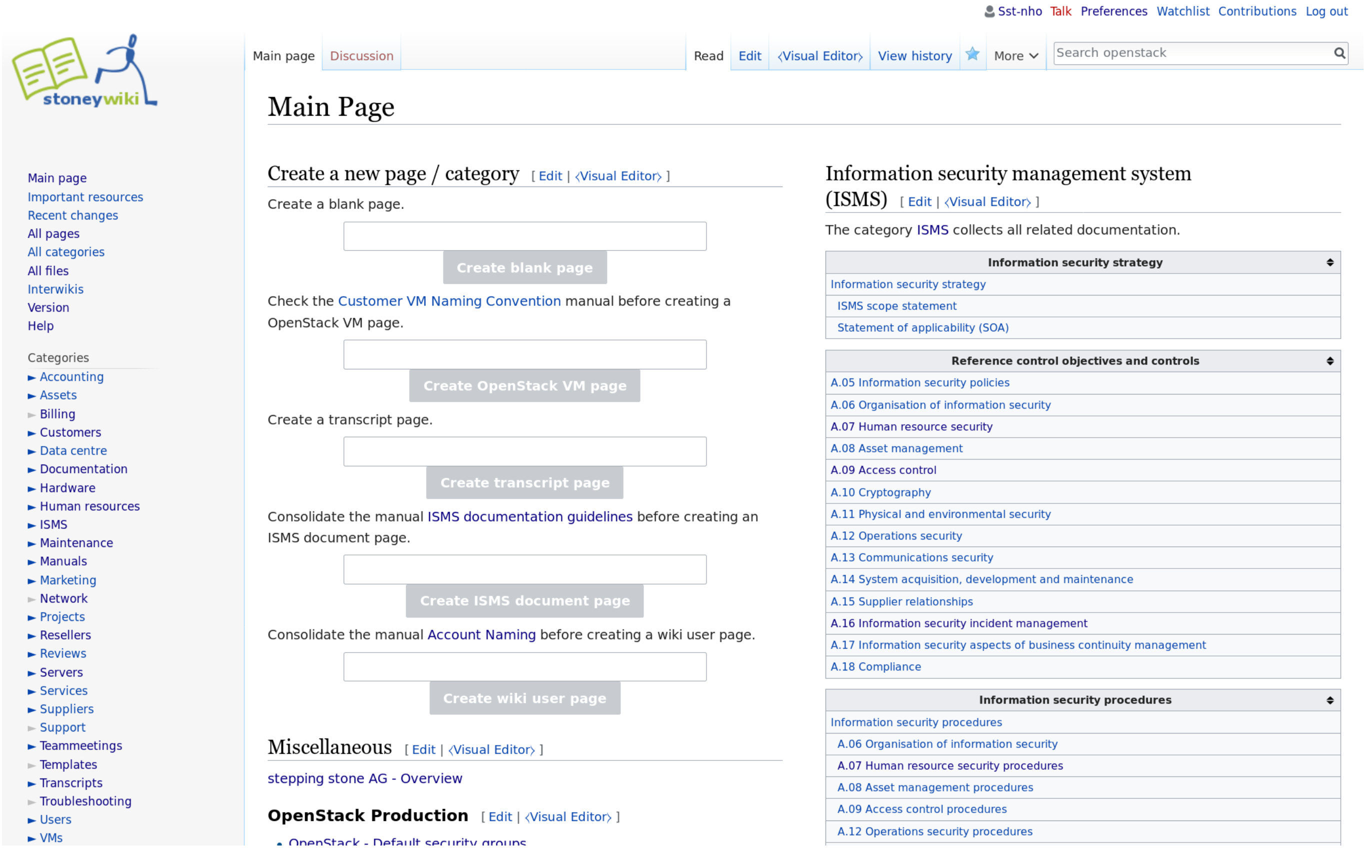
- ISO 27001 und die stepping stone AG
  - Mediawiki
- Umsetzungsbeispiel
  - Gitlab und Puppet
- Welchen Nutzen ziehen wir daraus?

ISO 27001 und die stepping stone AG

Ziele und Vorgaben

- Ziele (Control-objectives)
  - Im Standard vorgegeben
  - Anforderungen an Prozesse
- Vorgaben (Policies)
  - Implementieren die Ziele
  - Werden durch die stepping stone AG geschrieben

Ziele und Vorgaben



Main Page

Main page
Important resources
Recent changes
All pages
All categories
All files
Interwikis
Version
Help

Categories

- ► Accounting
- ► Assets
- ► Billing
- ► Customers
- ► Data centre
- ► Documentation
- ► Hardware
- ► Human resources
- ► ISMS
- ► Maintenance
- ► Manuals
- ► Marketing
- ► Network
- ► Projects
- ► Resellers
- ► Reviews
- ► Servers
- ► Services
- ► Suppliers
- ► Support
- ► Teammeetings
- ► Templates
- ► Transcripts
- ► Troubleshooting
- ► Users
- ► VMs

Create a new page / category [Edit | ‹Visual Editor›]

Create a blank page.

Create blank page

Check the Customer VM Naming Convention manual before creating a OpenStack VM page.

Create OpenStack VM page

Create a transcript page.

Create transcript page

Consolidate the manual ISMS documentation guidelines before creating an ISMS document page.

Create ISMS document page

Consolidate the manual Account Naming before creating a wiki user page.

Create wiki user page

Miscellaneous [Edit | ‹Visual Editor›]

stepping stone AG - Overview

OpenStack Production [Edit | ‹Visual Editor›]

- OpenStack - Default security groups

Information security management system (ISMS) [Edit | ‹Visual Editor›]

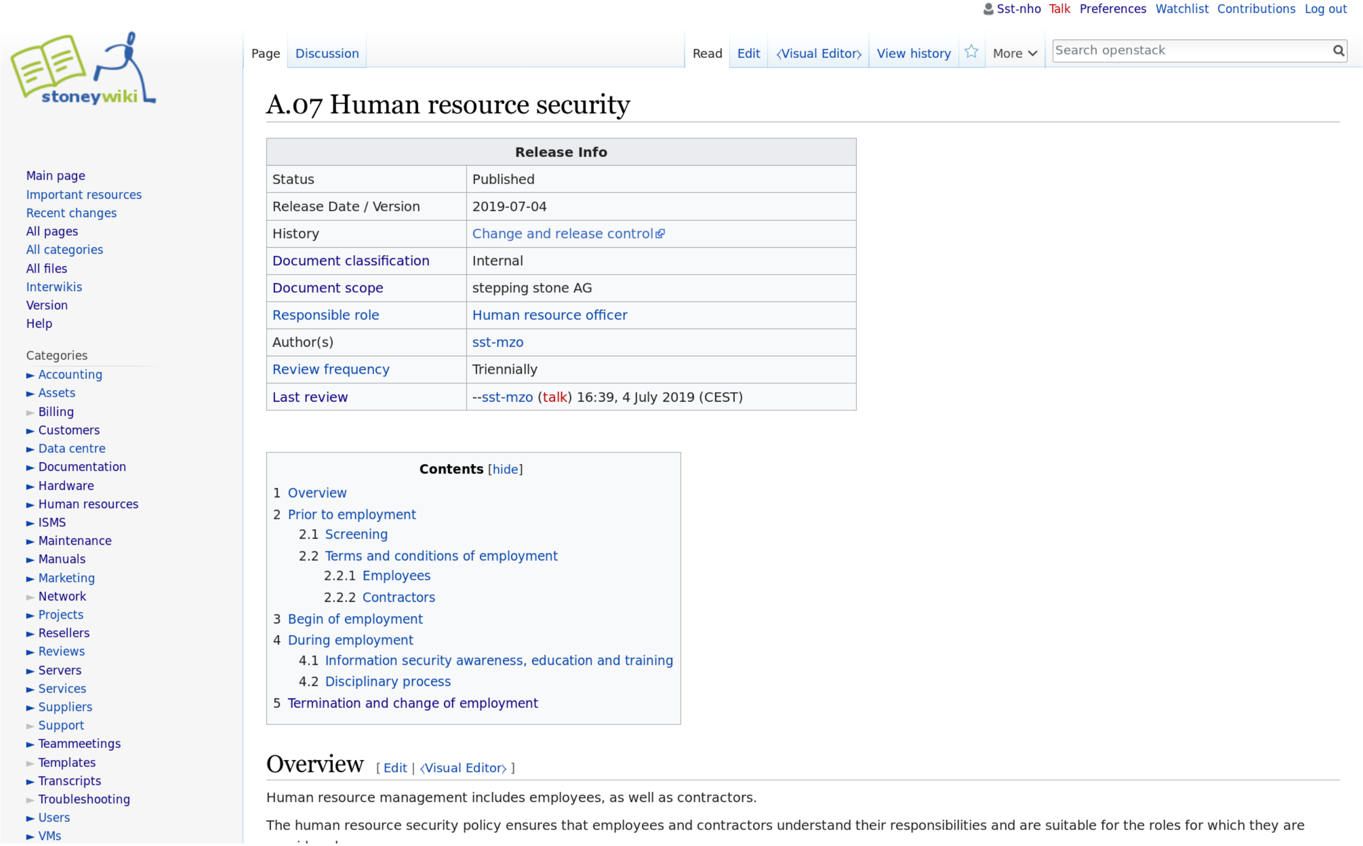
The category ISMS collects all related documentation.

Information security strategy
Information security strategy
ISMS scope statement
Statement of applicability (SOA)

Reference control objectives and controls
A.05 Information security policies
A.06 Organisation of information security
A.07 Human resource security
A.08 Asset management
A.09 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

Information security procedures
Information security procedures
A.06 Organisation of information security
A.07 Human resource security procedures
A.08 Asset management procedures
A.09 Access control procedures
A.12 Operations security procedures

HR Sicherheitsvorgaben



A.07 Human resource security

Release Info	
Status	Published
Release Date / Version	2019-07-04
History	Change and release control
Document classification	Internal
Document scope	stepping stone AG
Responsible role	Human resource officer
Author(s)	sst-mzo
Review frequency	Triennially
Last review	--sst-mzo (talk) 16:39, 4 July 2019 (CEST)

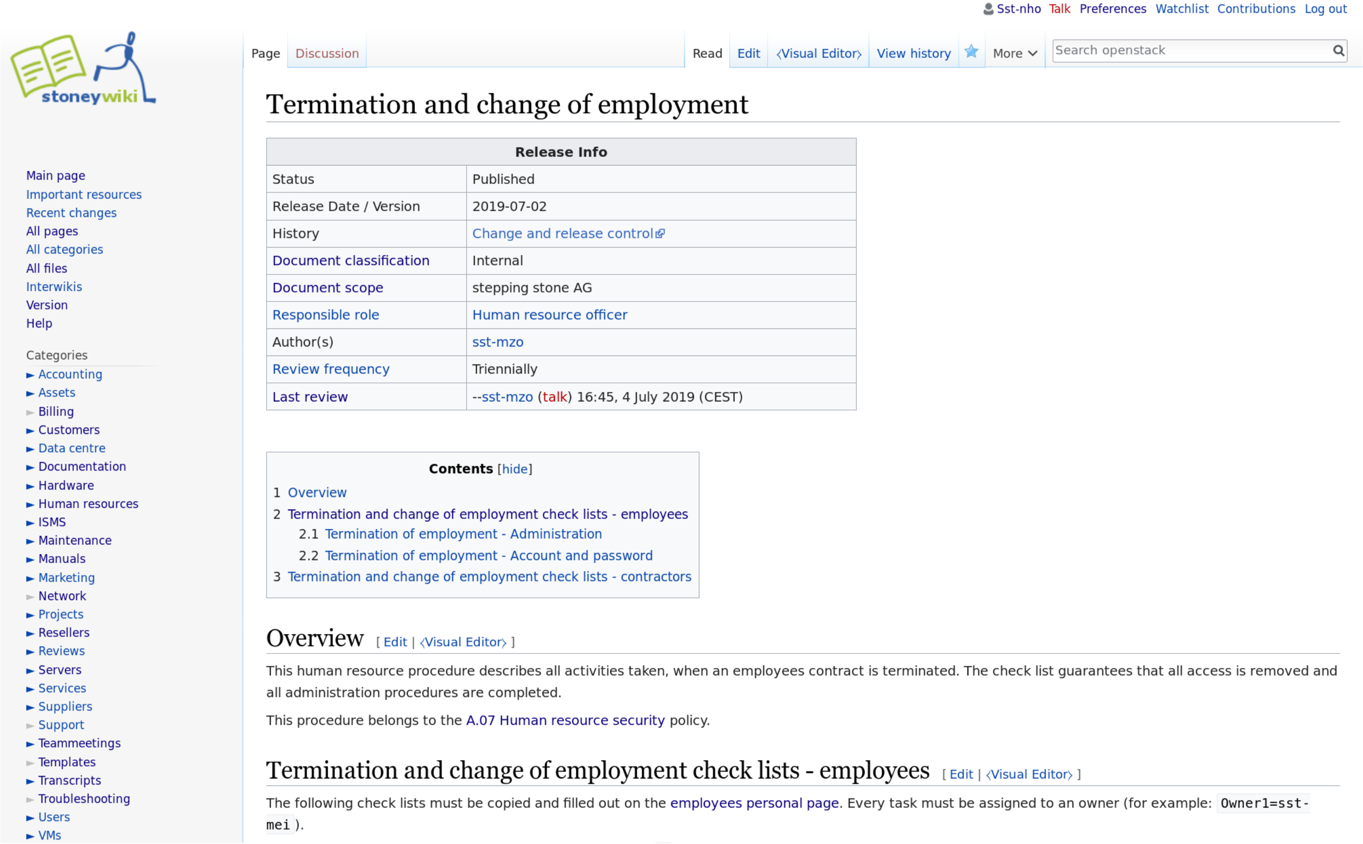
Contents [hide]

Overview [Edit | ‹Visual Editor›]

Human resource management includes employees, as well as contractors.

The human resource security policy ensures that employees and contractors understand their responsibilities and are suitable for the roles for which they are

Prozeduren



Sst-nho Talk Preferences Watchlist Contributions Log out

Page Discussion Read Edit ‹Visual Editor› View history More Search openstack

Main page
Important resources
Recent changes
All pages
All categories
All files
Interwikis
Version
Help

Categories
► Accounting
► Assets
► Billing
► Customers
► Data centre
► Documentation
► Hardware
► Human resources
► ISMS
► Maintenance
► Manuals
► Marketing
► Network
► Projects
► Resellers
► Reviews
► Servers
► Services
► Suppliers
► Support
► Teammeetings
► Templates
► Transcripts
► Troubleshooting
► Users
► VMs

Termination and change of employment

Release Info	
Status	Published
Release Date / Version	2019-07-02
History	Change and release control
Document classification	Internal
Document scope	stepping stone AG
Responsible role	Human resource officer
Author(s)	sst-mzo
Review frequency	Triennially
Last review	--sst-mzo (talk) 16:45, 4 July 2019 (CEST)

Contents [hide]

Overview [Edit | ‹Visual Editor›]

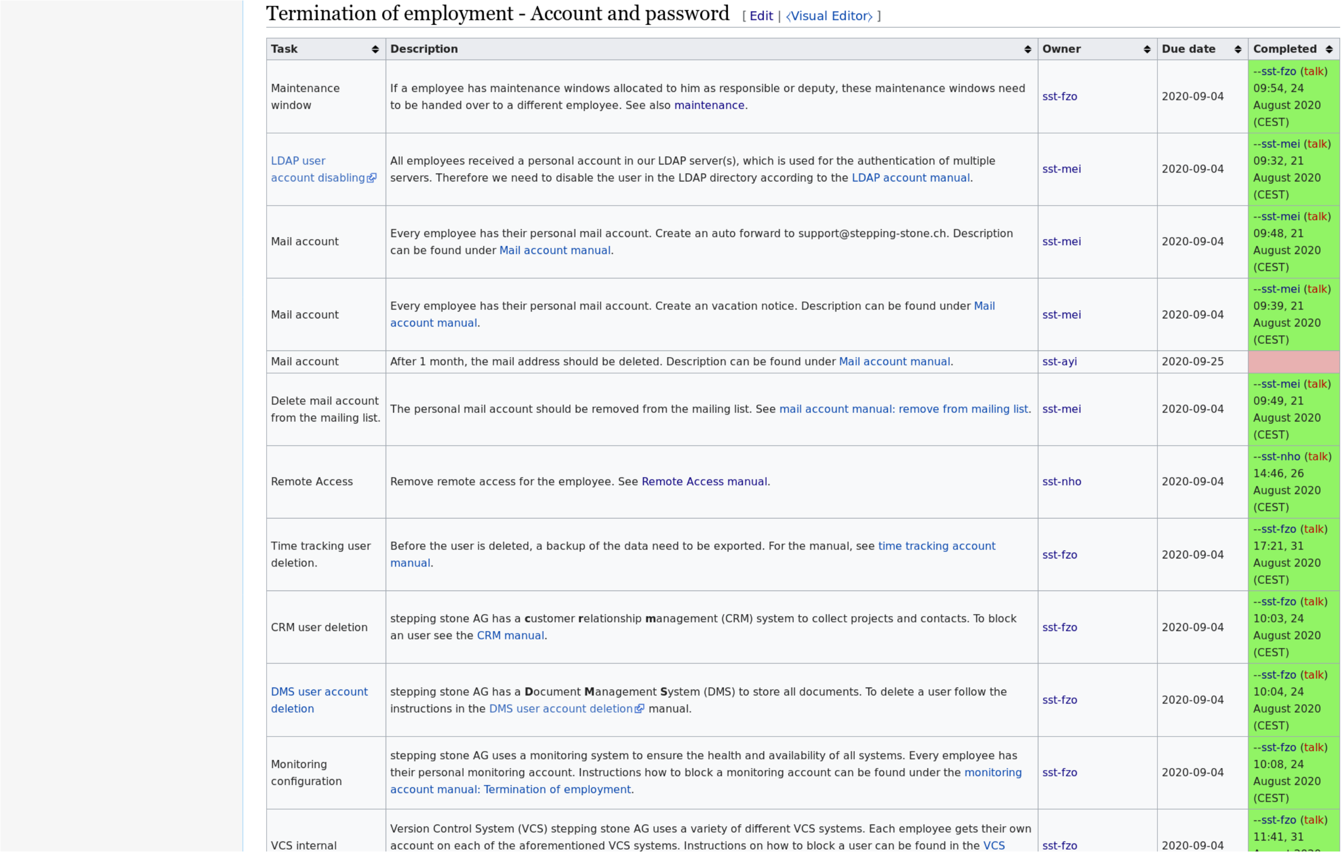
This human resource procedure describes all activities taken, when an employees contract is terminated. The check list guarantees that all access is removed and all administration procedures are completed.

This procedure belongs to the A.07 Human resource security policy.

Termination and change of employment check lists - employees [Edit | ‹Visual Editor›]

The following check lists must be copied and filled out on the employees personal page. Every task must be assigned to an owner (for example: `Owner1=sst-mei`).

Konkretes Beispiel



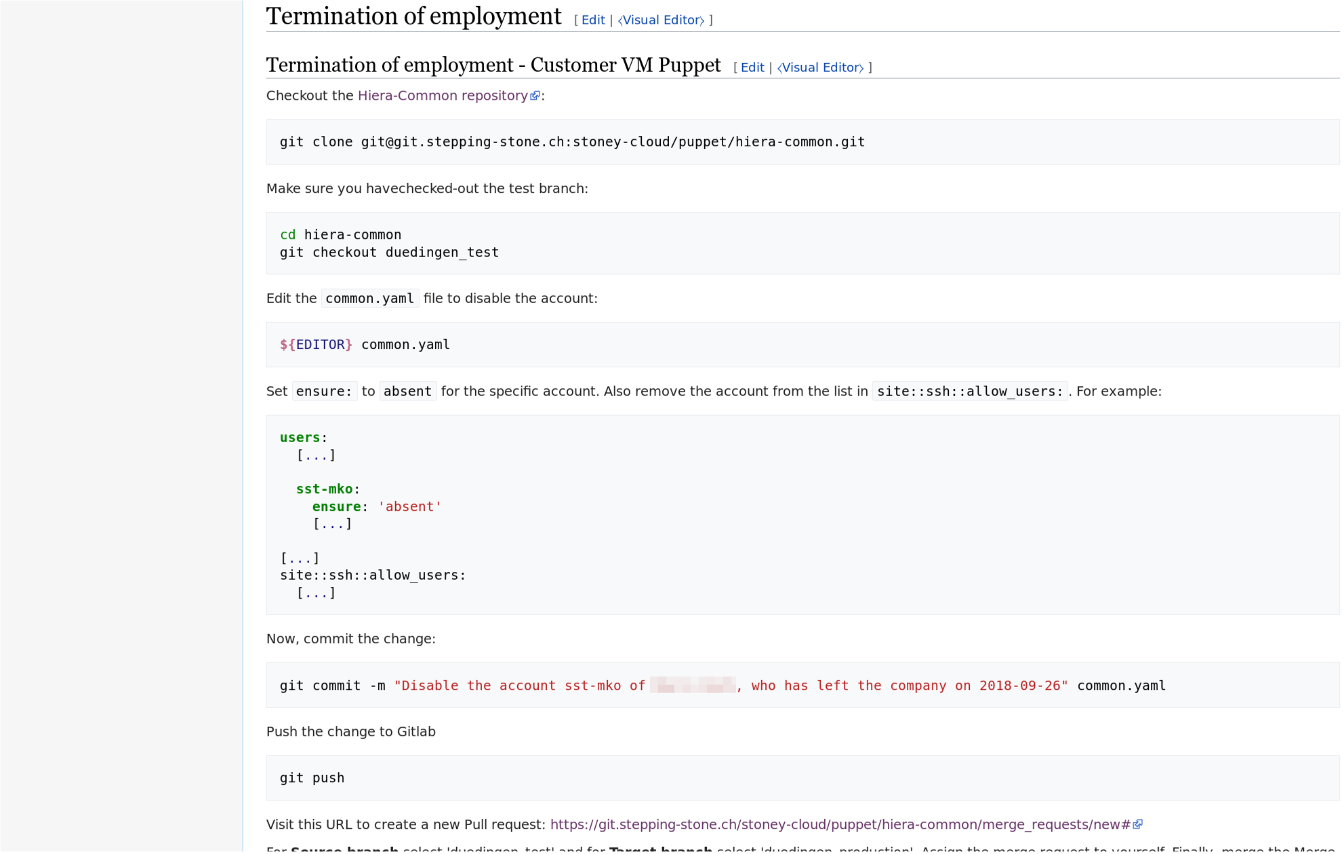
Termination of employment - Account and password

Task	Description	Owner	Due date	Completed
Maintenance window	If a employee has maintenance windows allocated to him as responsible or deputy, these maintenance windows need to be handed over to a different employee. See also maintenance.	sst-fzo	2020-09-04	--sst-fzo (talk) 09:54, 24 August 2020 (CEST)
LDAP user account disabling	All employees received a personal account in our LDAP server(s), which is used for the authentication of multiple servers. Therefore we need to disable the user in the LDAP directory according to the LDAP account manual.	sst-mei	2020-09-04	--sst-mei (talk) 09:32, 21 August 2020 (CEST)
Mail account	Every employee has their personal mail account. Create an auto forward to support@stepping-stone.ch. Description can be found under Mail account manual.	sst-mei	2020-09-04	--sst-mei (talk) 09:48, 21 August 2020 (CEST)
Mail account	Every employee has their personal mail account. Create an vacation notice. Description can be found under Mail account manual.	sst-mei	2020-09-04	--sst-mei (talk) 09:39, 21 August 2020 (CEST)
Mail account	After 1 month, the mail address should be deleted. Description can be found under Mail account manual.	sst-ayi	2020-09-25	
Delete mail account from the mailing list.	The personal mail account should be removed from the mailing list. See mail account manual: remove from mailing list.	sst-mei	2020-09-04	--sst-mei (talk) 09:49, 21 August 2020 (CEST)
Remote Access	Remove remote access for the employee. See Remote Access manual.	sst-nho	2020-09-04	--sst-nho (talk) 14:46, 26 August 2020 (CEST)
Time tracking user deletion.	Before the user is deleted, a backup of the data need to be exported. For the manual, see time tracking account manual.	sst-fzo	2020-09-04	--sst-fzo (talk) 17:21, 31 August 2020 (CEST)
CRM user deletion	stepping stone AG has a **c**ustomer **r**elationship **m**anagement (CRM) system to collect projects and contacts. To block an user see the CRM manual.	sst-fzo	2020-09-04	--sst-fzo (talk) 10:03, 24 August 2020 (CEST)
DMS user account deletion	stepping stone AG has a **D**ocument **M**anagement **S**ystem (DMS) to store all documents. To delete a user follow the instructions in the DMS user account deletion manual.	sst-fzo	2020-09-04	--sst-fzo (talk) 10:04, 24 August 2020 (CEST)
Monitoring configuration	stepping stone AG uses a monitoring system to ensure the health and availability of all systems. Every employee has their personal monitoring account. Instructions how to block a monitoring account can be found under the monitoring account manual: Termination of employment.	sst-fzo	2020-09-04	--sst-fzo (talk) 10:08, 24 August 2020 (CEST)
VCS internal	Version Control System (VCS) stepping stone AG uses a variety of different VCS systems. Each employee gets their own account on each of the aforementioned VCS systems. Instructions on how to block a user can be found in the VCS	sst-fzo	2020-09-04	--sst-fzo (talk) 11:41, 31

Handbücher

- Prozeduren verweisen auf Handbücher
  - Schritt-für-Schritt Anleitungen
    - Anlegen von Mail Accounts
    - VMs erstellen
    - Neue Hardware installieren

Handbücher



Termination of employment [Edit | ‹Visual Editor›]

Termination of employment - Customer VM Puppet [Edit | ‹Visual Editor›]

Checkout the Hiera-Common repository:

```
git clone git@git.stepping-stone.ch:stoney-cloud/puppet/hiera-common.git
```

Make sure you havechecked-out the test branch:

```
cd hiera-common
git checkout duedingen_test
```

Edit the `common.yaml` file to disable the account:

```
${EDITOR} common.yaml
```

Set `ensure:` to `absent` for the specific account. Also remove the account from the list in `site::ssh::allow_users:`. For example:

```
users:
  [...]

  sst-mko:
    ensure: 'absent'
    [...]

[...]
site::ssh::allow_users:
  [...]
```

Now, commit the change:

```
git commit -m "Disable the account sst-mko of [redacted], who has left the company on 2018-09-26" common.yaml
```

Push the change to Gitlab

```
git push
```

Visit this URL to create a new Pull request: https://git.stepping-stone.ch/stoney-cloud/puppet/hiera-common/merge_requests/new#

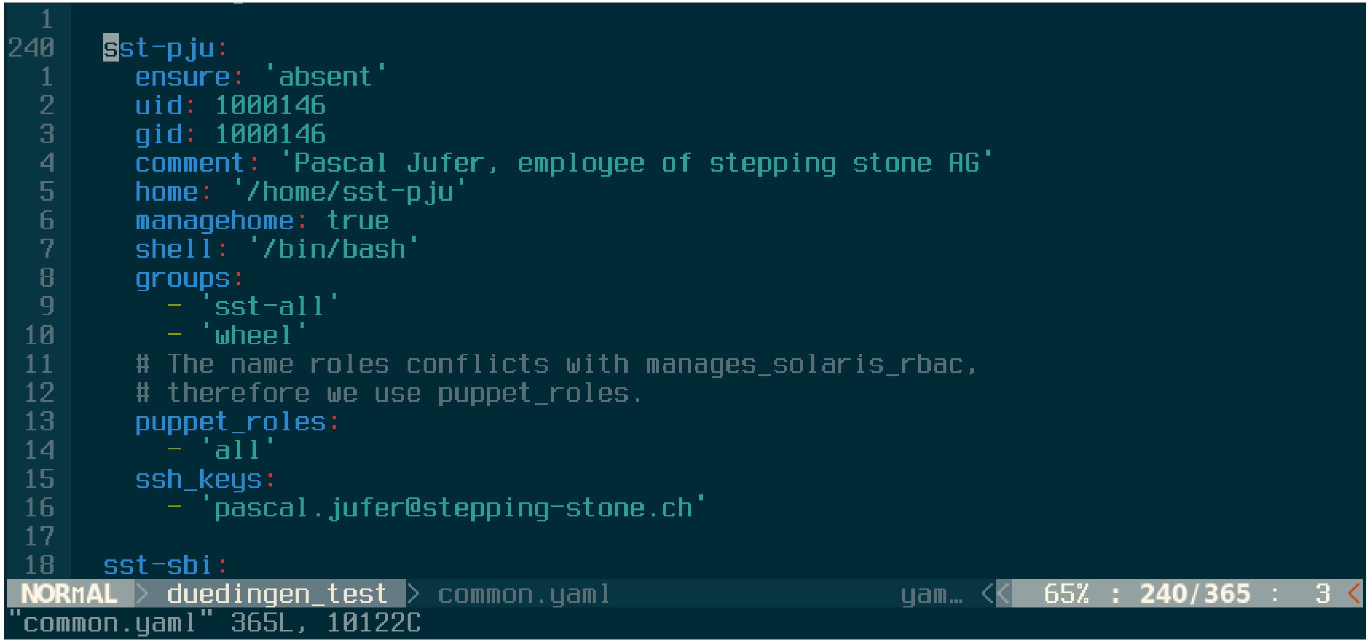
For **Source branch** select 'duedingen_test' and for **Target branch** select 'duedingen_production'. Assign the merge request to yourself. Finally, merge the Merge

Umsetzungsbeispiel

Hiera (Puppet Datenhaltung)

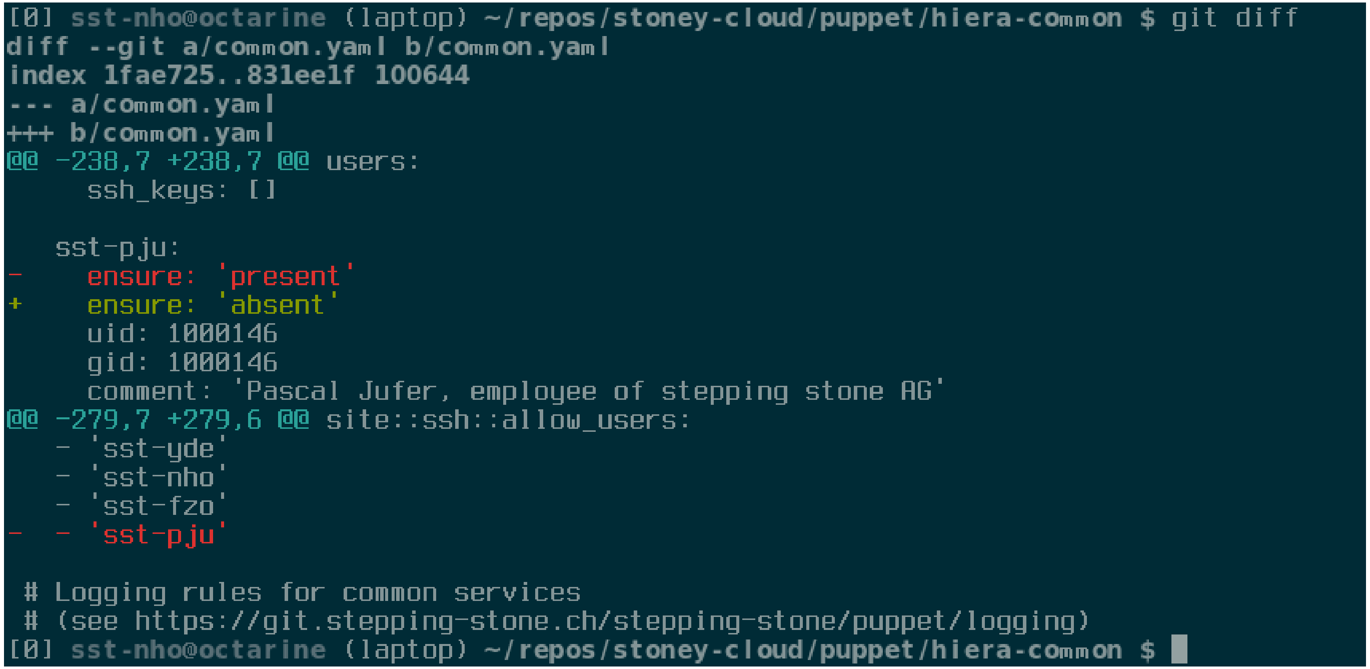
- Hierarchische Konfigurationen
  - Provider
  - Reseller
  - Customer
  - ...
  - Node

Nutzeraccount



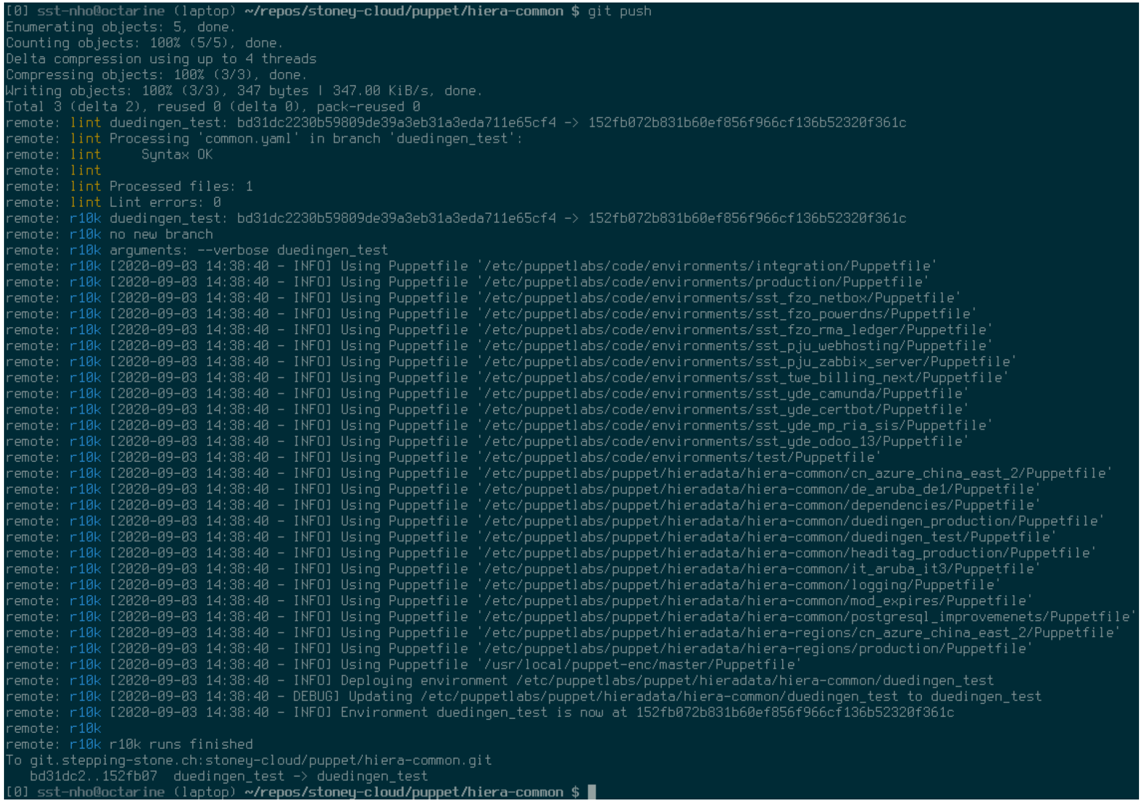
```
sst-pju:
  ensure: 'absent'
  uid: 1000146
  gid: 1000146
  comment: 'Pascal Jufer, employee of stepping stone AG'
  home: '/home/sst-pju'
  managehome: true
  shell: '/bin/bash'
  groups:
    - 'sst-all'
    - 'wheel'
  # The name roles conflicts with manages_solaris_rbac,
  # therefore we use puppet_roles.
  puppet_roles:
    - 'all'
  ssh_keys:
    - 'pascal.jufer@stepping-stone.ch'

sst-sbi:
NORMAL > duedingen_test > common.yaml                    yam… << 65% : 240/365 :  3 <
"common.yaml" 365L, 10122C
```

Nutzeraccount



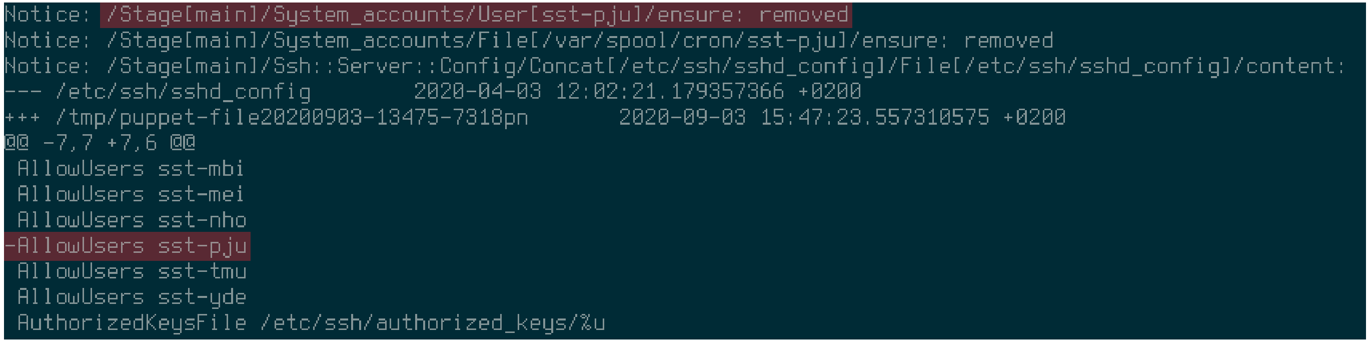
```
[0] sst-nho@octarine (laptop) ~/repos/stoney-cloud/puppet/hiera-common $ git diff
diff --git a/common.yaml b/common.yaml
index 1fae725..831ee1f 100644
--- a/common.yaml
+++ b/common.yaml
@@ -238,7 +238,7 @@ users:
     ssh_keys: []

   sst-pju:
-    ensure: 'present'
+    ensure: 'absent'
     uid: 1000146
     gid: 1000146
     comment: 'Pascal Jufer, employee of stepping stone AG'
@@ -279,7 +279,6 @@ site::ssh::allow_users:
   - 'sst-yde'
   - 'sst-nho'
   - 'sst-fzo'
-  - 'sst-pju'

 # Logging rules for common services
 # (see https://git.stepping-stone.ch/stepping-stone/puppet/logging)
[0] sst-nho@octarine (laptop) ~/repos/stoney-cloud/puppet/hiera-common $
```

Git push



```
[0] sst-nho@octarine (laptop) ~/repos/stoney-cloud/puppet/hiera-common $ git push
Enumerating objects: 5, done.
Counting objects: 100% (5/5), done.
Delta compression using up to 4 threads
Compressing objects: 100% (3/3), done.
Writing objects: 100% (3/3), 347 bytes | 347.00 KiB/s, done.
Total 3 (delta 2), reused 0 (delta 0), pack-reused 0
remote: lint duedingen_test: bd31dc2230b59809de39a3eb31a3eda711e65cf4 -> 152fb072b831b60ef856f966cf136b52320f361c
remote: lint Processing 'common.yaml' in branch 'duedingen_test':
remote: lint     Syntax OK
remote: lint
remote: lint Processed files: 1
remote: lint Lint errors: 0
remote: r10k duedingen_test: bd31dc2230b59809de39a3eb31a3eda711e65cf4 -> 152fb072b831b60ef856f966cf136b52320f361c
remote: r10k no new branch
remote: r10k arguments: --verbose duedingen_test
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/integration/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/production/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_fzo_netbox/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_fzo_powerdns/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_fzo_rma_ledger/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_pju_webhosting/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_pju_zabbix_server/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_twe_billing_next/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_yde_camunda/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_yde_certbot/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_yde_mp_ria_sis/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/sst_yde_odoo_13/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/code/environments/test/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/cn_azure_china_east_2/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/de_aruba_de1/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/dependencies/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/duedingen_production/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/duedingen_test/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/headitag_production/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/it_aruba_it3/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/logging/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/mod_expires/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-common/postgresql_improvemenets/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-regions/cn_azure_china_east_2/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/etc/puppetlabs/puppet/hieradata/hiera-regions/production/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Using Puppetfile '/usr/local/puppet-enc/master/Puppetfile'
remote: r10k [2020-09-03 14:38:40 - INFO] Deploying environment /etc/puppetlabs/puppet/hieradata/hiera-common/duedingen_test
remote: r10k [2020-09-03 14:38:40 - DEBUG] Updating /etc/puppetlabs/puppet/hieradata/hiera-common/duedingen_test to duedingen_test
remote: r10k [2020-09-03 14:38:40 - INFO] Environment duedingen_test is now at 152fb072b831b60ef856f966cf136b52320f361c
remote: r10k
remote: r10k r10k runs finished
To git.stepping-stone.ch:stoney-cloud/puppet/hiera-common.git
   bd31dc2..152fb07  duedingen_test -> duedingen_test
[0] sst-nho@octarine (laptop) ~/repos/stoney-cloud/puppet/hiera-common $
```

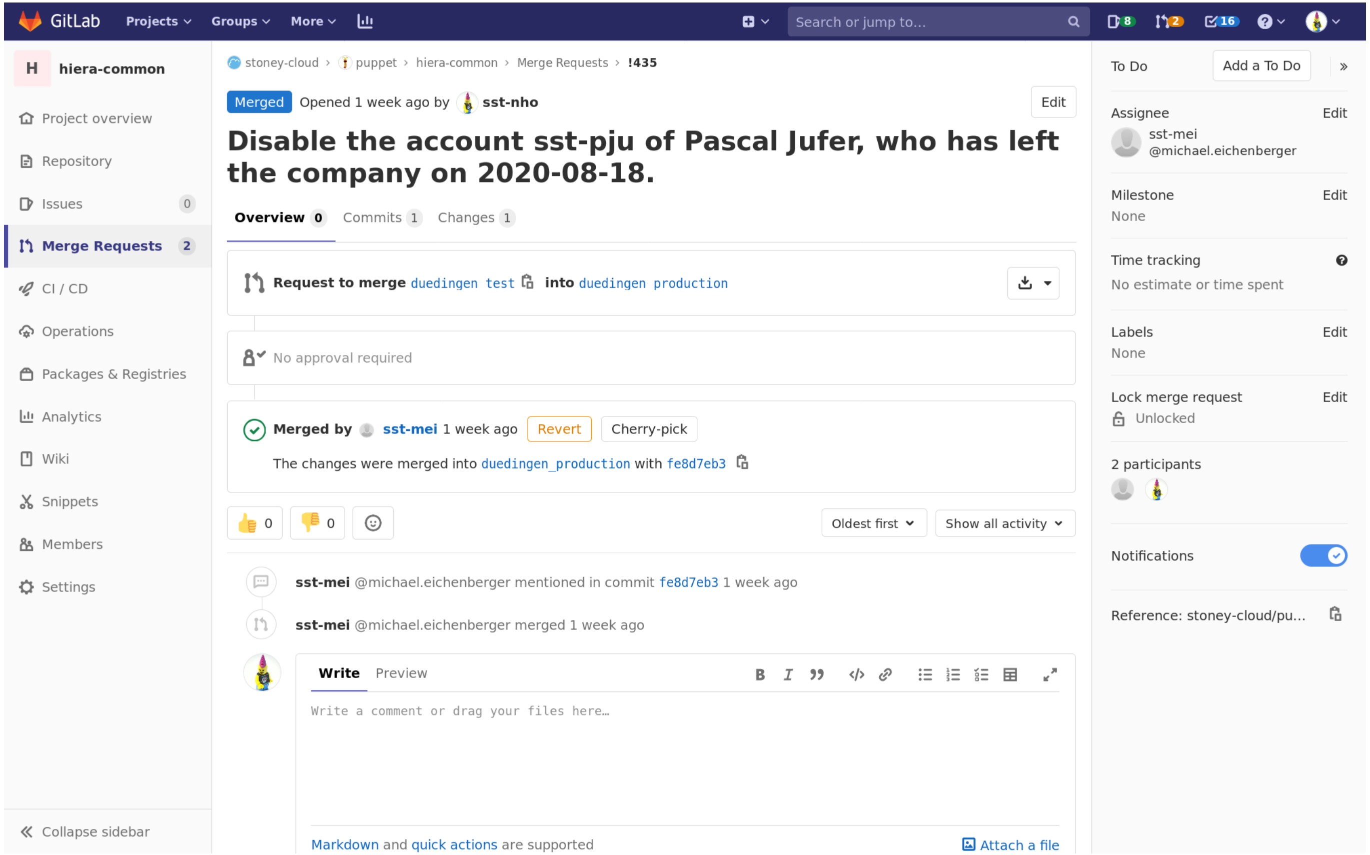
Puppet run



```
Notice: /Stage[main]/System_accounts/User[sst-pju]/ensure: removed
Notice: /Stage[main]/System_accounts/File[/var/spool/cron/sst-pju]/ensure: removed
Notice: /Stage[main]/Ssh::Server::Config/Concat[/etc/ssh/sshd_config]/File[/etc/ssh/sshd_config]/content:
--- /etc/ssh/sshd_config        2020-04-03 12:02:21.179357366 +0200
+++ /tmp/puppet-file20200903-13475-7318pn       2020-09-03 15:47:23.557310575 +0200
@@ -7,7 +7,6 @@
 AllowUsers sst-mbi
 AllowUsers sst-mei
 AllowUsers sst-nho
-AllowUsers sst-pju
 AllowUsers sst-tmu
 AllowUsers sst-yde
 AuthorizedKeysFile /etc/ssh/authorized_keys/%u
```

Gitlab: Merge request

stepping stone



Merged Opened 1 week ago by sst-nho

Disable the account sst-pju of Pascal Jufer, who has left the company on 2020-08-18.

Request to merge `duedingen test` **into** `duedingen production`

No approval required

Merged by sst-mei 1 week ago

The changes were merged into `duedingen_production` with `fe8d7eb3`

sst-mei @michael.eichenberger mentioned in commit fe8d7eb3 1 week ago

sst-mei @michael.eichenberger merged 1 week ago

Write a comment or drag your files here…

Assignee: sst-mei @michael.eichenberger

Milestone: None

Time tracking: No estimate or time spent

Labels: None

Lock merge request: Unlocked

2 participants

Notifications: on

Reference: stoney-cloud/pu...

Welchen Nutzen ziehen wir daraus?

Nutzen

- Logische Fortsetzung unserer Arbeitsweise
  - Flexible Umsetzung
  - Mediawiki
- Verbesserungspotential aufgezeigt
- Konsequente Automatisierung
  - Puppet
  - Gitlab

Fragen?

stepping stone AG
Wasserwerkgasse 7
CH-3011 Bern

Telefon: +41 31 332 53 63
www.stepping-stone.ch
info@stepping-stone.ch