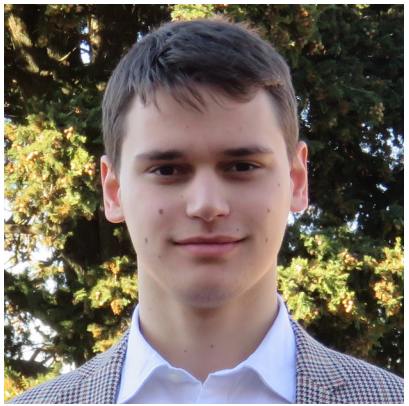
Remotely accessing files in a distributed LDAP+Samba-based infrastructure

”Cloud” in a new manner

Marco Marinello
me@marcomarinello.it

$ whoami

- CS Student @ UniBZ
- Developer / SysAdmin @ continuity.space (Italy)
- Member of TDF
- President of the Linux User Group of Bolzano
- Developer of the FUSS project



There is NO CLOUD, just other people's computers

GDPR

Privacy shield

Data protection

Remote Access

Remotely accessing files in a distributed LDAP+Samba-based infrastructure

M. Marinello

FUSS Team, Autonomous Province of Bolzano, 39100 Italy
e-mail: me@marcomarinello.it

March 23, 2020

ABSTRACT

Context. An in-production infrastructure of 64 schools running Debian-based networks with OpenLDAP and Kerberos. Samba is even provided for Windows compatibility. This O.S. is called "FUSS" * and is developed by the Autonomous Province of Bolzano.

What's FUSS?

FUSS

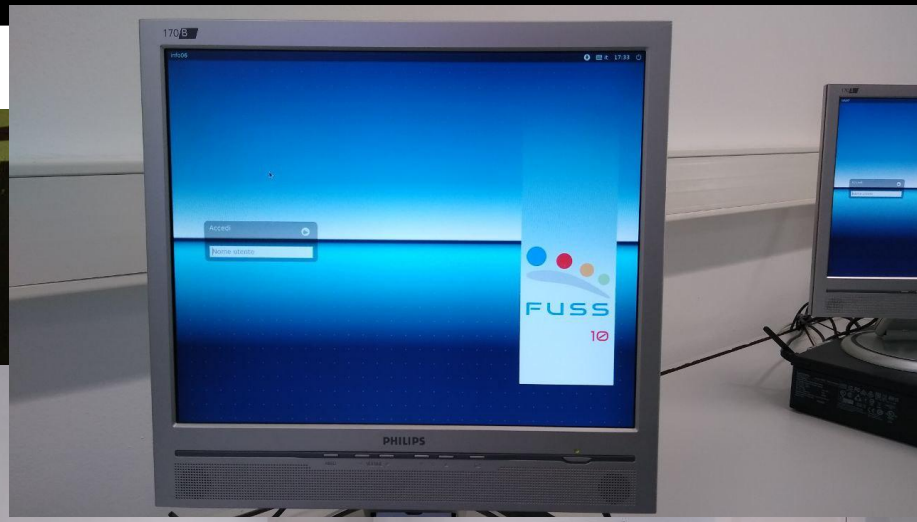
stands for

Free Upgrade for a digitally Sustainable School

What’s FUSS?

- Launched in 2005
- Covers 72 schools with 64 servers and 4000 PCs and Laptops
- Both server and client distro
- Selection of didactic software


FUSS


Accedi
Nome utente
FUSS
10
PHILIPS

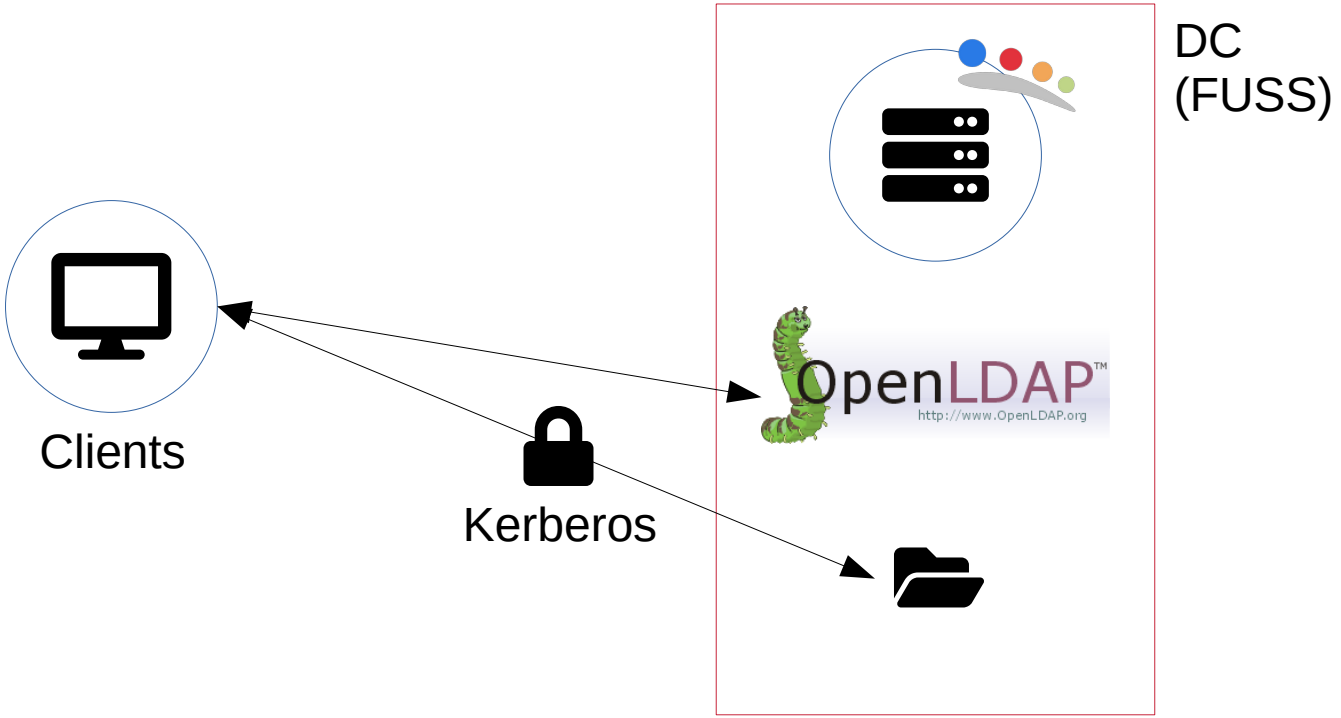

FUSS
https://fuss.bz.it

Schools are far

Goal

Make users files available remotely

How a school network works?

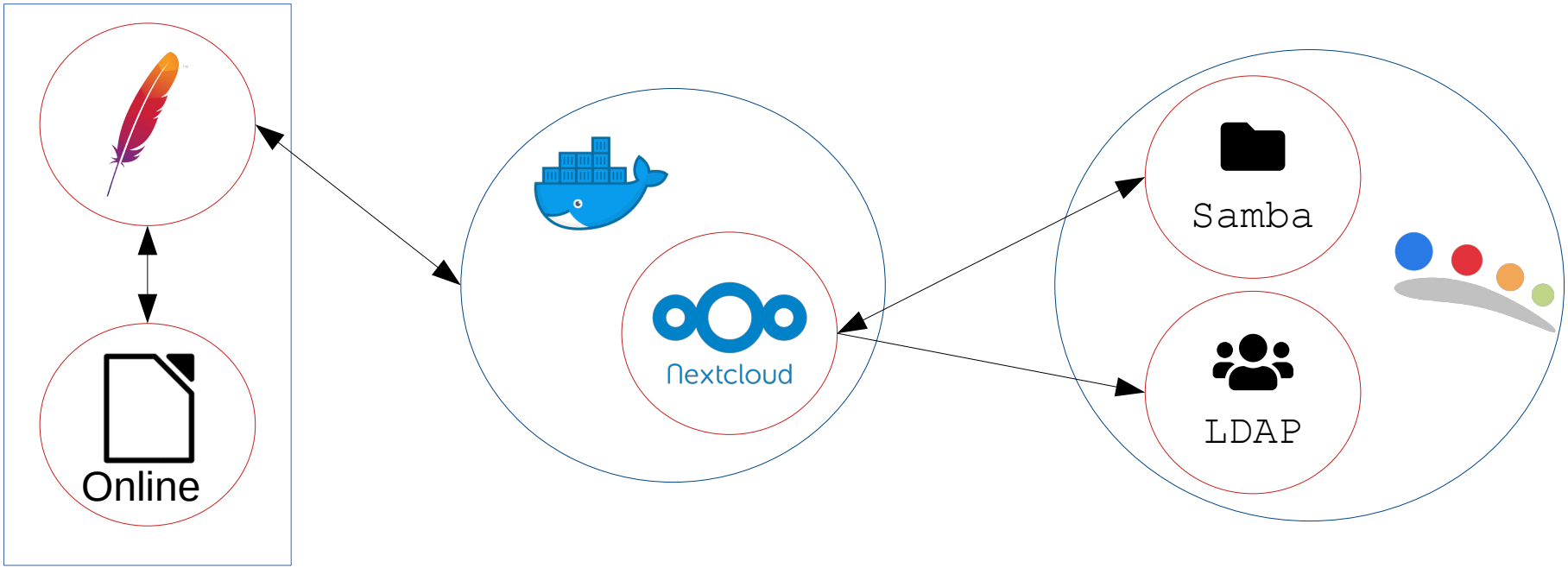


What’s FUSS Remote Access?

Solution to access your data outside the school network

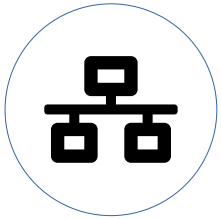
Online collaboration suite (LOOL)

Private cloud


Online
Nextcloud
Samba
LDAP

Why this solution?

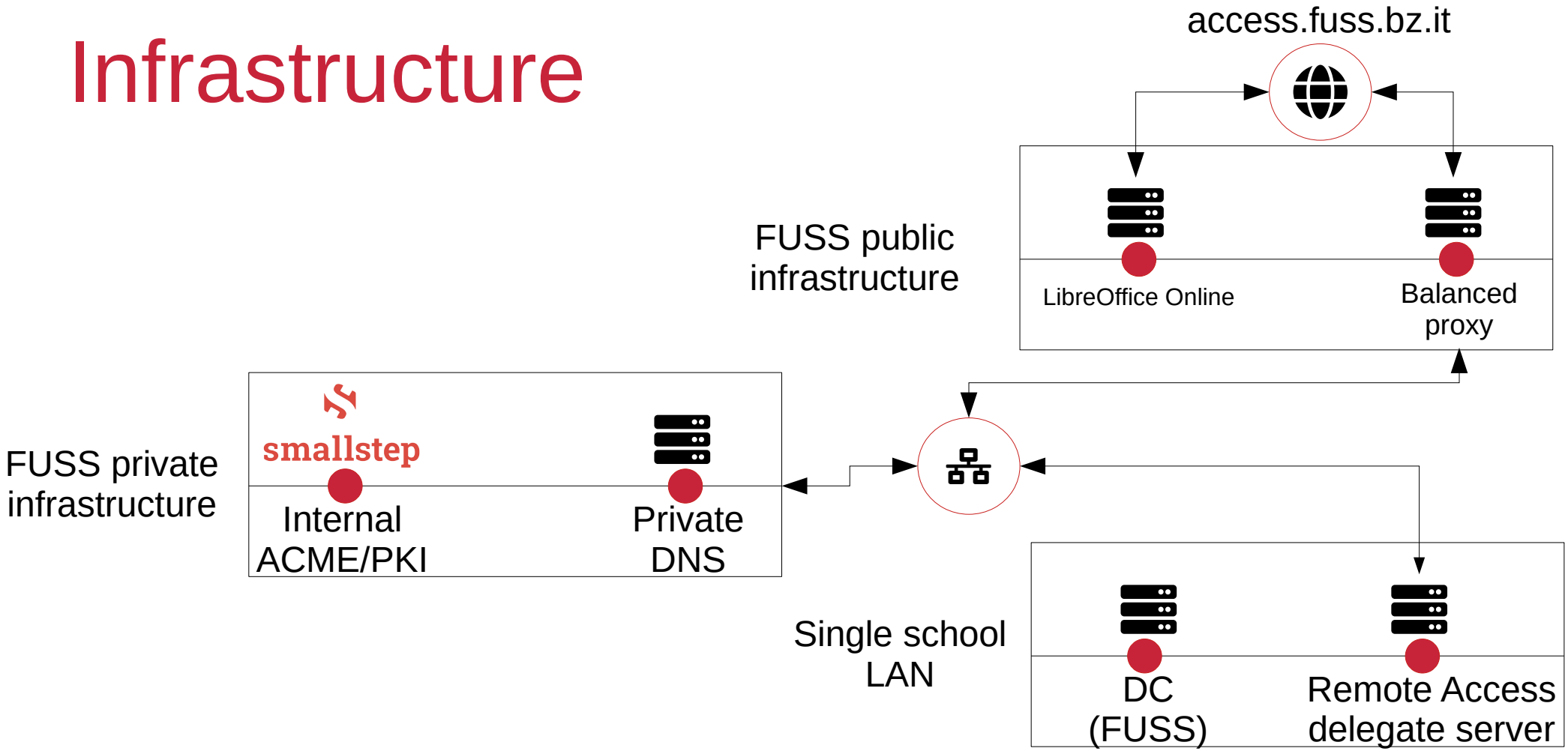
Data under control (GDPR)



Distributed storage

Same credentials as the school network (SSO)

Infrastructure



Building LibreOffice online

Automating stable compilation

The following script may be used to automatically fetch the latest (supposed) stable version and compile it. You can run it in something like a nightly build. In any case, using ccache is highly suggested to enhance a lot the build times after the first.

```
cd /opt
[ -e online ] || git clone --depth=1 https://git.libreoffice.org/online
cd online
git pull origin master
cd docker
git ls-remote https://git.libreoffice.org/core | cut -f 2 | grep -e '^refs/heads/libreoffice' | tail -1 | rev | cut -d '/' -f 1 | rev > core-branch
git ls-remote https://git.libreoffice.org/online | cut -f 2 | grep -e '^refs/heads/libreoffice' | tail -1 | rev | cut -d '/' -f 1 | rev > online-branch
LIBREOFFICE_BRANCH="$(cat core-branch)" LIBREOFFICE_ONLINE_BRANCH="$(cat online-branch)" DOCKER_HUB_TAG="$(cat online-branch)-$(date +%Y-%m-%d)" NO_DOCKER_PUSH="yes"
ONLINE_EXTRA_BUILD_OPTIONS="--enable-anonymization --with-max-connections=100000 --with-max-documents=100000" ./l10n-docker-nightly.sh
```

https://wiki.documentfoundation.org/Development/LibreOffice_Online
https://wiki.documentfoundation.org/Development/BuildingOnline

Pillars: the ACME protocol

"The Automatic Certificate Management Environment (ACME) protocol is a communications protocol for automating interactions between certificate authorities and their users' web servers, allowing the automated deployment of public key infrastructure at very low cost. It was designed by the Internet Security Research Group (ISRG) for their Let's Encrypt service."

(from Wikipedia)

Pillars: `certbot`

Is the software who implements the ACME protocol

Pillars: the ACME protocol

- The agent says to the server which domains he wants to verify (e.g. `domain.tld`);
- The server returns a token and a path in which he expects this token to be available;
- The agent moves the token in place and the server challenges via HTTP expecting to find the token he gave to the agent;
- If successful, the server signs a CSR uploaded by the agent. The private key is generated on the host and remains on the host.

Pillars: Smallstep

- Toolikit for internal PKI management
- SSH Single-sign-on
- Implementation of ACME server

smallstep

Pillars: Proxmox

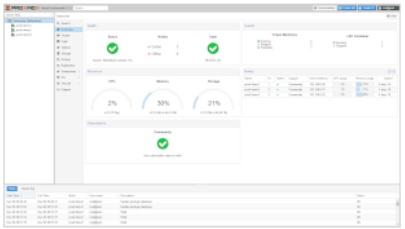
PROXMOX

Home | Virtualization | Email Security | Downloads | Training | Partners | News | About us

Home | Virtualization

Proxmox Virtual Environment

Compute, network, and storage in a single solution



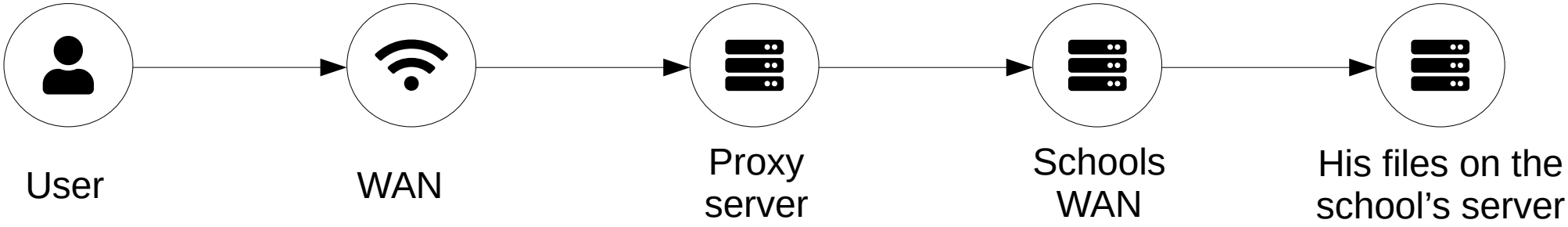
Proxmox VE is an open-source server management platform for your enterprise virtualization. It tightly integrates KVM hypervisor and LXC, software-defined storage, and networking functionality on a single platform. With the integrated web-based user interface you can easily manage VMs and containers, highly available clusters, or the integrated disaster recovery tools with ease.

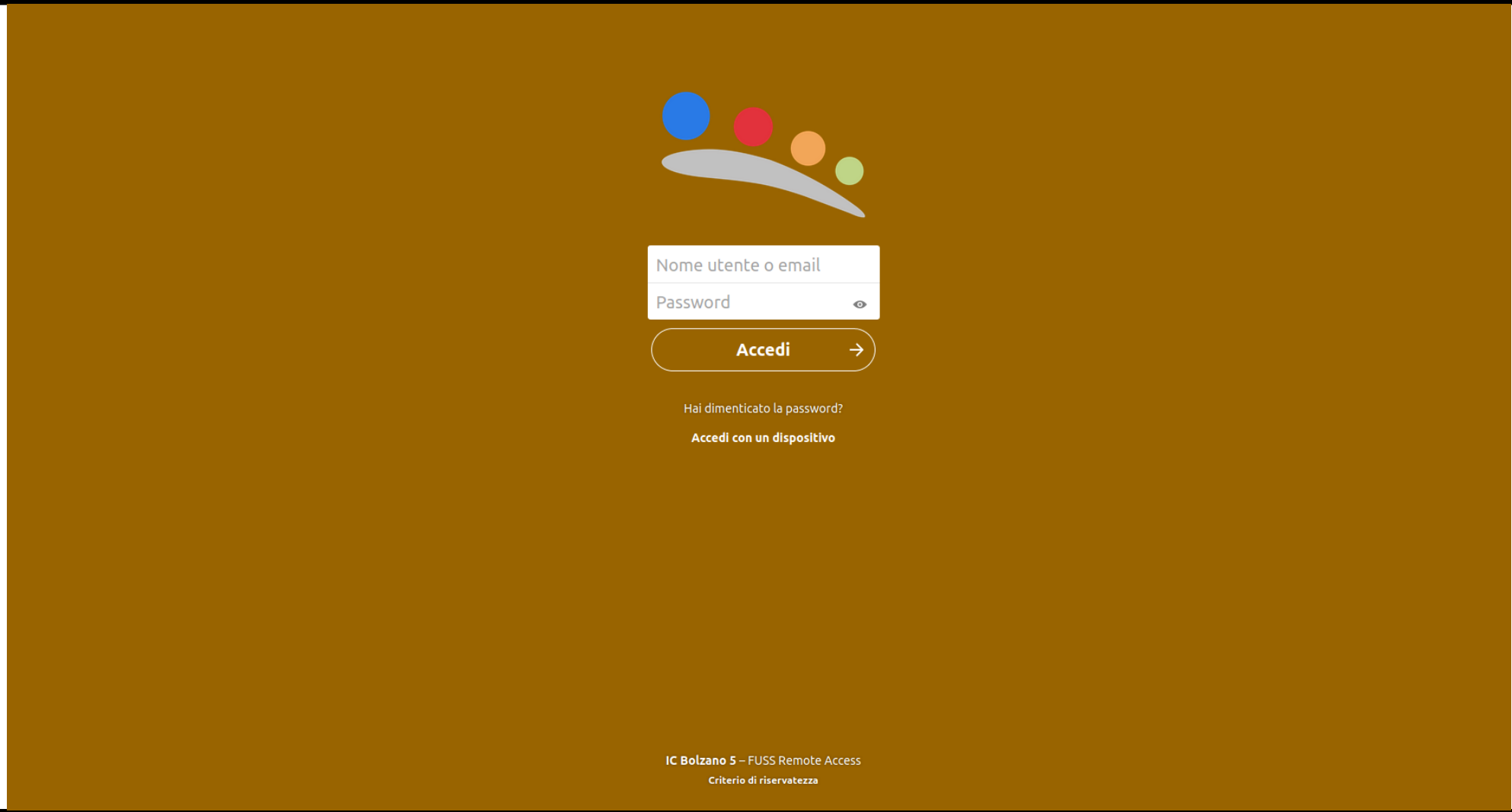
Enterprise-class features and a 100% software-based focus make Proxmox VE the perfect choice to virtualize your IT infrastructure, optimize existing resources and increase efficiencies with minimal expense. You can easily virtualize even the most demanding Linux and Windows application workloads, and dynamically scale computing and storage as your needs grow ensuring that your data center adjusts for future growth.

Ready to build an open and future-proof data center with Proxmox VE?

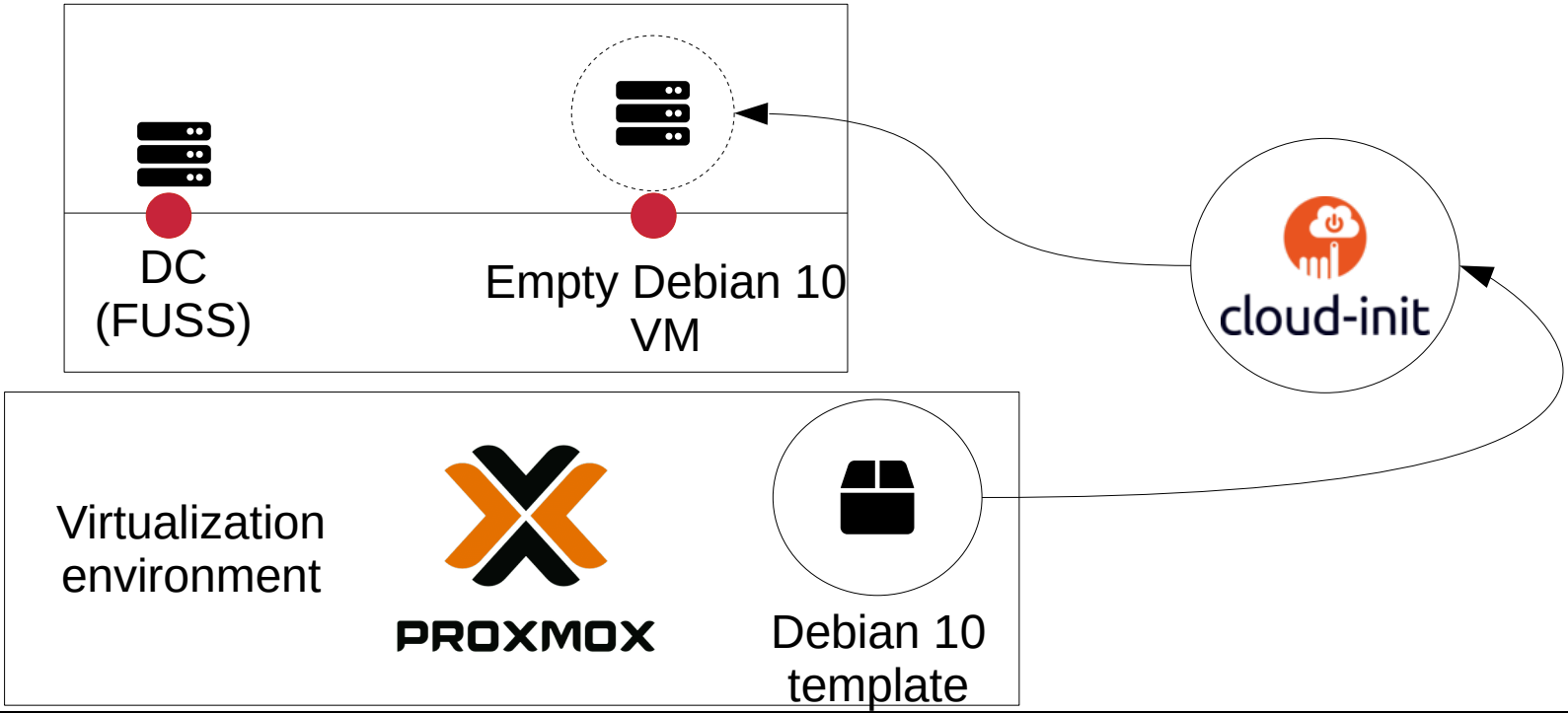
Get started | Download

Access path


User
WAN
Proxy server
Schools WAN
His files on the school’s server

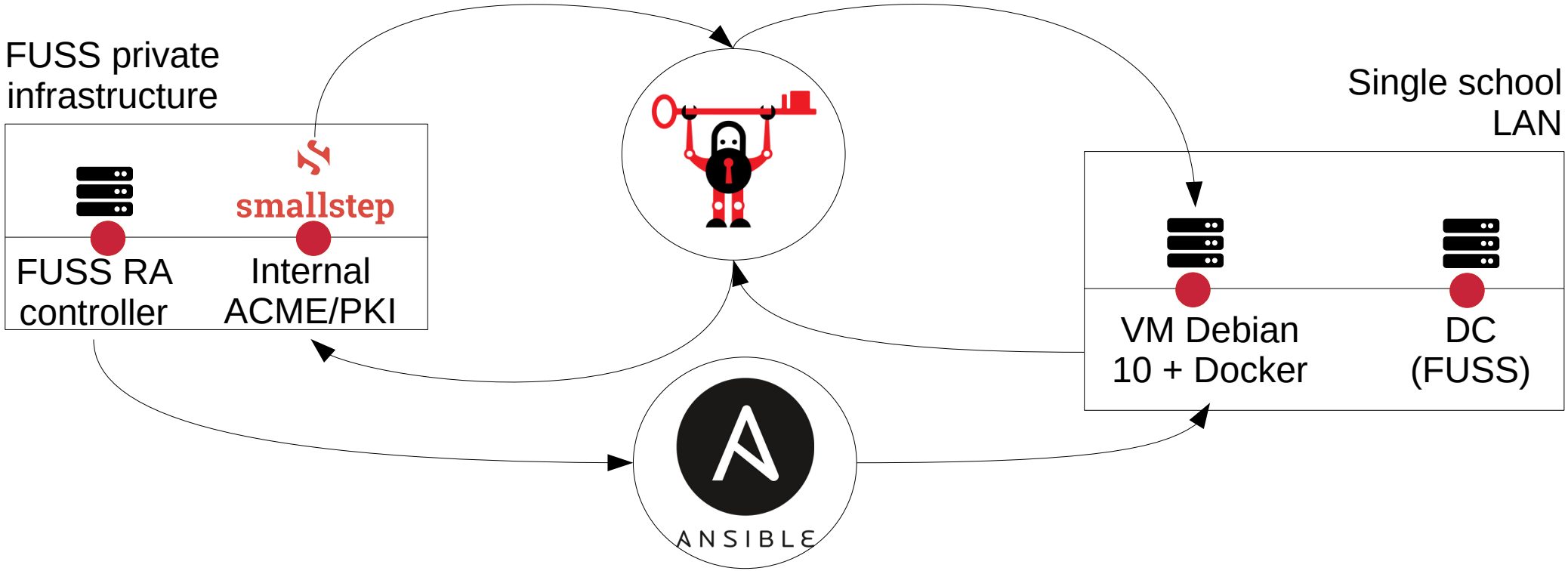

Nome utente o email
Password
Accedi
Hai dimenticato la password?
Accedi con un dispositivo
IC Bolzano 5 – FUSS Remote Access
Criterio di riservatezza

Deploy strategy
1. Creation of the delegate server



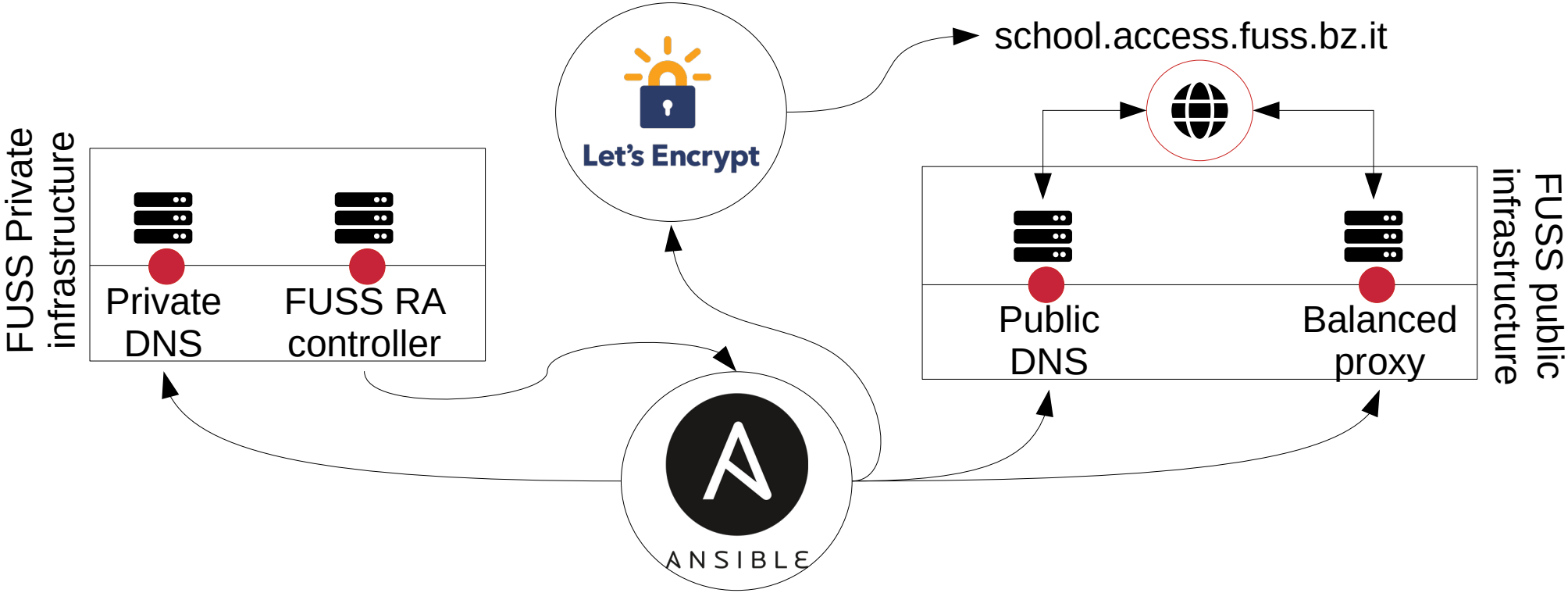
Deploy strategy

2. Delegate server setup

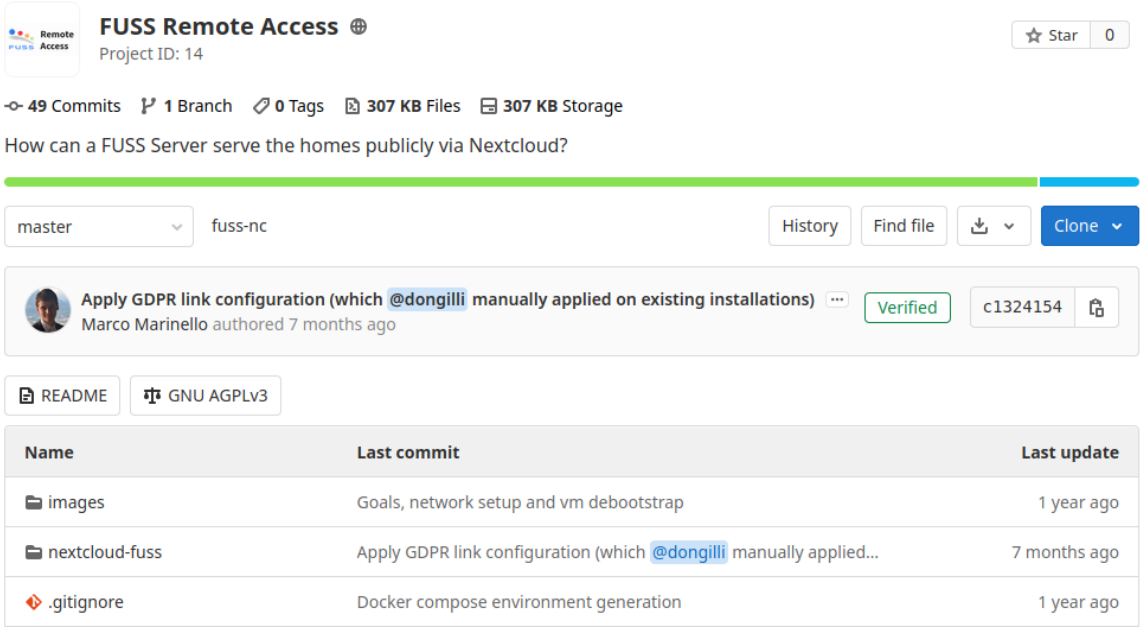


Deploy strategy

3. Orchestration of the central infrastructure



Give me the code!



- https://gitlab.fuss.bz.it/fuss-team/fuss-nc

Want to know more?

Feel free to get in touch with me:

marinello@libreoffice.org

Thank you!