

# Wendelin Exanalytics Security & Safety Design

2014-07-07 – Shanghai





# Agenda



## **Architecture Overview**

- Design Goals
- Security
- Safety



## Wendelin Core

#### 100% open source

Numpy / OpenCV-Python / Scikit-learn / etc.

**Data Analytics** 

**NEO** 

Distributed Storage

MariaDB

Elastic PaaS

ERP5

**Multicloud Deployment** 

**SlapOS** 

Multi Data Center







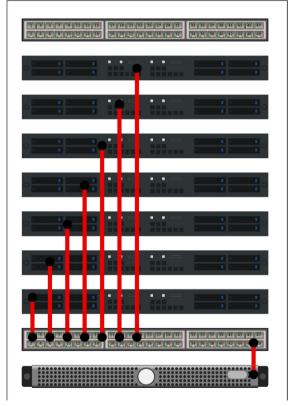
100% Python



#### Data Center Overview







10 Gbps L2 Switch Standard Server

IPMI L2 Switch

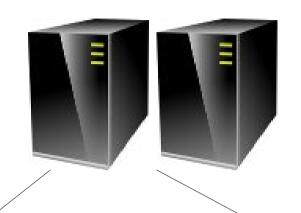
Management Serve

Management Network



**Bay LAN** 

## SlapOS Master Overview

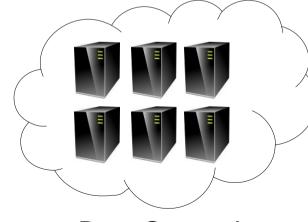


#### **SlapOS Master**

- Deployment
- Orchestration
- Accounting
- Disaster Recovery

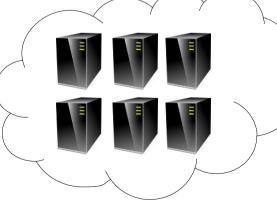
#### **SLAP Protocol**

SlapOS Nodes



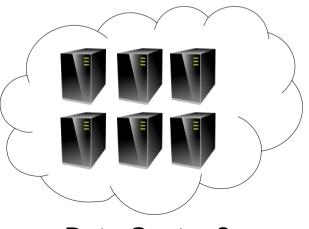
Data Center 1

SlapOS Nodes



Data Center 2

SlapOS Nodes



Data Center 3



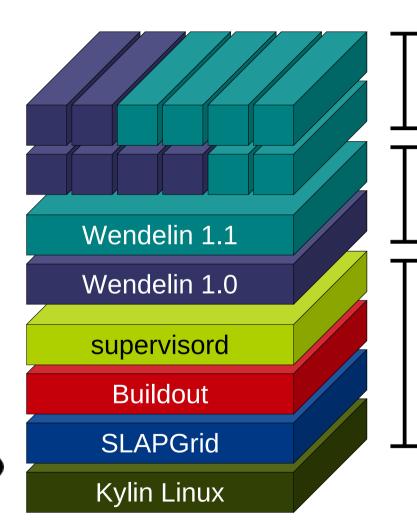
# SlapOS Node Overview

100+ software instances per server



SlapOS Node

Data Center



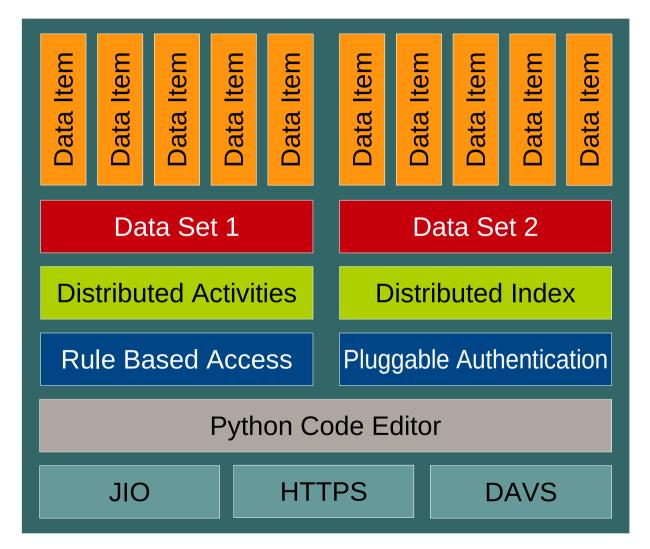
Software Instance

Software Release

SlapOS Kernel



## **ERP5 PaaS Overview**



**Data Management** 

Scalability

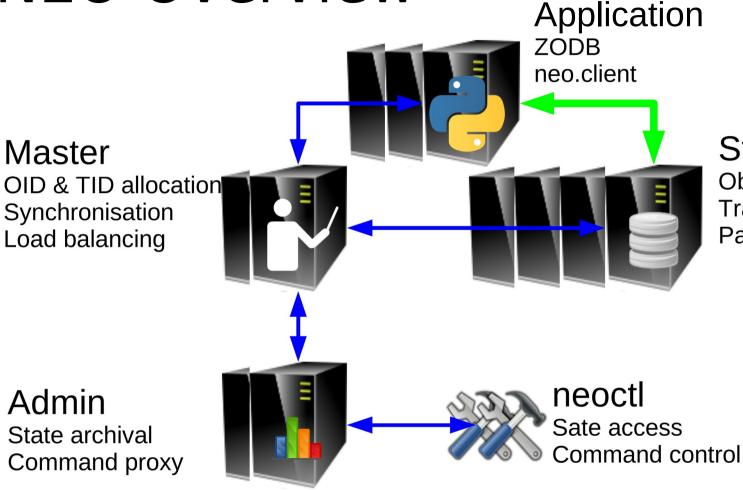
Security

**IDE** 

Input / Output



## **NEO Overview**









# **Numpy Overview**

#### neo.ndarray

	1	2	3	4	5	6	7	8	9	10	11	12
--	---	---	---	---	---	---	---	---	---	----	----	----





5 5

9 9





2 2

6 6

10 10





3 3

7 7

11 | 11







4 4

8 8

12 | 12



# Agenda

Architecture Overview



**Design Goals** 

- Security
- Safety



# Security & Safety

#### Security

- Data Encryption
- Data Access Rule
- User Authentication
- Computer Authentication
- Software Authentication
- Service Authentication
- Zero Knowledge
- Intrusion protection
- Public Key Infrastructure

#### Safety

- Availability
- Consistency
- Scalability
- Persistence
- Disaster Recovery



# Agenda

- Architecture Overview
- Design Goals



**Security** 

Safety



Data Encryption

Storage

Original data in neo.client processing node

Application

Command control

Master OID & TID allocation Synchronisation Load balancing

Admin State archival Command proxy



Storage Object data Transaction data Partition table

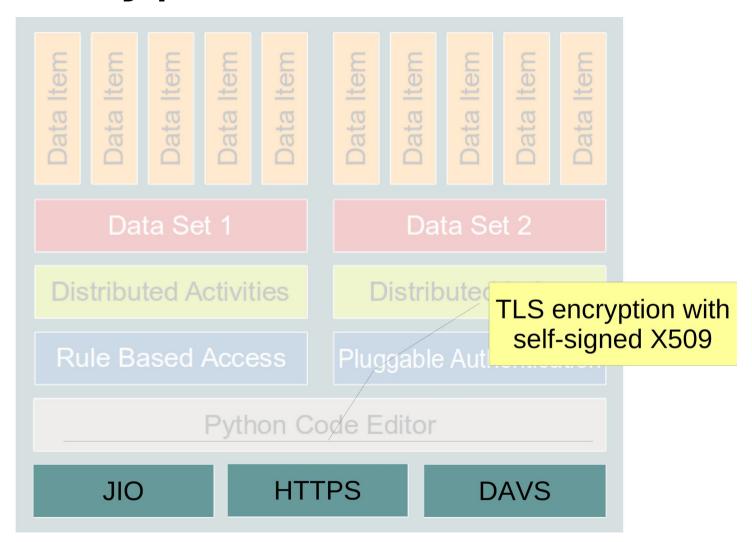
> **Encrypted data** inside storage





## Data Encryption

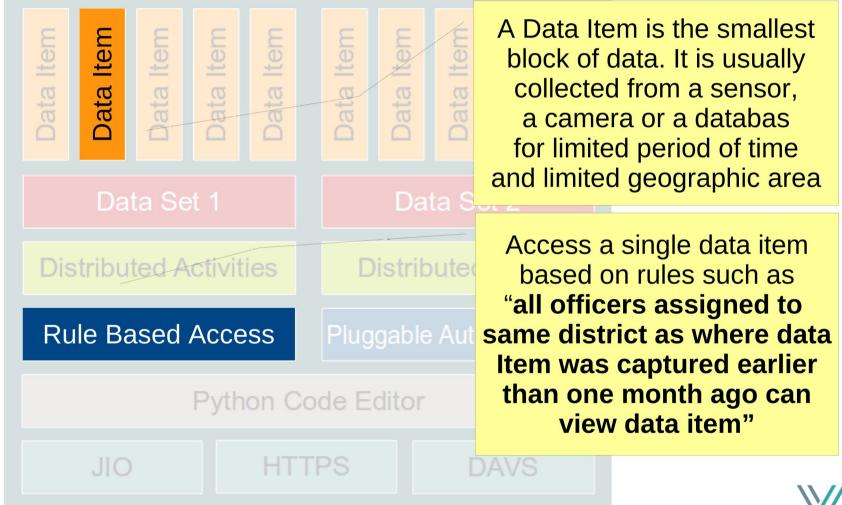






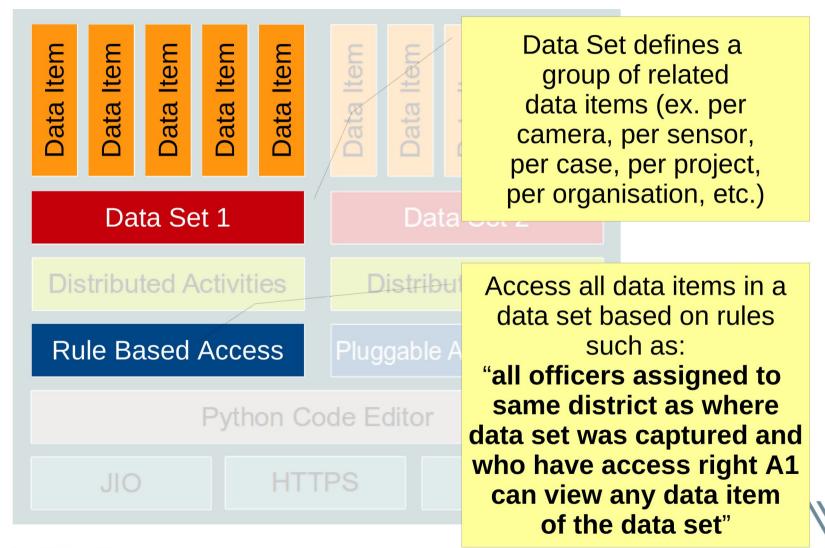
#### Data Access Rules

#### Data Item



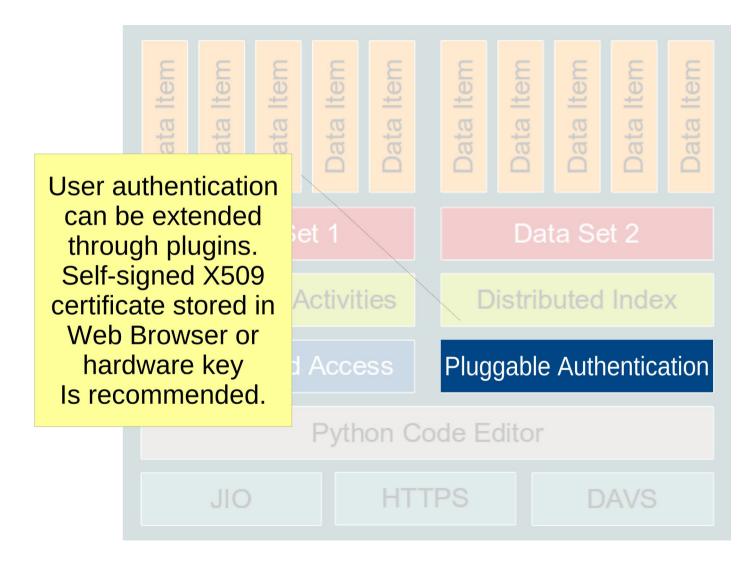
## Data Access Rules

#### Data Set



## User Authentication

#### X509





## Computer Authentication

## X509



Each computer has its own X509 certificate to authenticate to SlapOS Master for secure deployment

Super visoru

Buildout

SLAPGrid

Kylin Linux

Software Instance

Software Release

SlapOS Kernel



## Software Authentication

## X509

100+ software

Each deployed software is signed with X509 certificate of authorized system administrator



Wendelin 1.0 supervisord

Software Instance

Software Release

SlapOS Kernel



## Service Authentication

#### X509

WENDELIN



# Zero Knowledge

## zero root

Each service runs with non privileged user

slapgrid runs with non privileged user

Kylin Linux runs
without sshd and without
remote root access

Data Center

supervisord **SLAPGrid** Kylin Linux

Software Instance

Software Release

SlapOS Kernel



## Zero Knowledge

## zero password

No password or credential to access running services is kept in SlapOS Master



#### **SlapOS Master**

- Deployment
- Orchestration
- Accounting
- Disaster Recovery

SLAP Protocol

Credentials to access a a service are kept as a hash in the computer that runs the service





Data Center 2



Data Center 3



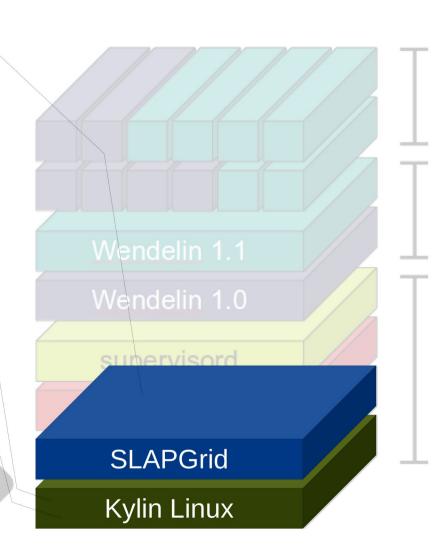
#### Intrusion Protection

slapgrid collects resource usage logs to detect abnormal behaviour of running processes

Kylin Linux runs
without sshd and without
remote root access

Kylin Linux source code has been audited by Chinese Ministry of Defense

Data Center



Software Instance

Software Release

SlapOS Kernel



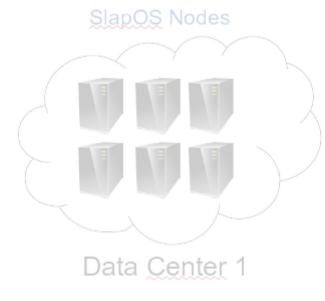
# Public Key Infrastructure (PKI)

SlapOS Master acts as PKI and generates X509 certificates for users, computers, software and services



#### **SlapOS Master**

- Deployment
- Orchestration
- Accounting
- Disaster Recovery







WENDELIN

# Agenda

- Architecture Overview
- Design Goals
- Security



**Safety** 



## **Availability**

System remains available in case of unavailability of SlapOS master

System remains available in case of unavailability of SlapOS node

SlapOS Nodes



Data Center 1 Data Center 2

# SlapOS

#### SlapOS Master

- Deployment
- Orchestration
- Accounting
- Disaster Recovery







Data Center 3



**Availability** 

**NEO** 

System remains
Available in case
of unavailability
master node

OID & TID allocation Synchronisation Load balancing

System remains
Available in case
of unavailability
control node

State archival Command proxy



Sate access

Command co

System remains available in case of unavailability of compute node

Object data
Transaction data
Partition table

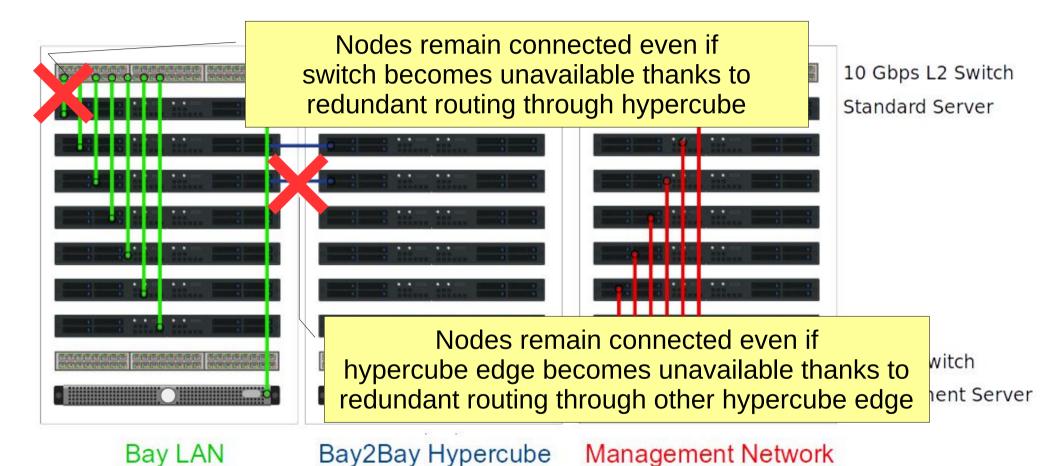
System remains available in case of unavailability of storage node





## **Availability**

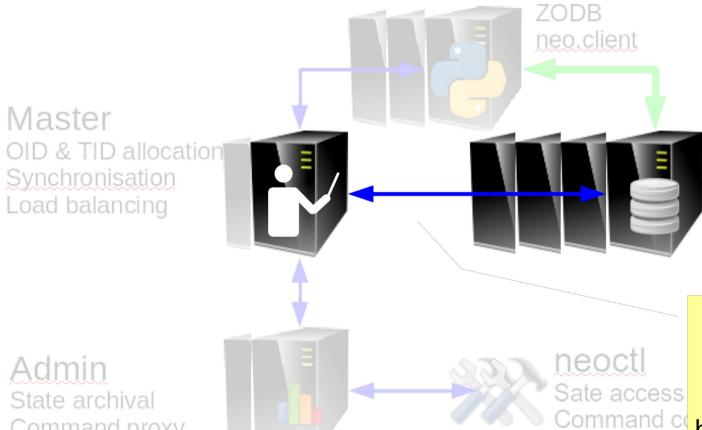






Consistency





Storage Object data Transaction data Partition table

Application

Command proxy

All storage nodes remain consistent thanks to transaction ID generated by master node and stored with each object or block

# Scalability

## **NEO**

Master
OID & TID allocation
Synchronisation
Load balancing

Add more computer nodes for more computation

Storage
Object data
Transaction data
Partition table

Application

Admin
State archival
Command proxy



All storage nodes remain consistent thanks to transaction ID generated by master node and stored with each object or block



## Persistence

# SlapOS

100+ software instances per server

Each service on SlapOS node
has a minimum persistence
ttime parameter to prevent
unexpected data destruction as
potential consequence of
human error or intrusion on
SlapOS master

Data Center

Nendelin 1.1

Nendelin 1.0

supervisord

Buildout

 ${\sf SLAPGrid}$ 

Kylin Linux

Software Instance

Software Release

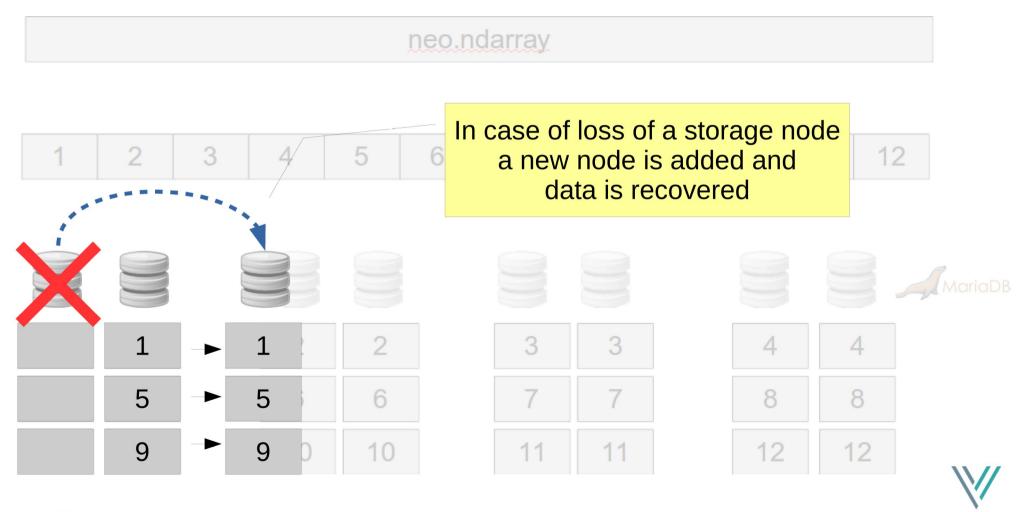
SlapOS Kernel



## Disaster Recovery

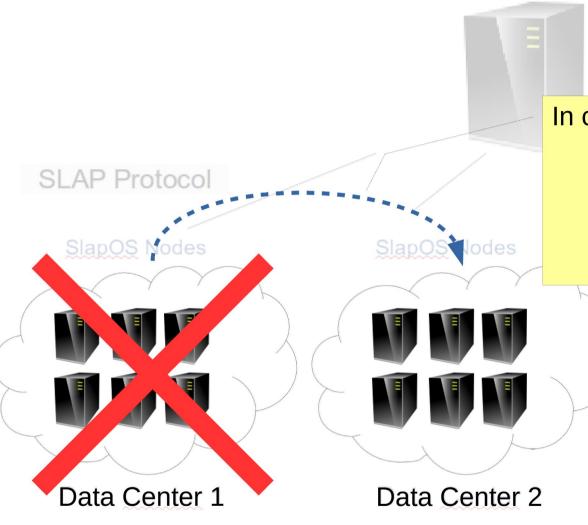
## Storage

WENDELIN



## Disaster Recovery

## Datacenter



#### **SlapOS Master**

- Deployment
- Orchestration

In case of loss of a data center node another data center that has a real time copy of data and application configuration kept in sync automatically and tested daily is used instead







## **Wendelin Exanalytics** *Security & Safety Design*

2014-07-07 - Shanghai





#### Agenda



#### > Architecture Overview

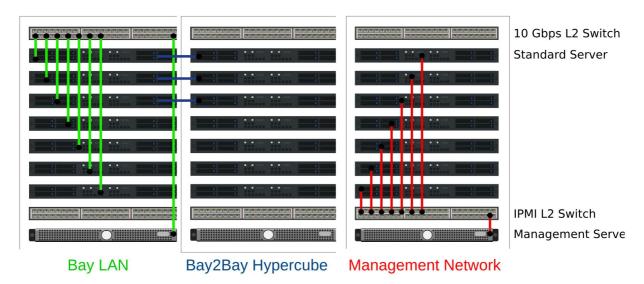
- Design Goals
- Security
- Safety



© 2014 Wendelin Project et al. – CC SA-NC

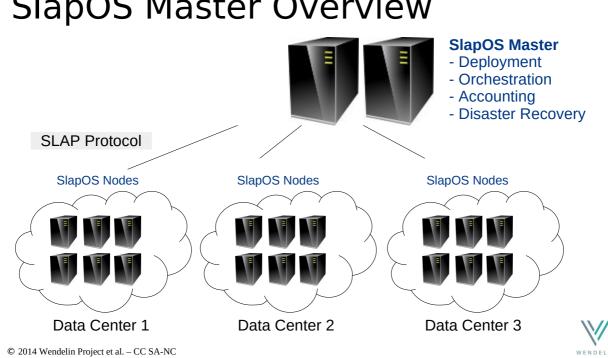
# Wendelin Core | Numpy / OpenCV-Python / Scikit-learn / etc. | Data Analytics | | NEO | Distributed Storage | MariabB | | ERP5 | Elastic PaaS | | Multicloud Deployment | | Multi Data Center | | Wunder | Distributed Storage | Distributed Stora

#### **Data Center Overview**

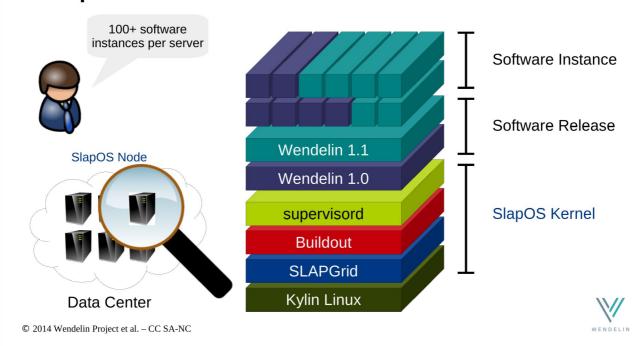




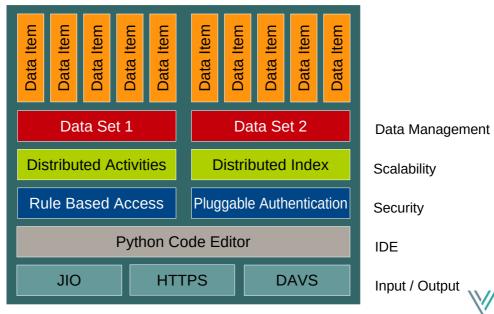
#### SlapOS Master Overview

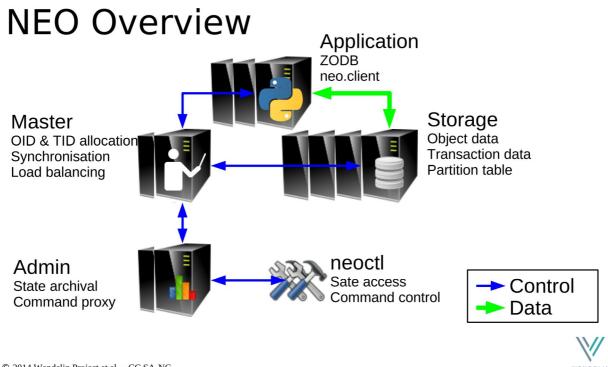


#### SlapOS Node Overview

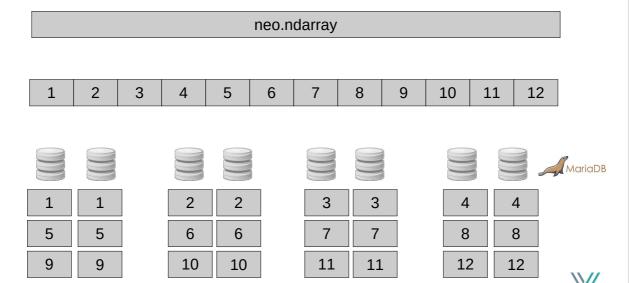


#### **ERP5 PaaS Overview**





## **Numpy Overview**



## Agenda

• Architecture Overview



**Design Goals** 

- Security
- Safety



#### Security & Safety

#### Security

- Data Encryption
- Data Access Rule
- User Authentication
- Computer Authentication
- Software Authentication
- Service Authentication
- Zero Knowledge
- Intrusion protection
- Public Key Infrastructure

#### Safety

- Availability
- Consistency
- Scalability
- Persistence
- Disaster Recovery



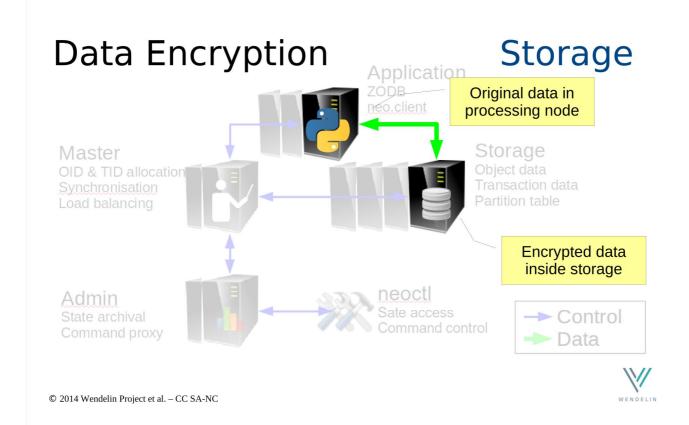
## Agenda

- Architecture Overview
- Design Goals



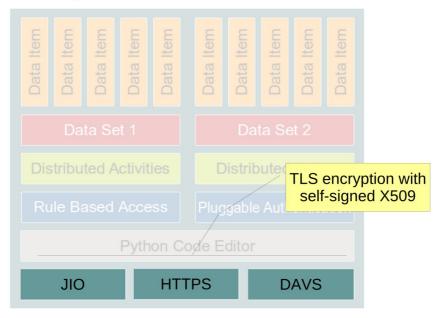
SecuritySafety





## **Data Encryption**



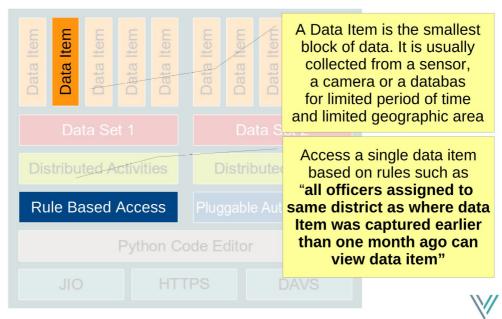






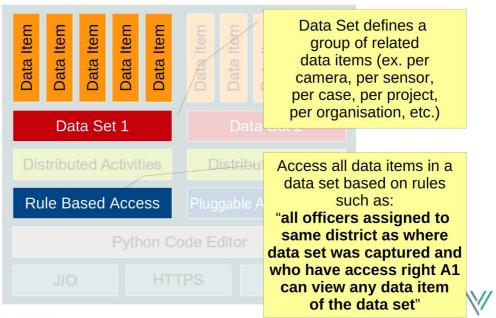
#### **Data Access Rules**

#### Data Item



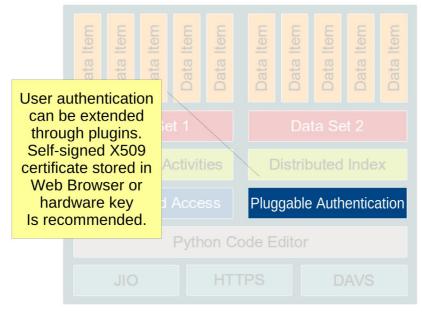
#### **Data Access Rules**

#### **Data Set**



#### **User Authentication**

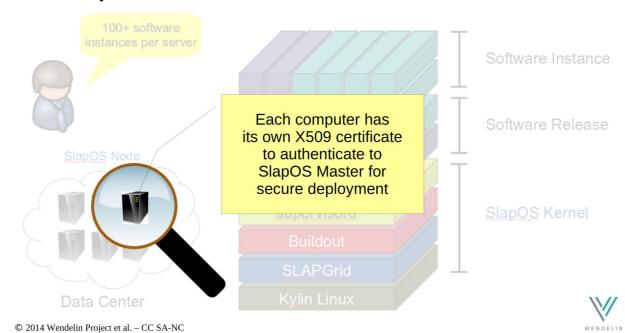
X509





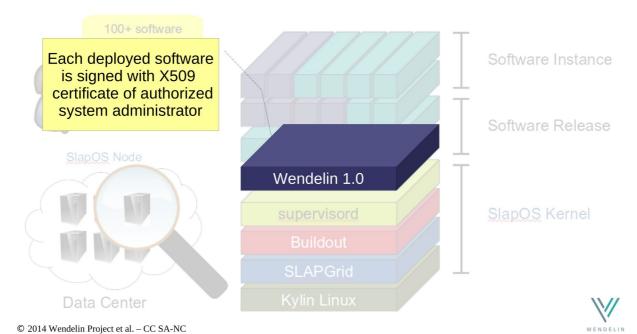
#### Computer Authentication

X509



#### Software Authentication

X509

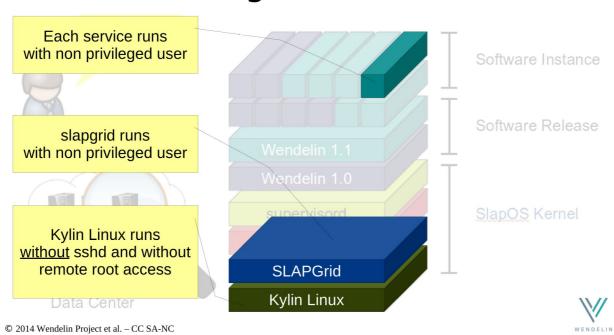


© 2014 Wendelin Project et al. – CC SA-NC

## Service Authentication 100+ software instances per server Each service has its own X509 certificate to authenticate to SlapOS Master for secure orchestration SlapOS Kernel Buildout X509 Software Instance Software Release

#### Zero Knowledge

#### zero root



#### Zero Knowledge

#### zero password

No password or credential to access running services is kept in SlapOS Master



SlapOS Master

- Deployment
- Orchestration
- Accounting
- Disaster Recovery

SLAP Protocol

Credentials to access a a service are kept as a hash in the computer that runs the service





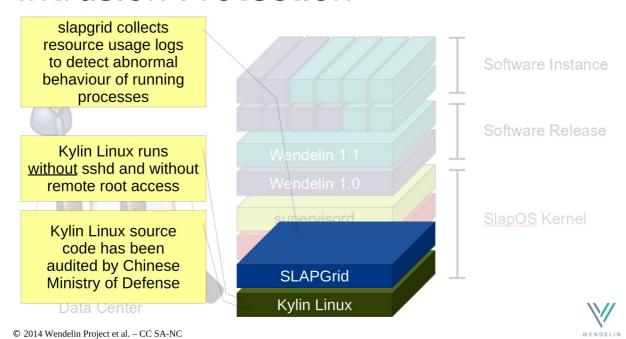
Data Center 1

© 2014 Wendelin Project et al. – CC SA-NC

Data Center 3



#### **Intrusion Protection**



#### Public Key Infrastructure (PKI)

SlapOS Master acts as PKI and generates X509 certificates for users, computers, software and services



#### **SlapOS Master**

- Deployment
- Orchestration
- Accounting
- Disaster Recovery

SlapOS Nodes



Data Center 1

SlapUS Nodes



Data Center 2

SlapOS Nodes



Data Center 3



## Agenda

- Architecture Overview
- Design Goals
- Security



Safety



#### **Availability**

System remains available in case of unavailability of SlapOS master

System remains available in case of unavailability of SlapOS node





© 2014 Wendelin Project et al. – CC SA-NC



#### SlapOS

#### **SlapOS Master**

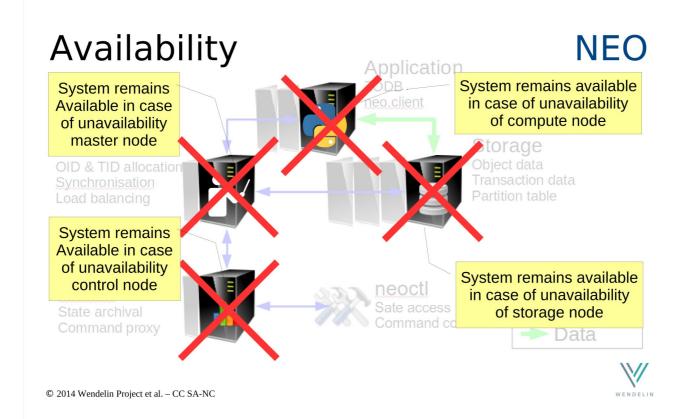
- Deployment
- Orchestration
- Accounting
- Disaster Recovery

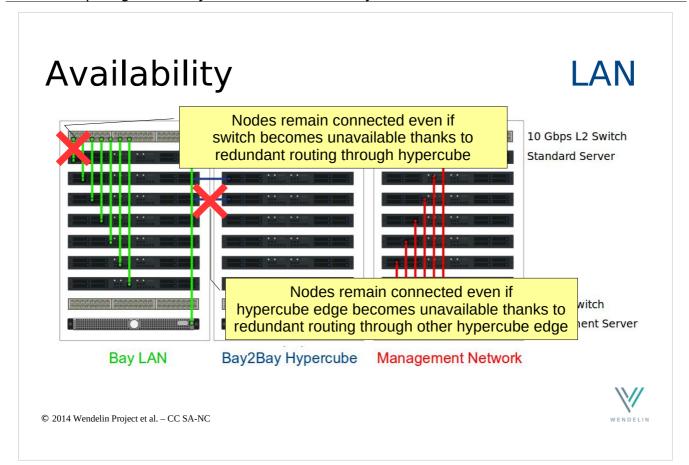


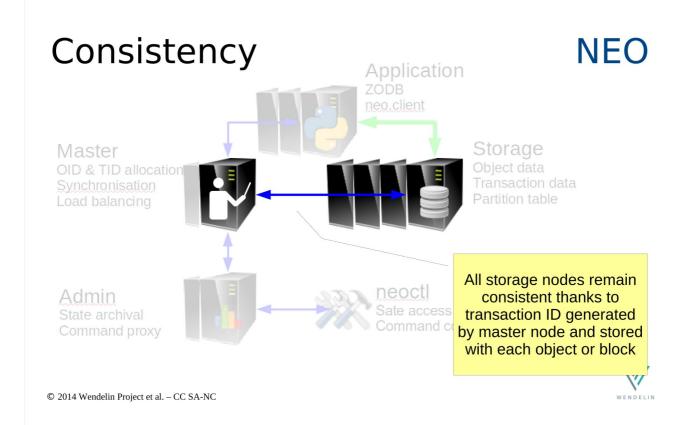


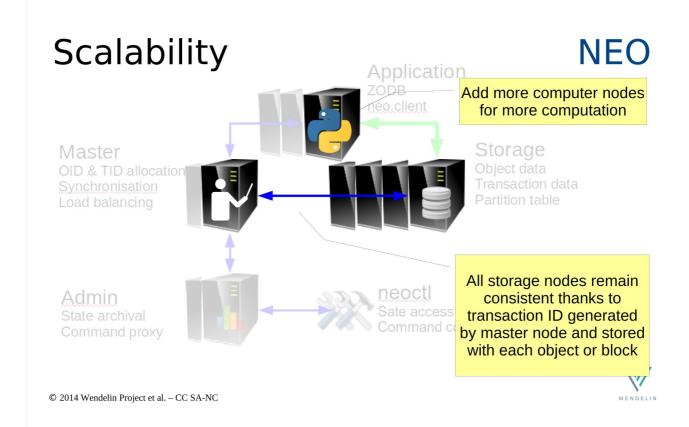
Data Center 3









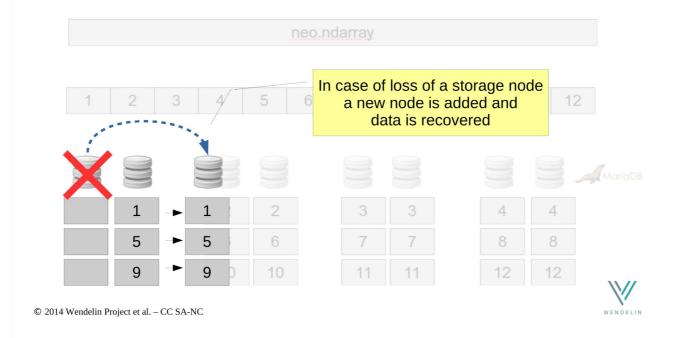


© 2014 Wendelin Project et al. – CC SA-NC

# Persistence 100+ software instances per server Software Instance Software Release Each service on SlapOS node has a minimum persistence time parameter to prevent unexpected data destruction as potential consequence of human error or intrusion on SlapOS master SlapOS Kernel Buildout SLAPGrid

#### Disaster Recovery

#### Storage



#### Disaster Recovery

#### Datacenter

