Migrating 515 AD servers to Samba

In a galaxy NOT far far away!

Caglar Ulkuderner
caglar@profelis.com.tr

* All StarWars images are sourced at www.StarWars.com

Regions

Digital Transformation

Ankara İstanbul Sofya Doha

37.301
Computer

1.184
Location

515
Server

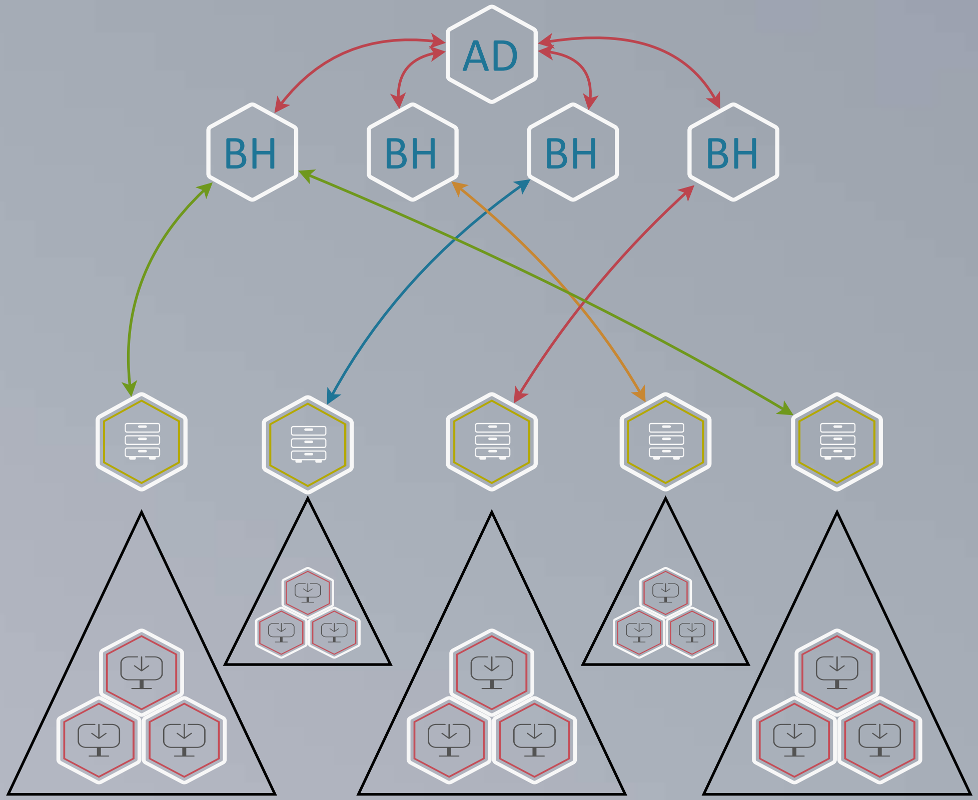
Galaxy

Ministry of Finance
Revenue Administration

Organisatinal page
www.gib.gov.tr

Project page
gibux.gib.gov.tr

Network Topology



1034032109

Kullanıcı adı: 999888777

Parola:

37.301
Computer

1.184
Location

History of **Gibux**

Starting Project

April 2013

Analysing and design

R&D **Phase**

June 2013 -February 2014

Developing required OS modules and
some device drivers which is required for production

First Flight

February 2014

Release Candidate version
has been installed on two tax office

Production **Release**

January 2015

Production release has been published and
mass installation started to country wide

Central Information System

March 2015

CIS go live to keep tracks
of every installed Gibux release

Fully **Operational**

January 2018

Finished deployments in country wide

AD to Samba...

Project **Requirements**

Forest **Structure**

Need to support hybrid structure with Microsoft AD, work as a part of forest.

ACL Support

Every user must have his/her private and public directory to keep files safe and share if necessary

Local DNS Support

Every site must have a local DNS infrastructure to use local resources.

DHCP & TFTP **Support**

Every Samba server must support DHCP and TFTP to handle Gibux machines and PXE installation.

Easy Management

Site technicians must take care of local user requirements.

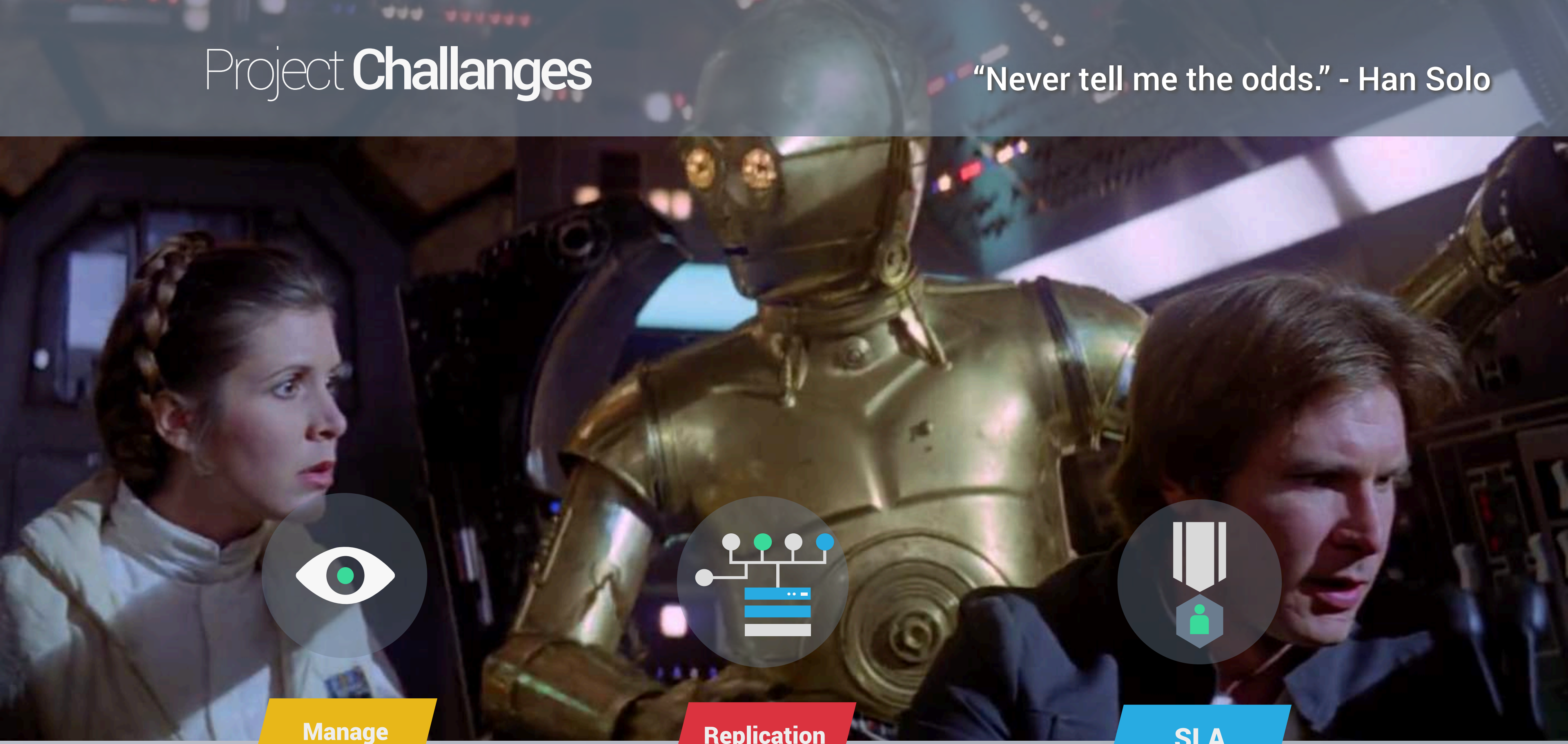
Automated **Migration**

Current data on Microsoft AD must be easily migrated by local technicians.

> **"Do or do not, there is no try."**
>
> *Master Yoda*

Project Challanges

“Never tell me the odds.” - Han Solo



Manage

Web Based Management

1. Need local web based management services like **Samba**, **BindDNS**, **TFTP**, **SaltStack**

2. Central Management for all servers

Replication

Max 15 min

Every server must complete the replication in 15 minutes NTDS management must be managed centrally

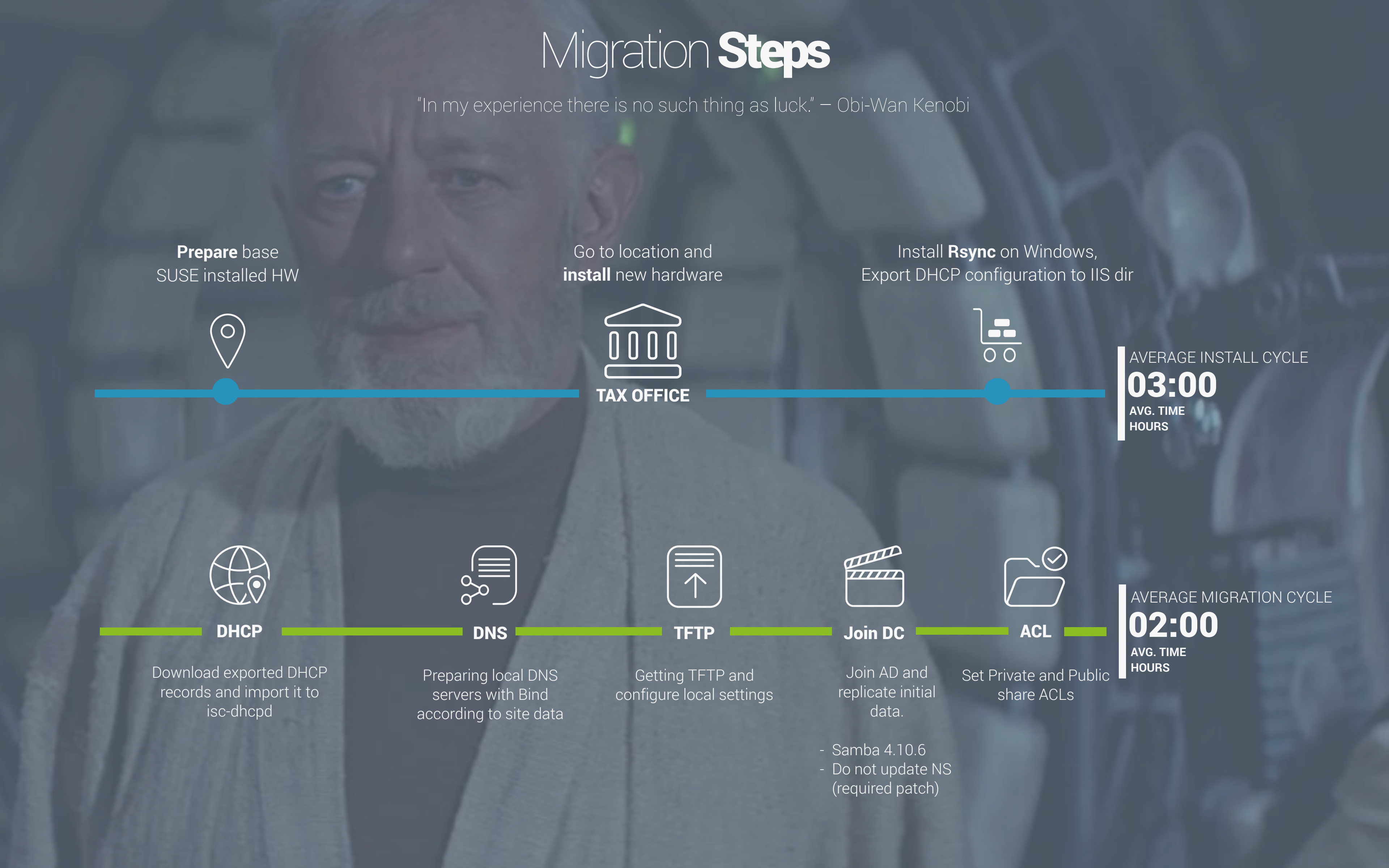
SLA

Max 15 min.

In working hours there is no tolerance of failure. If any problem occures you have to respond in 15 minutes. Transactions must continue and problem has to be solved in 1 hour.

Migration **Steps**

“In my experience there is no such thing as luck.” – Obi-Wan Kenobi



Prepare base
SUSE installed HW

Go to location and
install new hardware

TAX OFFICE

Install **Rsync** on Windows,
Export DHCP configuration to IIS dir

AVERAGE INSTALL CYCLE
03:00
AVG. TIME
HOURS

DHCP

Download exported DHCP records and import it to isc-dhcpd

DNS

Preparing local DNS servers with Bind according to site data

TFTP

Getting TFTP and configure local settings

Join DC

Join AD and replicate initial data.

- Samba 4.10.6
- Do not update NS (required patch)

ACL

Set Private and Public share ACLs

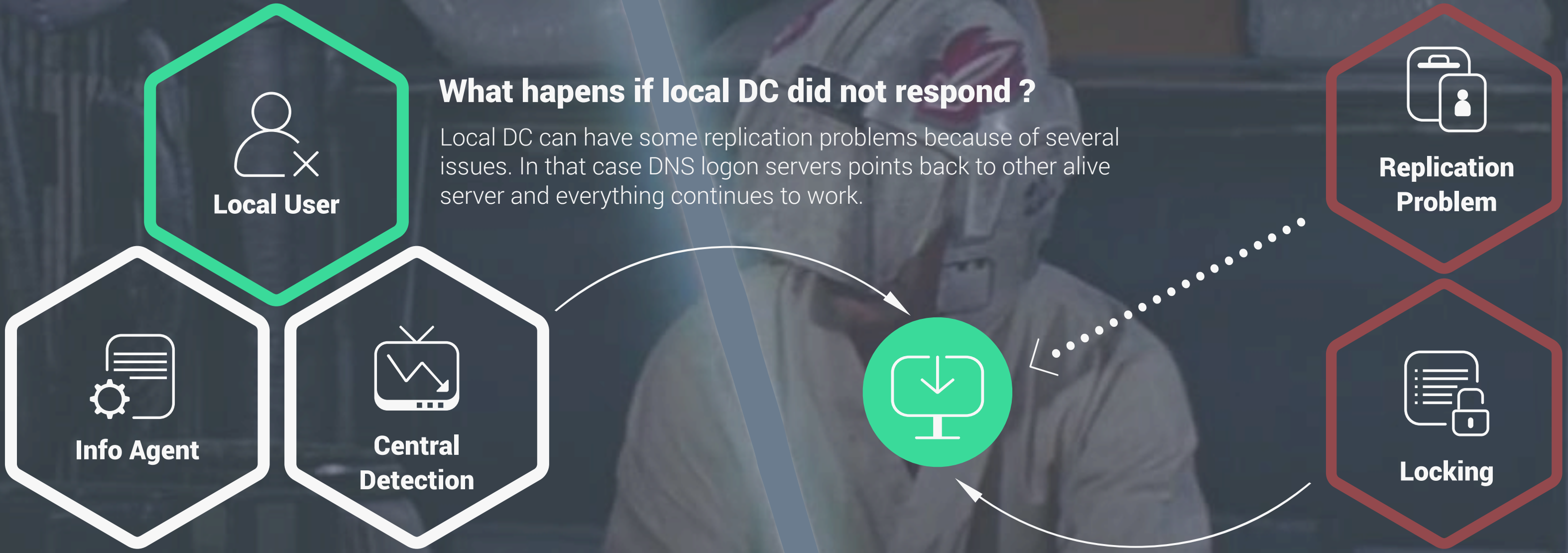
AVERAGE MIGRATION CYCLE
02:00
AVG. TIME
HOURS

What if a **problem** occures or **replication** breaks

"Your eyes can deceive you. Don't trust them." – Obi-Wan Kenobi

What hapens if local DC did not respond ?

Local DC can have some replication problems because of several issues. In that case DNS logon servers points back to other alive server and everything continues to work.



Local User

Info Agent

Central Detection

Replication Problem

Locking

What is **check-list** before join

"Somebody has to save our skins." – Leia Organa

Network

Check latency on WAN

If you will open your network on WAN, latency is very important. You need to arrange kernel parameters and NTDS

DNS

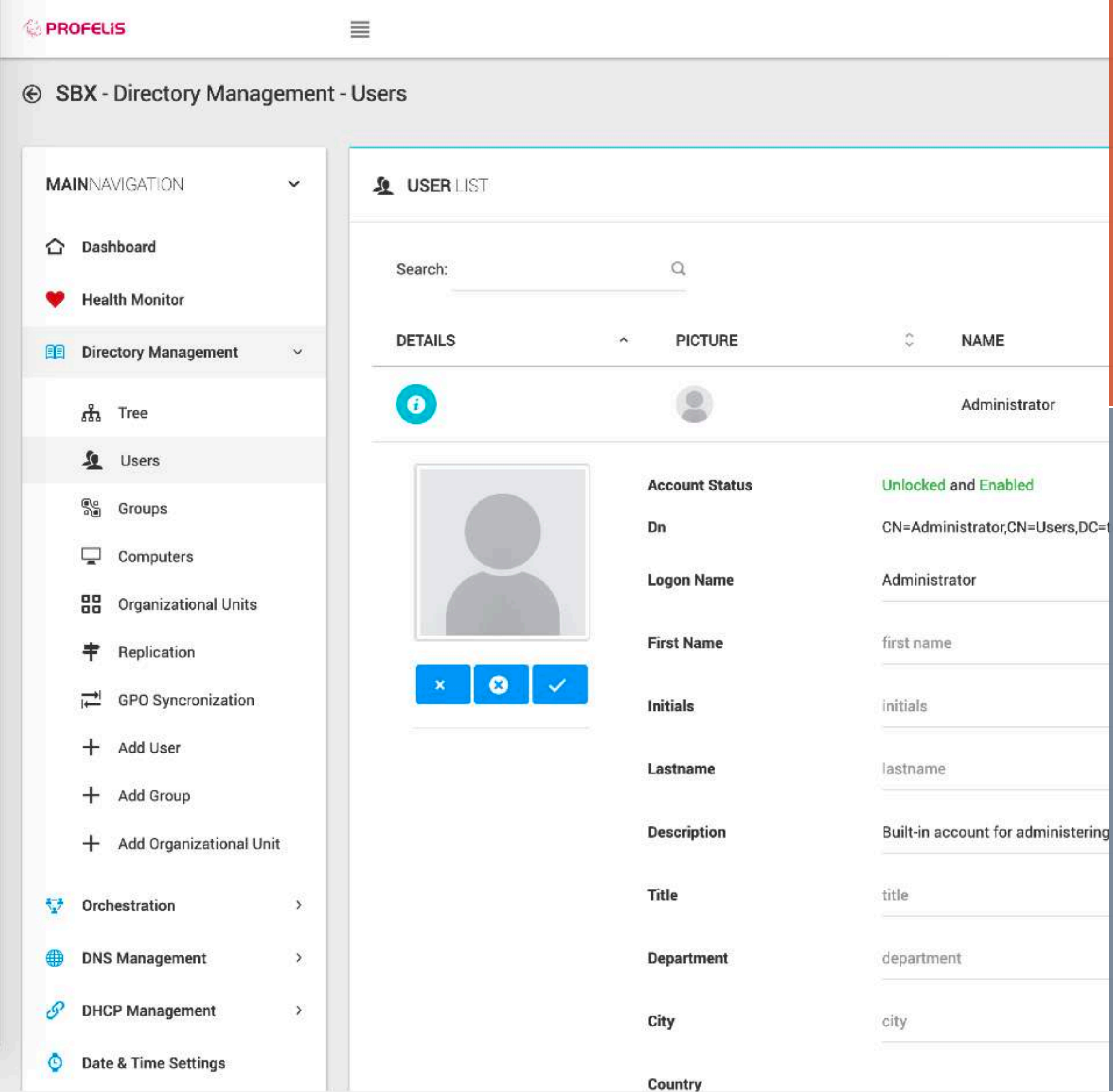
Old DNS records are pain

DNS is very important part of Directory Server. Old datas, removed zones cause resolution problems which also triggers replication problems.

Metadata

Old objects, huge problems

Uncleaned metadata objects cause replication problems. If you need to use an IP which used by demoted server you must clean metadata



SBX - Directory Management - Users

DETAILS	PICTURE	NAME	DESCRIPTION
i		Administrator	Built-in account for administering the computer/domain

Account Status: Unlocked and Enabled

Dn: CN=Administrator,CN=Users,DC=testdomain,DC=com

Logon Name: Administrator

First Name: first name

Initials: initials

Lastname: lastname

Description: Built-in account for administering the computer/domain

Title: title

Department: department

City: city

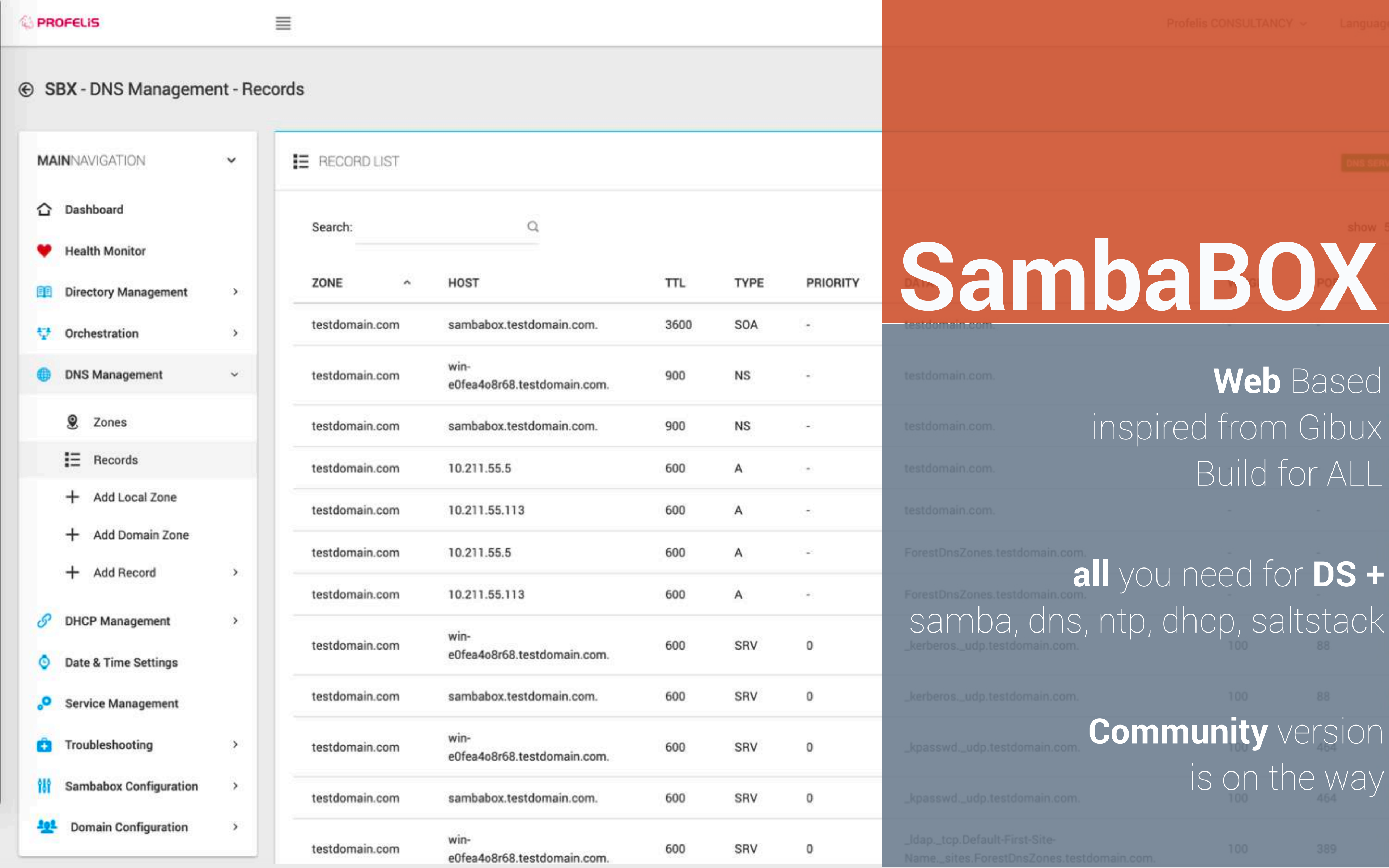
Country

SambaBOX

Web Based
inspired from Gibux
Build for ALL

all you need for **DS +**
samba, dns, ntp, dhcp, saltstack

Community version
is on the way



PROFELIS

Profelis CONSULTANCY

Languag

SBX - DNS Management - Records

MAIN NAVIGATION

- Dashboard
- Health Monitor
- Directory Management
- Orchestration
- DNS Management
  - Zones
  - Records
  - Add Local Zone
  - Add Domain Zone
  - Add Record
- DHCP Management
- Date & Time Settings
- Service Management
- Troubleshooting
- Sambabox Configuration
- Domain Configuration

RECORD LIST

DNS SERV

Search:

show 5

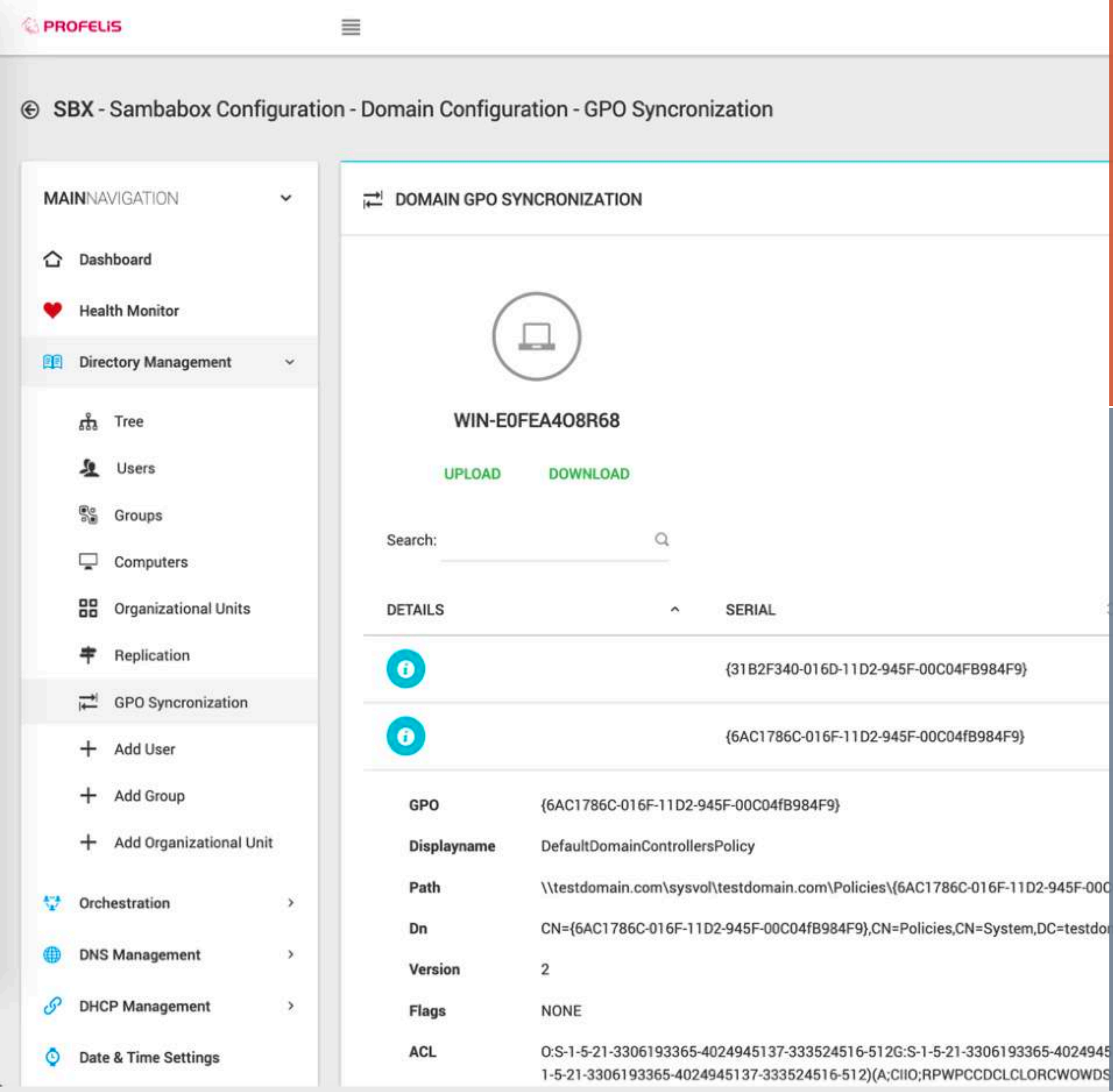
ZONE	HOST	TTL	TYPE	PRIORITY	DATA		
testdomain.com	sambabox.testdomain.com.	3600	SOA	-	testdomain.com.	-	-
testdomain.com	win-e0fea4o8r68.testdomain.com.	900	NS	-	testdomain.com.		
testdomain.com	sambabox.testdomain.com.	900	NS	-	testdomain.com.		
testdomain.com	10.211.55.5	600	A	-	testdomain.com.		
testdomain.com	10.211.55.113	600	A	-	testdomain.com.	-	-
testdomain.com	10.211.55.5	600	A	-	ForestDnsZones.testdomain.com.	-	-
testdomain.com	10.211.55.113	600	A	-	ForestDnsZones.testdomain.com.	-	-
testdomain.com	win-e0fea4o8r68.testdomain.com.	600	SRV	0	_kerberos._udp.testdomain.com.	100	88
testdomain.com	sambabox.testdomain.com.	600	SRV	0	_kerberos._udp.testdomain.com.	100	88
testdomain.com	win-e0fea4o8r68.testdomain.com.	600	SRV	0	_kpasswd._udp.testdomain.com.	100	464
testdomain.com	sambabox.testdomain.com.	600	SRV	0	_kpasswd._udp.testdomain.com.	100	464
testdomain.com	win-e0fea4o8r68.testdomain.com.	600	SRV	0	_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.testdomain.com.	100	389

SambaBOX

Web Based
inspired from Gibux
Build for ALL

all you need for **DS +**
samba, dns, ntp, dhcp, saltstack

Community version
is on the way



PROFELIS

SBX - Sambabox Configuration - Domain Configuration - GPO Syncronization

MAIN NAVIGATION

- Dashboard
- Health Monitor
- Directory Management
  - Tree
  - Users
  - Groups
  - Computers
  - Organizational Units
  - Replication
  - GPO Syncronization
  - Add User
  - Add Group
  - Add Organizational Unit
- Orchestration
- DNS Management
- DHCP Management
- Date & Time Settings

DOMAIN GPO SYNCRONIZATION

WIN-E0FEA4O8R68

UPLOAD DOWNLOAD

Search:

DETAILS	SERIAL	DISPLAY NAME	LOCAL STATUS
ⓘ	{31B2F340-016D-11D2-945F-00C04FB984F9}	Default Domain Policy	EXISTS
ⓘ	{6AC1786C-016F-11D2-945F-00C04fB984F9}	Default Domain Controllers Policy	

GPO	{6AC1786C-016F-11D2-945F-00C04fB984F9}
Displayname	DefaultDomainControllersPolicy
Path	\\testdomain.com\sysvol\testdomain.com\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}
Dn	CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System,DC=testdomain,DC=com
Version	2
Flags	NONE
ACL	O:S-1-5-21-3306193365-4024945137-333524516-512G:S-1-5-21-3306193365-4024945137-333524516-512D:PAI(A;;RPWPCCLCLORCWOWDSW;;;S-1-5-21-3306193365-4024945137-333524516-512)(A;CIIO;RPWPCCDCLCLORCWOWDSDDTSW;;;S-1-5-21-3306193365-4024945137-333524516-512)(A;;RPWPCCLCLORCWOWDSW;;;S

SambaBOX

Web Based
inspired from Gibux
Build for ALL

all you need for **DS +**
samba, dns, ntp, dhcp, saltstack

Community version
is on the way

> “**Time** exists in order that everything doesn’t happen all at once… and **space** exists so that it doesn’t all happen to you.”

Susan Sontag

Do you **need help**?

Read **wiki:** wiki.samba.org

man

Mail **Lists**

Read **T**he **F**ine **M**anual

samba.org/samba/docs

SerNET

Samba +

lists.samba.org

bugzilla.samba.org

debug samba

gitlab.com/samba-team/samba/

Catalyst

Google

Microsoft

samba.org/samba/support

Git

HUGE **thank you!** to SAMBA TEAM

https://www.samba.org/samba/team/

May the force be with you!

Question

Thank **YOU**

?

SambaXP 2020

PROFELIS

www.profelis.com.tr
sambabox.profelis.com.tr

* All StarWars images are sourced at www.StarWars.com