ADUCID Server Kit Installation Guide

Version 3.0.4

Release date February 1, 2016

Antala Staška 2027/79, 140 00 Prague 4 | T +420 271 100 100 | F +420 271 100 101
Vídeňská 125, 619 00 Brno | T +420 547 100 100 | F +420 547 100 101
Sady 5. května 59, 301 00 Pilsen | T +420 271 100 100 | F +420 271 100 101
Teslova 30, 821 02 Bratislava | T +421 (2) 4821 3111 | F +421 (2) 4821 3199

ISO 9001 ISO 14001 ISO/IEC 27001 ISO/IEC 20000
CZ > Corp. ID 25313029 | Registration Court RC Brno, File no. B2113
SK > Corp. ID 35787546 | Commercial Register DC Bratislava, Section Sa file 2431/B

Table of Contents

1. Introduction

The ADUCID Server Kit - Installation Guide provides information on how to prepare the environment for installing ADUCID Server Kit.

Specific contents:

- Deployment scenarios, network configuration
- Import to VMWare infrastructure
- System configuration
- Initial startup

The reader of this document is assumed to have administrator-level knowledge of the Linux operating system.

2. System requirements

Requirement	Description
VMware	VMware ESX 4 or later
RAM	Minimum 512 MB RAM for the ADUCID Server Kit virtual machine; recommended 2 GB RAM
CPU	Minimum 1 x 200 MHz CPU; recommended 2 x 2 GHz CPU

Table 2-1 ADUCID Server Kit hardware requirements

3. Implementing ADUCID Server Kit into your network infrastructure

3.1. Inbound communication

Port	Description
22/ssh (TCP)	Port for ssh access for remote administration
80/http (TCP)	ADUCID/Apache HTTP Server
443/https (TCP)	ADUCID/Apache HTTP Server
636/ldaps (TCP)	Port for LDAP replication

Table 3-1 ADUCID Server Kit inbound communication requirements

3.2. Outbound communication

With default settings, you do not need to enable outbound communication. To function properly, ADUCID Server Kit needs the TCP/IP protocols listed in the following table.

Port	Description
636/ldaps (TCP)	Port for LDAP replication (between individual cluster nodes)
123/ntp (UDP)	Time synchronization (only if the ntpd service is enabled)
53/domain (TCP/UDP)	DNS

Table 3-2 ADUCID Server Kit outbound communication requirements

3.3. Deployment diagram - one node

Basic components are shown on the picture below. Inbound communication is enabled on the Apache HTTP Server. It terminates SSL (for HTTPS connection) and filters queries for the R3 and R4 interfaces.

Apache Tomcat is runtime environment for the AIM, UIM and AIM-proxy components of ADUCID.

OpenLDAP is a database of identities, personal information and selected configuration parameters of the ADUCID system.

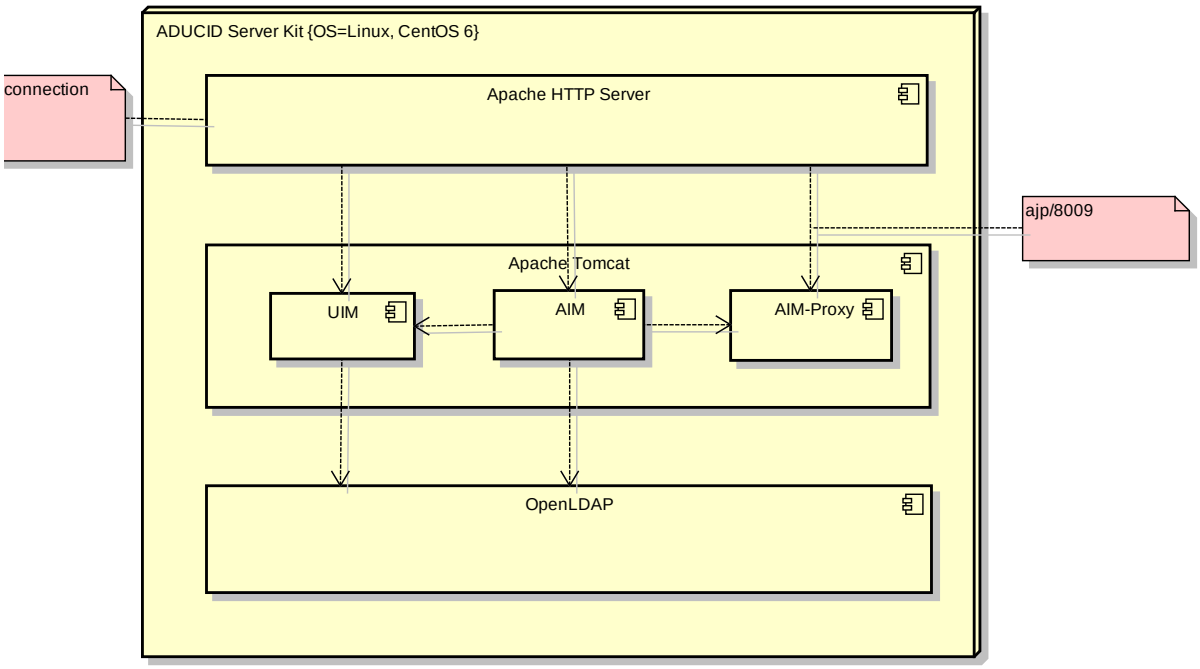

Figure 3-1 Deployment - one node

3.4. Deployment diagram - cluster

ADUCID infrastructure allows high availability deployment. ADUCID configurator directly supports two-node cluster deployment. This type of deployment supports workload distribution. The balancer must route all traffic to a single functional node.

It is possible to build an infrastructure with multiple nodes and load balancing. It depends on the implementation and balancer type. This solution, however, is not supported by the ADUCID configurator.

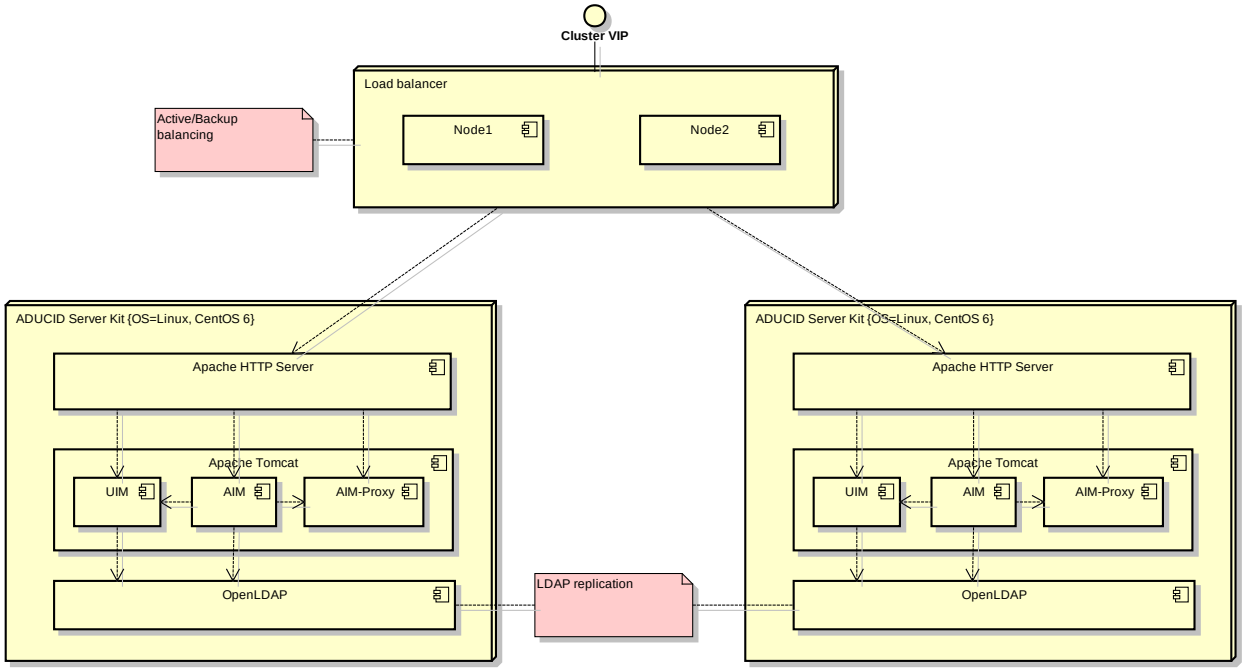

Figure 3-2 Deployment - multiple nodes

4. Importing VM into your virtual infrastructure

First, you need to import the virtual machine into the VMware infrastructure. This can be done in multiple ways. For example, you can use VMware vCenter Converter Standalone.

- Run „`VMware vSphere Client`“
- Choose `File > Deploy OVF Template`, the application wizard appears
  - Choose the virtual machine from the DVD (vm\orangebox*.ova)
  - Set the name for the new virtual machine
  - Set the location for the new virtual machine

4.1. Verifying import

After the import has finished, new virtual machine appears in the list of virtual machines. Verify its existence using VMware vSphere Client. Connect to the vCenter server. The virtual machine must be included in the list of virtual machines.

5. Initial startup of the virtual machine

For the initial startup, you need access to the virtual machine’s console. Once the VM has started, you can log in to ADUCID Server Kit only from the console. **No password** is set for the “root” user.

After you log in, follow these steps:

- Set the password for the “root” user.
- Create an account for remote access.
- Set the time zone and time.
- Set the system network.
  - Configure the network interface (address, network mask, default gateway).
  - Specify a hostname
  - Specify DNS servers (/etc/resolv.conf)

- Type the hostname and domain name into /etc/hosts, for example:

```
10.0.0.1 orangebox orangebox.example.com
```

- For cluster deployments, we also recommend to specify the address of the second cluster in the /etc/hosts file.
- Connect the virtual machine's network adapter to the appropriate virtual switch. In the network adapter settings, set the adapter as connected, and also to connect at power-on of the VM.

5.1. Verifying network connectivity

Connectivity can be verified using the ping program. Ping a server name to verify both connectivity and DNS resolution. Ping a server address outside the network where the ADUCID Server Kit is located (e.g. ping www.google.com).

6. Adding ADUCID Server Kit to DNS

The server (or servers) must be added to DNS. Verify that resolution works both ways (forward and reverse), e.g. using nslookup or dig.

7. System update

Operating system is now functional. System already includes all updates available at the time of release. Installing new system updates is recommended. If the server is connected to the internet via a proxy server, set the following commands for the proxy:

```
export http_proxy=http://proxy.example.com:3128
export https_proxy=http://proxy.example.com:3128
export ftp_proxy=http://proxy.example.com:3128
```

Update using the following command:

```
yum -y update
```

If an update affects any key components, like core or glibc, we suggest that you restart the system after the update has finished.

After the system core has been updated and the system restarted, vmware-tools must be re-configured.

```
vmware-config-tools.pl
```

8. Time synchronization

In order for ADUCID to function properly, the correct time must be set in the system. Use the "date" command to verify the system time. In the OS, set the synchronization either using VMware or NTP.

Time does not need to be accurate. The ADUCID proprietary technology does not critically depend on accurate time. Regardless, we recommend that time is set with a ±30 s accuracy, which can be achieved using either of the methods suggested above.

9. Certificates for SSL

ADUCID Server Kit uses certificates for single-purpose point-to-point encryption only. Certificates do not need to be signed by a CA to function properly, you can use self-signed certificates. You will need two certificates - one for the httpd apache, and one for the ldap server.

The certificates are located in the `/etc/pki/tls/certs` directory. To generate a certificate, run the "make" command in this directory with the "file name" as parameter. The file extension must be "pem".

When creating a certificate, the "Common Name" is the most important item. Common Name must correspond to the server's domain name. For cluster installations, the HTTP server certificate must contain a DNS name that resolves to a virtual address in the balancer. A certificate for OpenLDAP always contains a DNS name of the given node.

Instructions for the apache certificate:

```
cd /etc/pki/tls/certs
/bin/rm -f httpd.pem
make httpd.pem
```

You do not need to edit the configuration of the mod_ssl module of the Apache HTTPD server. Open the /etc/httpd/conf.d/ssl.conf configuration file. Edit the SSLCertificateFile and SSLCertificateKeyFile parameters to point to the newly created certificate file.

```
SSLCertificateFile /etc/pki/tls/certs/httpd.pem
SSLCertificateKeyFile /etc/pki/tls/certs/httpd.pem
```

Instructions for the ldap certificate:

```
cd /etc/pki/tls/certs
/bin/rm -f slapd.pem
make slapd.pem
chown ldap:ldap slapd.pem
```

10. ADUCID configuration

Now you have a working server connected to the network. You can start configuring ADUCID.

- First installation step is to prepare the AIM server operator's icon. The icon is displayed on the PEIG and is an important element for a visual user check. Copy your icon to the `/usr/share/pixmaps` directory. The icon must be in the PNG format, the minimum size is 48 x 48 pixels. Set the file ownership to user "root" and access mode to 644.
- We recommend installing a default icon for the Apache HTTPd server as well. You can use the same icon as in the previous step. Copy it to the `/var/www/html` folder and rename to favicon.ico. Set the file ownership to user "root" and access mode to 644.
- Log in to ADUCID Server Kit as the "root" user.
- We recommend setting a value for the `ServerAdmin` and `ServerName` parameter in the `/etc/httpd/conf/httpd.conf` file.
- Insert the DVD (e.g. mount the ISO image or mount a local DVD drive).
- Mount the /dev/cdrom into /media/ADUCID (`mount /dev/cdrom /media/ADUCID`).
  - Run `aducid-configurator`.
    - Set parameters for ADUCID Server Kit.
    - AIM host – a DNS name corresponding to a location where ADUCID is available (e.g. orangebox.example.com). For a cluster installation, a DNS name that points to a virtual address in the load balancer is specified here.

- SPID - unique identifier that identifies ADUCID as identity provider. This string must be globally unique. Therefore we recommend using the DNS name for SPID. For clusters, all nodes must have the same SPID.
- Display Name - the name that displays on PEIG when used with the installed AIM server. It is recommended to set this property to your organization's name. For a cluster installation, all nodes should be set to the same value.
- Internal network - the R4 interface of the UIM application will be available from this network. This interface is used for communication between the server part of the application and the AIM application. It should not be freely accessible from the internet. You can choose an internal network address, DMZ address or address of a particular server, etc.
- UIM - install the UIM component (recommended) - UIM (User Identity Management) is a web application for ADUCID management and simple user administration. In some deployment scenarios, it might be more appropriate to deploy UIM on a different server than AIM. In such a case, do not install UIM.
- AIM-proxy - install the AIM-proxy component (recommended) - a component that enables ADUCID to log in to the UIM without modifying the browser (redirect login). This component is mandatory if UIM is installed.
- LDAP Base dn - base DN of ADUCID's internal LDAP. We recommend using your organization's domain. The setting is important for potential integration with the organization's LDAP.
- Password - the password for the system account used by the AIM and UIM components to access the LDAP database. If the password is not set, a random password will be generated. For cluster installations, identical passwords must be set for both nodes. If you let the system generate a random password for the first node, get its value in the /etc/tomcat6/ADUCID.properties file and apply for the second node.
- Icon - the path to the icon that you copied earlier to the /usr/share/pixmaps directory.
- Cluster - specifies whether the installation is a cluster installation.
  - *This Node Id - cluster node number - install node 1 first.*
  - *Second Node - the opposite cluster node address. Specify a fully qualified DNS name here.*
  - *Replication password - a password for the technical account that is used for LDAP replication. Must be identical for both cluster nodes.*
- Click Apply and wait for the installation to finish.
- Unmount the CD.

After installation is complete, your settings are stored in the "~/.aducid-setup" file. Settings will be reloaded when the configurator starts next time. The file contains sensitive information. **We recommend deleting it** before the server starts working in production mode.

Installation progress is captured in the ~/aducid-install.log file. Deleting the file before the server starts working in production mode is also recommended.

10.1. Verifying the installation

We recommend verifying AIM functionality after installation. Use your browser to access the following URLs:

- http://orangebox.example.com/UIM/version
- http://orangebox.example.com/AIM/version
- http://orangebox.example.com/AIM-proxy/version

The browser will display a simple text page with version information for each component.

If the pages show a version number, you can access the UIM application's address:

- http://orangebox.example.com/UIM/

If PEIG is disabled, a UIM application page will show and you will be asked to enable PEIG.

You can verify whether the cluster has been installed properly by reviewing the LDAP database on the second node. If all is functioning properly, synchronization will be performed within a few seconds after slapd service starts. LDAP objects on the first node will also display on the second node. You can verify this by running the "slapcat" command on the second node.

11. Notes and abbreviations

Below is a summary of abbreviations used in the document, and their meaning:

ADUCID®

ADUCID® is a new authentication system providing electronic identity services and infrastructures. Based on new ideas, rules, procedures and implementations, ADUCID® establishes an identification and authentication framework, within which a unified authentication method can function and be supported.

The main purpose of ADUCID® is to provide identification and authentication services in the cybernetic world of ICT systems using the ADUCID® secure authentication layer.

ADUCID® provides:

- Electronic identity services
- Secure authentication services
- Essential infrastructure for these services

PEIG®

PEIG® (Personal Electronic Identity Guardian) is a device that can fully manage electronic identities of its user. Under the user identity it also provides automatic authentication between the client application (used by the user) and the server part of the target application (that the user is accessing).

AIM

ADUCID Identity Machine - implements ADUCID server functionality. It performs all ADUCID operations and provides access to user data stored along with electronic identities in the LDAP database.

Using standard network interface (web services), it provides target applications with services related to identity administration. AIM contains administrator and user graphic interface (called UIM). AIM can also provide authorization services (including administration of authorization attributes of the relevant identities).

UIM Graphic administrator interface for AIM

DN Distinguished Name

DNS Domain Name System

LDAP Lightweight Directory Access Protocol

NTP Network Time Protocol

OS Operating System

CA Certification Authority

VM Virtual Machine

12. Literature

[1] *ADUCID Architecture*

[2] *ADUCID Integration Manual*

[3] *ADUCID Server Kit – Administration Guide*

