ALSID FOR ACTIVE DIRECTORY
INSTALLATION PROCEDURE

1. Document contributors:

<table>
<thead>
<tr>
<th>Author</th>
<th>Qualification</th>
<th>Contact address</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALSID</td>
<td>DevOps team</td>
<td><a href="mailto:support@alsid.com">support@alsid.com</a></td>
</tr>
</tbody>
</table>

2. Document history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date (dd/mm/yyyy)</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4.0</td>
<td>12/07/2019</td>
<td>ALSID</td>
<td>Initial document</td>
</tr>
<tr>
<td>2.5.0</td>
<td>23/10/2019</td>
<td>ALSID</td>
<td>Update for 2.5.0</td>
</tr>
<tr>
<td>2.5.3</td>
<td>19/12/2019</td>
<td>ALSID</td>
<td>Use InitDbSize</td>
</tr>
<tr>
<td>2.6.0</td>
<td>21/02/2020</td>
<td>ALSID</td>
<td>Update for 2.6.0</td>
</tr>
<tr>
<td>2.6.1</td>
<td>05/03/2020</td>
<td>ALSID</td>
<td>Update for 2.6.1</td>
</tr>
<tr>
<td>2.6.3</td>
<td>04/04/2020</td>
<td>ALSID</td>
<td>Update for 2.6.3</td>
</tr>
<tr>
<td>2.7.0</td>
<td>06/06/2020</td>
<td>ALSID</td>
<td>Update for 2.7.0</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS

I. **Introduction** ......................................................................................................................... 3
   1. Document objectives ........................................................................................................... 3
   2. Abbreviations ................................................................................................................... 3
   3. Infrastructure presentation ............................................................................................... 3
      3.1. Network Overview ....................................................................................................... 3
      3.2. Recommended architectures ....................................................................................... 6
      3.3. Meta-Kapteyn architecture (optional) ........................................................................... 8
      3.4. Installation log file ...................................................................................................... 8
   4. Prerequisites ...................................................................................................................... 8
      4.1. Minimal configuration ................................................................................................. 8
      4.2. Supported context ......................................................................................................... 9
      4.3. Binaries ....................................................................................................................... 9

II. **Installation** ...................................................................................................................... 11
   1. Install Storage Manager .................................................................................................... 11
   2. Install Security Engine Node ............................................................................................ 13
      2.1. One machine ............................................................................................................... 13
      2.2. Four machines ............................................................................................................ 16
   3. Install Directory Listener .................................................................................................. 23
   4. Access to specific Active Directory objects or containers ................................................. 25

III. **Annexes** ........................................................................................................................... 26
   1. How to change IIS certificate for AlsidForAD Web Application ........................................ 26
   2. Meta-Kapteyn configuration file ....................................................................................... 31
   3. How to back up Storage Manager .................................................................................... 32
      3.1. InfluxDB ..................................................................................................................... 32
      3.2. MSSQL ....................................................................................................................... 32
   4. Expert Mode for Directory Listener ................................................................................. 33
      4.1. Additional subnets for Ceti ......................................................................................... 33
   5. What is a complex password? ........................................................................................... 33
   6. How to horizontally scale up/down services to improve data processing performance? ...... 34
      6.1. Scale Up ..................................................................................................................... 34
1. INTRODUCTION

1. Document objectives

This document is intended to help you perform a clean installation of ALSID’s on-premise solution. Each component is made of one server:

- A Directory Listener targeting audited domains,
- A Security Engine Node also acting as a Control Plane,
- A Storage Manager hosting all data, based on MSSQL and InfluxDB.

Note: For many examples, the “E” partition letter will be used by default for data partition.

2. Abbreviations

The following table lists the abbreviations used in this documentation:

<table>
<thead>
<tr>
<th>Abbr.</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DL / DLxx</td>
<td>Directory Listener</td>
</tr>
<tr>
<td>SEN / SENxx</td>
<td>Security Engine Node</td>
</tr>
<tr>
<td>DB / DBxx</td>
<td>Storage Manager</td>
</tr>
<tr>
<td>WI / Wixx</td>
<td>Web Interface, or any application offering a website</td>
</tr>
<tr>
<td>PC / PCxx</td>
<td>Personal Computer, or devices used as a computer</td>
</tr>
<tr>
<td>CP / CPxx</td>
<td>Control Plane (also referred as Web Interface)</td>
</tr>
<tr>
<td>IoE / IoExx</td>
<td>Indicator of Exposure</td>
</tr>
<tr>
<td>DC / DCxx</td>
<td>Domain Controller</td>
</tr>
</tbody>
</table>

3. Infrastructure presentation

The following information is provided as a referral for this document. The infrastructure presented here must be considered as a supported architecture.

3.1. Network Overview

The network is spliced across three areas. The following schema shows an overview of the network communication:

![Network Overview Diagram](image)

Figure 1: Network overview

To go further, please read the following schema and its associated network matrix. They describe each required protocol and port used by Alsid’s platform:
The following network matrix describes each required protocol and port used by Alsid’s platform.

<table>
<thead>
<tr>
<th>Network flows (From -&gt; To)</th>
<th>Alsid’s usage</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Alsid’s Directory Listeners -&gt; Domain controllers</td>
<td>Directory, Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636 ICMP/echo-request ICMP/echo-response</td>
</tr>
<tr>
<td></td>
<td>User and Computer Authentication, Forest Level Trusts</td>
<td>Kerberos</td>
<td>TCP/88, TCP/464 and UDP/464</td>
</tr>
<tr>
<td></td>
<td>User and Computer Authentication, Name Resolution, Trusts</td>
<td>DNS</td>
<td>UDP/53 and TCP/53</td>
</tr>
<tr>
<td></td>
<td>Replication, User and Computer Authentication, Group Policy, Trusts</td>
<td>RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS</td>
<td>TCP Dynamic (&gt; 1024)</td>
</tr>
<tr>
<td></td>
<td>Directory, Replication, User and Computer</td>
<td>Global Catalog</td>
<td>TCP/3268 and TCP/3269</td>
</tr>
<tr>
<td>Network flows (From -&gt; To)</td>
<td>Alsid’s usage</td>
<td>Type of traffic</td>
<td>Protocol and Port</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Authentication, Group Policy, Trusts</td>
<td>Replication</td>
<td>RPC Endpoint Mapper</td>
<td>TCP/135</td>
</tr>
<tr>
<td>Alsid’s Directory Listeners -&gt; Alsid’s Security engine nodes</td>
<td>Alsid’s communication bus</td>
<td>Advanced Message Queuing Protocol</td>
<td>TCP/5671 and TCP/5672</td>
</tr>
<tr>
<td>Alsid’s internal API flows (Optional)</td>
<td></td>
<td>TL/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>End-users -&gt; Alsid’s Security engine nodes</td>
<td>Alsid’s end-user services (Web portal, REST API, etc.)</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td>Alsid’s platform -&gt; Support services</td>
<td>Time synchronization</td>
<td>NTP</td>
<td>UDP/123</td>
</tr>
<tr>
<td></td>
<td>Update infrastructure (e.g., WSUS or SCCM)</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td>PKI infrastructure</td>
<td>HTTP/HTTPS</td>
<td>TCP/80 or TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider SAML server</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
<tr>
<td></td>
<td>Identity provider LDAP</td>
<td>LDAP/LDAPS</td>
<td>TCP/389 and TCP/636</td>
</tr>
<tr>
<td></td>
<td>Identity provider OAuth</td>
<td>TLS/HTTP</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>
In addition to the Active Directory protocols, some additional flows may be required depending on Alsid’s platform configuration. These protocols and ports need to be opened between Alsid’s platform and the targeted service.

<table>
<thead>
<tr>
<th>Network flows (From &lt;-&gt; To)</th>
<th>Alsid’s usage (optional)</th>
<th>Type of traffic</th>
<th>Protocol and Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alsid’s Security engine nodes &lt;-&gt; Cybersecurity services</td>
<td>Alsid Web Application</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td>5</td>
<td>Email notifications</td>
<td>SMTP</td>
<td>TCP/25, TCP/587, TCP/465, TCP/2525, TCP/25025 (depending on the SMTP server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Syslog notifications</td>
<td>Syslog</td>
<td>TCP/601, TCP/6515, UDP/514 (depending on the event log server’s configuration)</td>
</tr>
<tr>
<td></td>
<td>Alsid REST API</td>
<td>HTTP/TLS</td>
<td>TCP/443</td>
</tr>
<tr>
<td>Alsid’s Security engine nodes &lt;-&gt; Alsd’s Storage Manager</td>
<td>MSSQL Server database access</td>
<td>MSSQL queries</td>
<td>TCP/1433</td>
</tr>
<tr>
<td>6</td>
<td>InfluxDB Server access</td>
<td>InfluxDB queries over HTTP</td>
<td>TCP/8086</td>
</tr>
</tbody>
</table>

3.2. Recommended architectures

The application runs through many engines that are divided across multiple machines. The power we need depends on the AD activity traffic, which is hard to estimate before deploying. Most of the time, it can be correlated with the number of active users in the AD.

Under 300,000 active users, we recommend using a three-server architecture. Each server has one or more services, and each server must be considered as an independent entity.
Figure 3: Standard architecture

If there are more than 300,000 active users, these three servers will be overloaded, and performance will be insufficient. Security Engine Node needs to be split into four machines.

Figure 4: Extended infrastructure

For more information about the hardware specification, please refer to *Minimal configuration* on page 8.
3.3. Meta-Kapteyn architecture (optional)

For example, let’s consider a group which is in Europe and has a subsidiary in North America. They are not directly connected and there is no trust relationship between their Active Directory domains. Meta-Kapteyn can be used as a consolidation platform to display both dashboards of Europe and North America instances on a single page.

This feature is optional and is not required for the analysis.

For more information, please refer to Meta-Kapteyn configuration file on page 31 and contact support@alsid.com.

3.4. Installation log file

If the installer cannot install Alsid for AD on a machine, please forward us the log file to our support address (support@alsid.com). This file is in your %temp% folder and its name is always starting with “MSI” followed by random numbers. For example: MSI165931.LOG.

4. Prerequisites

4.1. Minimal configuration

The Alsid_for_AD_On-Premise_technical_prerequisites_vX.X document describes the sizing requirements to run the solution. Running AlsidForAD on a configuration thinner than these prerequisites is not supported.

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>2 cores, at least 2.6 GHz</td>
<td>12 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>4 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>30 GB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>2 Virtual Machines</td>
<td>8 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>30 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>200 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>16 GB of RAM</td>
<td>300 GB</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
<td>1 Virtual Machine</td>
<td>10 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>300 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>400 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>16 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>400 GB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>500 GB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>4 Virtual Machines</td>
<td>VM1: 8 cores, at least 2.6 GHz</td>
<td>VM1: 16 GB of RAM</td>
<td>VM1: 1 TB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM2: 12 cores, at least 2.6 GHz</td>
<td>VM2: 32 GB of RAM</td>
<td>VM2: 300 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM3: 8 cores, at least 2.6 GHz</td>
<td>VM3: 16 GB of RAM</td>
<td>VM3: 100 GB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VM4: 16 cores, at least 2.6 GHz</td>
<td>VM4: 32 GB of RAM</td>
<td>VM4: 100 GB</td>
</tr>
</tbody>
</table>
### Storage managers - Sizing Matrix

<table>
<thead>
<tr>
<th>Active AD users</th>
<th>Instance required</th>
<th>vCPU (per instance)</th>
<th>Memory (per instance)</th>
<th>Disk space (per instance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 – 25 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>8 GB of RAM</td>
<td>350 GB</td>
</tr>
<tr>
<td>25 001 – 50 000</td>
<td>1 Virtual Machine</td>
<td>8 cores, at least 2.6 GHz</td>
<td>12 GB of RAM</td>
<td>450 GB</td>
</tr>
<tr>
<td>50 001 – 75 000</td>
<td>1 Virtual Machine</td>
<td>12 cores, at least 2.6 GHz</td>
<td>24 GB of RAM</td>
<td>550 GB</td>
</tr>
<tr>
<td>75 001 – 100 000</td>
<td>1 Virtual Machine</td>
<td>12 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>800 GB</td>
</tr>
<tr>
<td>100 001 – 150 000</td>
<td>1 Virtual Machine</td>
<td>12 cores, at least 2.6 GHz</td>
<td>32 GB of RAM</td>
<td>1 TB</td>
</tr>
<tr>
<td>150 001 – 300 000</td>
<td>1 Virtual Machine</td>
<td>16 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>2 TB</td>
</tr>
<tr>
<td>300 001 – 500 001+</td>
<td>2 Virtual Machine</td>
<td>16 cores, at least 2.6 GHz</td>
<td>64 GB of RAM</td>
<td>3 TB</td>
</tr>
</tbody>
</table>

#### 4.2. Supported context
- AlsidForAD works with Windows Server 2016 with the latest available update.
- AlsidForAD installer requires Local Administrator rights on Windows Server 2016. If the account used for the installation is not the built-in one, make sure that this account can run programs without restrictions.
- AlsidForAD services require Local Administrator rights to run local services on the machine.
- AlsidForAD requires a dedicated data partition. AlsidForAD must not be run on the OS partition to prevent system freeze if the partition is full.
- AlsidForAD SQL instance requires the virtual accounts usage feature.
- AlsidForAD works on a three-tier model. One or two VMs are not supported. At least three VMs and eventually more than one DL are supported. **Exception:** Ceti-TLS mode requires only one VM from a customer point-of-view.
- AlsidForAD must be considered as a black-box: Each machine must be considered as dedicated to the product and must not be shared for another purpose.
- AlsidForAD can create any folder starting with the ‘Alsid’ prefix on the data partition. Therefore, do not create folders starting with ‘Alsid’ on the data partition.
- Erlang known issues: HOMEDRIVE environment variable must not be modified. The PATHEXT environment variable must contains the .EXE and .BAT file extensions.

#### 4.3. Binaries

Alsid for Active Directory installer binary is available on its release portal [https://release.alsid.app](https://release.alsid.app):
- AlsidForAD_v2.X.X.exe

This package contains the files required to perform installation/uninstallation/update and to reconfigure the solution with different IP addresses (if needed).

> It is highly recommended to reboot all machines before starting a new installation.
**Windows Server (Desktop Experience)**

The installer binary must be placed in a valid location on each server to be set up. In the following example, on the Storage Manager machine, we put it on the Desktop:

<table>
<thead>
<tr>
<th>Binaries location</th>
<th>Binaries content</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Users\Administrator\Desktop\</td>
<td><img src="image" alt="Desktop Window" /></td>
</tr>
</tbody>
</table>

- Extended debug logging can be activated with the following command (replace the first path by your executable file location, and the second by your log file path):

```
"C:\Users\Administrator\Desktop\AlsidForAD_2.X.X.exe" /I+V /E:C:\example.log"
```

**Windows Server Core**

The installer GUI can be displayed on a Server Core. Type this command to start the installation:

- Run the following command (replace the path by your executable file location):

```
C:\Users\Administrator\Desktop\AlsidForAD_2.X.X.exe
```
II. INSTALLATION

1. Install Storage Manager

During this step, the process will deliver the following applications:

- InfluxDB
- MSSQL

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

![Welcome dialog on Storage Manager](image)

Figure 5: Welcome dialog on Storage Manager

On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy the **Storage Manager** feature, you must select only this feature.

Once this is done, change the **Location if needed** by editing **ONLY** the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the drive letter is E. Then, click on the “Next” button.
Type a complex password (if you need more details, please refer to What is a complex password? on page 33 for the SQL database. The instance name used is ALSID by default. Change it only if necessary. Otherwise, keep ALSID default instance name and click on the “Next” button. You are now ready to install Alsid for AD.

⚠️ We strongly recommend you keep the default instance name (“ALSID”). If you change it, please refer to the following documentation to use a valid name: https://docs.microsoft.com/en-us/sql-server/install/instance-configuration?view=sql-server-2017

Wait for the end of the installation and click on YES to reboot the server.
If virtual account usage is prohibited on the SQL machine, this step will fail. The MSSQL service can run as NT AUTHORITY\SYSTEM account instead of a virtual account after the installation.

If you are looking for a procedure to back up the Influx and MSSQL databases, please refer to *How to back up Storage Manager* on page 32.

2. Install Security Engine Node

During this step, the process will deliver the following applications:

- Alsid components
  - Cancri
  - Caroli
  - Cephei
  - Ceti-Bridge
  - Corvi
  - Corvi2
  - Cygni
  - Electra
  - Enif
  - Equuleus
  - Eridanis
  - Kaptelyn
  - IIS
  - RabbitMQ

The SEN machine can be split into different machines to improve performance on huge infrastructures.

2.1. One machine

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.
On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy the SecurityEngineNode feature, you must select only this feature.

Once this is done, change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the drive letter is E. Then, click on the “Next” button.

Indicate the Storage Manager’s IP address in the two dedicated fields and type the password of the SQL database that you previously chose. Then, click on the “Next” button.
In order to make Alsid’s web application and services (SAML, SMTP, etc.) available for the end users, please enter the DNS name (preferred) or the IP address the end users will use to access Alsid’s platform.

By default, the installation process creates a self-signed certificate with the DNS name, or the IP typed. If you are willing to change this certificate, please refer to How to change IIS certificate for AlsidForAD Web Application on page 26.

Wait for the end of the installation and click on YES to reboot the server.
2.2. Four machines

The standard architecture for the Alsid for AD on-premises solution is made of three VMs by default. However, if the environment that you are willing to monitor is wider than 300K users, you must consider splitting the SEN into four different machines.

As mentioned in Prerequisites on page 8, it is recommended to use the following architecture for SEN components when three VMs are not enough:

<table>
<thead>
<tr>
<th>Security Engine Nodes - Sizing Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM name</td>
</tr>
<tr>
<td>VM1:</td>
</tr>
<tr>
<td>VM2:</td>
</tr>
<tr>
<td>VM3:</td>
</tr>
<tr>
<td>VM4:</td>
</tr>
</tbody>
</table>
◊ **VM1 - RabbitMQ**

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

![Welcome dialog on Security Engine Node](image1)

Figure 12: Welcome dialog on Security Engine Node (1)

On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy the RabbitMQ feature, you must select only this feature.

Once this is done, change the **Location if needed** by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the drive letter is E. Then, click on the “Next” button and install Alsid for AD.

![Features dialog on Security Engine Node](image2)

Figure 13: Features dialog on Security Engine Node (1)

Wait for the end of the installation and click on **YES** to reboot the server.
VM2 - Node services and Cephei/CetiBridge

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

![Welcome dialog on Security Engine Node (2)](image)

On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy **Node, Cephei** and **CetiBridge**, you must select only these features:

- Cephei
- CetiBridge
- Electra
- Enif
- Equuleus
- Eridanis
- Kapteyn

Once this is done, change the **Location if needed** by editing **ONLY** the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the drive letter is **E**. Then, click on the “Next” button and install Alsid for AD.
Indicate the Storage Manager’s IP address in the two dedicated fields and type the password of the SQL database that you previously chose. Then, click on the "Next" button.

In order to make Alsid’s web application and services (SAML, SMTP, etc.) available for the end users, please enter the DNS name (preferred) or the IP address the end users will use to access Alsid’s platform.

By default, the installation process creates a self-signed certificate with the DNS name, or the IP typed. If you are willing to change this certificate, please refer to please refer to How to change IIS certificate for AlsidForAD Web Application on page 26.

You also have to type the RabbitMQ's IP address before clicking on the "Next" button and install Alsid for AD.
Wait for the end of the installation and click on **YES** to reboot the server.

◊ **VM3 - Cancri, Caroli and Corvi**

The installation mechanism is fully automated through an executable file. To perform the installation, execute “\Alsid\ForAD\v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To deploy only **Cancri**, **Caroli** and **Corvi**, you must select only these features.

Once this is done, change the **Location if needed** by editing **ONLY** the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the drive letter is **E**. Then, click on the “Next” button and install Alsid for AD.
Figure 19: Features dialog on Security Engine Node (3)

Indicate RabbitMQ’s IP address and Eridanis’ IP address in the two dedicated fields before clicking on the “Next” button and install Alsid for AD.

Figure 20: Security Engine Node settings dialog on SEN (3) install

Wait for the end of the installation and click on YES to reboot the server.
**VM4 - Cygni**

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.

![Welcome dialog on Security Engine Node (4)](image)

**Figure 21: Welcome dialog on Security Engine Node (4)**

On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy the **Cygni** feature, you must select only this feature.

Once this is done, change the **Location if needed** by editing **ONLY** the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the driver letter is **E**. Then, click on the “Next” button and install Alsid for AD.

![Features dialog on Security Engine Node (4)](image)

**Figure 22: Features dialog on Security Engine Node (4)**
Indicate **RabbitMQ's IP address** and **Eridanis' IP address** in the two dedicated fields before clicking on the “Next” button and install Alsid for AD.

![Security Engine Node settings dialog on SEN (4) install](image)

Wait for the end of the installation and click on **YES** to reboot the server.

### 3. Install Directory Listener

During this step, the process will deliver the following applications:

- Alsid component
  - Ceti

In a specific context, it can be useful to deploy more than one DL within the same infrastructure. For example, if two forests are registered in the solution but those two are on different networks because of legal restrictions, you can deploy one DL in the first subnet and another DL in the second subnet.

**Expert Mode:**
This configuration requires to check the “Expert mode” box on the first installer window to display advanced installation options. For more details, please refer to **Expert Mode for Directory Listener on page 33**.

The installation mechanism is fully automated through an executable file. To perform the installation, execute “AlsidForAD_v2.X.X.exe” with full Local Administrator privileges and click on the “Next” button.
On the next dialog, you can choose the features you want to deploy. By default, everything is selected. You must specify what you don’t want to install. To only deploy the DirectoryListener feature, you must select only this feature.

Once this is done, change the Location if needed by editing ONLY the drive letter. You can do this by clicking on the “Browse” button. Here in our example, the driver letter is E. Then, click on the “Next” button.

Indicate RabbitMQ’s IP address in the dedicated field before clicking on the “Next” button and install Alsid for AD.
4. Access to specific Active Directory objects or containers

Alsid’s platform achieves its security monitoring without the need of administrative privileges. Despite its many advantages (operation safety, limited attack surface, etc.), this approach relies on the ability of the user account used by the platform to read all the Active Directory objects stored in a domain (including user accounts, organizational units, groups, etc.).

By default, most of the objects natively benefit from a default read access for the group Domain Users used by Alsid’s service account. However, some containers need to be manually configured to allow read access to Alsid’s user account:

<table>
<thead>
<tr>
<th>Active Directory objects or containers requiring manual read access setup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN=Deleted Objects, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>Container hosting deleted objects</td>
</tr>
<tr>
<td>CN=Password Settings Container, CN=System, DC=&lt;DOMAIN&gt;, DC=&lt;TLD&gt;</td>
<td>[Optional] Container hosting Password Strategy Objects</td>
</tr>
</tbody>
</table>

For each of the below containers, Alsid requires to grant access to the service account used by the platform via the following command line:

```
dsacl "<__CONTAINER__>" /takeownership

dsacl "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
```

In the previous table, `<__CONTAINER__>` refers to the container to grant access to. `<__SERVICE_ACCOUNT__>` refers to the service account used by Alsid’s platform.

This command needs to be run on every domain monitored by Alsid’s platform.
III. ANNEXES

1. How to change IIS certificate for AlsidForAD Web Application

When the AlsidForAD SEN module is installed, a self-signed certificate is created and binds to the AlsidForAD web application.

The certificate name is chosen during the installation and is equal to webAppHostName. Let’s assume that the chosen name is the IP address of the SEN server where the IIS role is installed, since this is the most common scenario.

If, by assumption, the IP address of the SEN server is 10.0.48.55 after installation, the web application can be accessed via https://10.0.48.55.

![Figure 27: Login page of AlsidForAD](image)

There are two important pieces involved here so you can access the web application via HTTPS:

- Self-signed certificate
- Web App binding

During installation, a self-signed certificate is created and placed in the IIS Server Certificate store.

To access this certificate, go to **Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager**, and click on Server Name on the left (Connections) pane followed by a double-click on ‘Server Certificates’.
During installation, IIS Site Binding is created by using the HTTPS port (443 by default) and the self-signed certificate.

To explore this binding, go to **Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager** and expand the **Sites** menu on the left pane. Right-click on your site (Default Web Site, in this example) and choose **Edit Bindings**. A new window **Site Bindings** will pop up, and from there you can select **https** binding and click on **Edit**.

On the **Edit Site Binding** window that will appear, you can find installed IIS certificates in the dropdown menu at the bottom of the dialog.
To use your certificate for the AlsidForAD web application, you must:

- Install your certificate in IIS
- Edit site binding to use your installed certificate.

To install the IIS Certificate, go to **Windows Start > Windows Administrative Tools > Internet Information Services (IIS) Manager** and click on Server Name on the left (Connections) pane followed by a double-click on 'Server Certificates'.

From there, choose 'Import' on the right pane menu and import your certificate.
You can also choose any other way to install the IIS certificate. The end goal is to have your certificate appear on the IIS Server Certificates list.

To edit site binding, navigate to **Edit Site Binding** as described above, and choose your newly installed certificate from the SSL certificate dropdown menu at the bottom of the dialog:
Right-click on the website on the left pane and restart to take effect.
2. Meta-Kapteyn configuration file

Meta-Kapteyn installation requires at least two instances of AlsidForAD. For example, let’s consider that we are installing Meta-Kapteyn with this configuration:

![Diagram showing Meta-Kapteyn architecture example]

The configuration file must be like:

```
"InstanceName","EridanisNodeIp","EnifNodeIp","EquuleusNodeIp","ElectraNodeIp"
"InfrastructureA","192.168.1.3","192.168.1.3","192.168.1.3","192.168.1.3"
"InfrastructureB","192.168.10.3","192.168.10.3","192.168.10.3","192.168.10.3"
```
3. How to back up Storage Manager

3.1. InfluxDB

◊ Backup

To perform a remote backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to E:\Alsid\AlsForAD\StorageManager\AfadInfluxDB\InfluxDB
- Run the following command (replace the yellow part by the real expected value):

  `influxd backup-portable -host <host:port><path-to-backup>`

To perform a local backup, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to E:\Alsid\AlsForAD\StorageManager\AfadInfluxDB\InfluxDB
- Run the following command (replace the yellow part by the real expected value):

  `influxd backup-portable <path-to-backup-files>`

◊ Restore

To perform a remote restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to E:\Alsid\AlsForAD\StorageManager\AfadInfluxDB\InfluxDB
- Run the following command (replace the yellow part by the real expected value):

  `influxd restore -portable -host <host:port><path-to-backup-files>`

To perform a local restoration, please follow those steps:

- Open a PowerShell (x64) window as an administrator
- Move to E:\Alsid\AlsForAD\StorageManager\AfadInfluxDB\InfluxDB
- Run the following command (replace the yellow part by the real expected value):

  `influxd restore -portable <path-to-backup-files>`

⚠️ The backup is a folder, not a file.

Source: [https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/](https://docs.influxdata.com/influxdb/v1.7/administration/backup_and_restore/)

3.2. MSSQL

Please follow the official documentation to perform MSSQL backup or restoration: [https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-transact-sql?view=sql-server-ver15](https://docs.microsoft.com/en-us/sql/t-sql/statements/backup-transact-sql?view=sql-server-ver15)

The database name is “dsc” prior to version 2.6.0, and “alsidforad” for ulterior versions.
4. Expert Mode for Directory Listener

Expert Mode: The following options are only available when this mode is switched on.

4.1. Additional subnets for Ceti

You can specify the subnet(s) you want to use for Ceti. If you want to add more than one subnet, use a comma as a separator between the CIDR subnets you will use. For example, 10.0.0.1/32, 192.168.0.0/24.

In the following screenshots, we are only using one subnet. Then, click on the “Next” button and install Alsid for AD.

![Figure 35: Directory Listener settings dialog with Expert Mode](image)

Wait for the end of the installation and click on YES to reboot the server.

5. What is a complex password?

Password policies depend on business sectors and legal restrictions. This is a well-known topic in the cybersecurity world and some articles are published every year to answer the question: What is a complex password in our time? We are not going to answer it, but we will explain what a complex password for the installer is.

We must match the complexity requirements of any client. That’s why we based our criteria on the current password policy that is applied to create a new local account on the machine.

6. How to horizontally scale up/down services to improve data processing performance?

6.1. Scale Up

◊ **Cancri**
The scaling up mechanism of this component is fully automated through a PowerShell Script. To perform the scaling:

- Open a PowerShell (x64) window as an administrator
- Move to Cancri location (here AlsidForAD has been installed on the E drive) E:\Alsid\AlsidForAD\SecurityEngineNode\n- Run the following command (replace the yellow part by the real expected value):

```
\Install-CancriService.ps1 -drive <your partition letter here> -role SecurityEngineNode -numberOfInstances <Number of Cancri services>
```

- Example (partition letter is E and we want 3 instances of Cancri):

```
\Install-CancriService.ps1 -drive E -role SecurityEngineNode -numberOfInstances 3
```

◊ **Caroli**
The scaling up mechanism of this component is fully automated through a PowerShell Script. To perform the scaling:

- Open a PowerShell (x64) window as an administrator
- Move to Caroli location (here AlsidForAD has been installed on the E drive) E:\Alsid\AlsidForAD\SecurityEngineNode\n- Run the following command (replace the yellow part by the real expected value):

```
\Install-CaroliService.ps1 -drive <your partition letter here> -role SecurityEngineNode -numberOfInstances <Number of Caroli services>
```

- Example (partition letter is E and we want 3 instances of Caroli):

```
\Install-CaroliService.ps1 -drive E -role SecurityEngineNode -numberOfInstances 3
```

◊ **Eridanis**
To scale up the total number of Eridanis instances, the `ERIDANIS_WORKER_COUNT` environment variable must be updated.

To perform the scaling:

- Open a PowerShell (x64) window as an administrator
- Run the following command (replace the yellow part by the real expected value):

```
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', <number of Eridanis instances>, 'Machine')
Restart-Service -Name 'alsid_Eridanis'
```

- Example (we want 3 instances of Eridanis):

```
[System.Environment]::SetEnvironmentVariable('ERIDANIS_WORKER_COUNT', 3, 'Machine')
Restart-Service -Name 'alsid_Eridanis' -Force
```