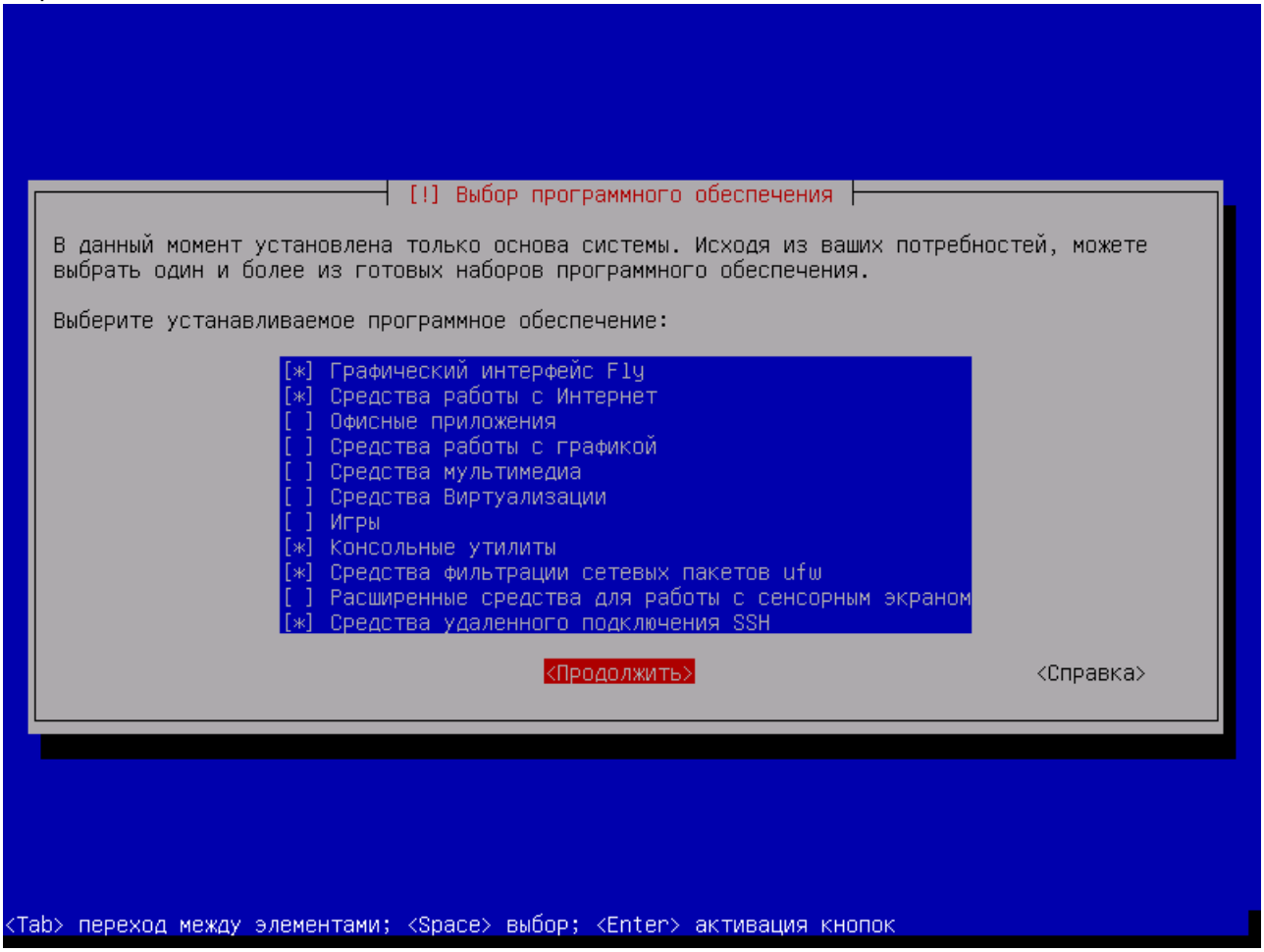
Установка тестовой среды с JMS 4 LX

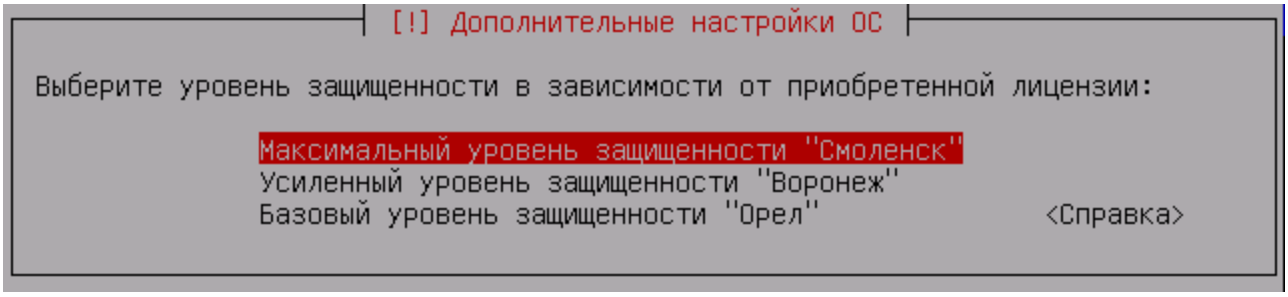
Подготовка сервера ALSE 1.7.4 для JMS4LX

Порты для подключений: JMS: 5000, 5001/tcp JWA: 8120, 8121, 8122/tcp

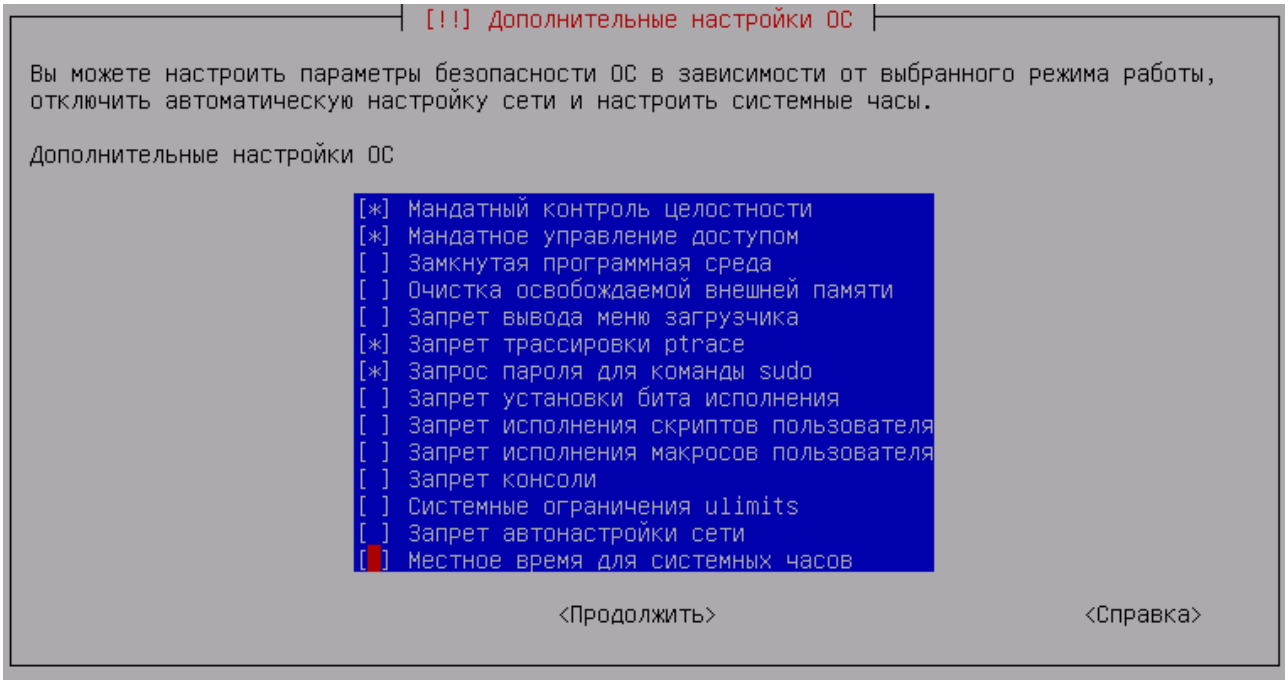
- Перечень компонент:



- УЗ:

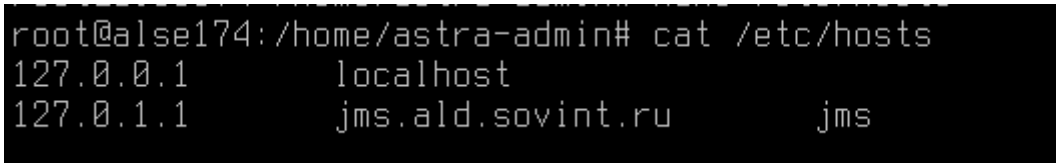


- Доп. настройки:



- Задать hostname

```
sudo hostnamectl set-hostname jms
nano /etc/hosts
```



- Ввести компьютер в домен:

```
sudo tee /etc/security/limits.d/90-fsize.conf 2&>/dev/null << EOF
* hard fsize unlimited
* soft fsize unlimited
EOF
sudo apt install astra-ad-sssd-client -y
sudo astra-ad-sssd-client -y -d {{ server.domain }} -u {{
defaults.domainadmin }}
```

```
 * Received NetLogon info from: dc01.ald.sovint.ru
 * Set computer password
 * Retrieved kvno '2' for computer account in directory: CN=JMS,CN=Computers,DC=ald,DC=sovint,DC
=ru
 * Checking RestrictedKrbHost/jms.ald.sovint.ru
 *    Added RestrictedKrbHost/jms.ald.sovint.ru
 * Checking RestrictedKrbHost/JMS
 *    Added RestrictedKrbHost/JMS
 * Checking host/jms.ald.sovint.ru
 *    Added host/jms.ald.sovint.ru
 * Checking host/JMS
 *    Added host/JMS
 * Discovered which keytab salt to use
 * Added the entries to the keytab: JMS$@ALD.SOVINT.RU: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/JMS@ALD.SOVINT.RU: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: host/jms.ald.sovint.ru@ALD.SOVINT.RU: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/JMS@ALD.SOVINT.RU: FILE:/etc/krb5.keytab
 * Added the entries to the keytab: RestrictedKrbHost/jms.ald.sovint.ru@ALD.SOVINT.RU: FILE:/etc
/krb5.keytab
 * /usr/sbin/update-rc.d sssd enable
 * /usr/sbin/service sssd restart
 * Successfully enrolled machine in realm
update-alternatives: используется /usr/lib/x86_64-linux-gnu/cifs-utils/cifs_idmap_sss.so для пре
доставления /etc/cifs-utils/idmap-plugin (idmap-plugin) в ручном режиме
Завершено.
Компьютер подключен к домену.
Для продолжения работы, необходимо перезагрузить компьютер!
astra-admin@jms:~$
```

- ```
  sudo apt install postgresql
  sudo -u postgres psql -c "ALTER USER \"postgres\" WITH PASSWORD
  'VzHgRoC7cvWgMEHjqrkw';"
  ```

- ```
  #установить из base repo
  sudo apt install gss-ntlmssp -y
  ```

- ```
  sudo tee ./InitialConfigurationAD.ini << EOF
  [service]
  execPath=/opt/eap-engine/Aladdin.EAP.Engine
  integrationManagerUrls=http://*:8120
  controlManagerUrls=http://localhost:8119
  authenticationManagerUrls=http://*:8121
  clientManagerUrls=http://*:8122

  [database]
  type=PostgreSQL
  serverAddress=127.0.0.1
  serverPort=5432
  databaseName=JMS4DB-AD
  serverLogin=postgres
  serverPassword=VzHgRoC7cvWgMEHjqrkw
  databaseLogin=postgres
  databasePassword=VzHgRoC7cvWgMEHjqrkw

  [accountSystem]
  type=AD
  name=ald.sovint.ru
  serverAddress=dc01.ald.sovint.ru
  serverPort=389
  ```
  ```

```
container=OU=root,dc=ald,dc=sovint,dc=ru
userName=CN=jmsuser,OU=root,DC=ald,DC=sovint,DC=ru
password=0680i7Pk8M5jxdcYnMbs
disabledContainers=Program Data,System,Application
useSsl=false
;useSsl=true
mapping=false
attributes=*
referralChasing=false

[primaryUser]
accountName=jmsadmin

[licenses]
path=/opt/eap-engine/licenses/ald.sovint.ru.lic
EOF
```

- Установить серверную часть JMS:

```
apt install -f /distrib/aladdin-eap-engine_4.1.0.6244_x64.deb
```

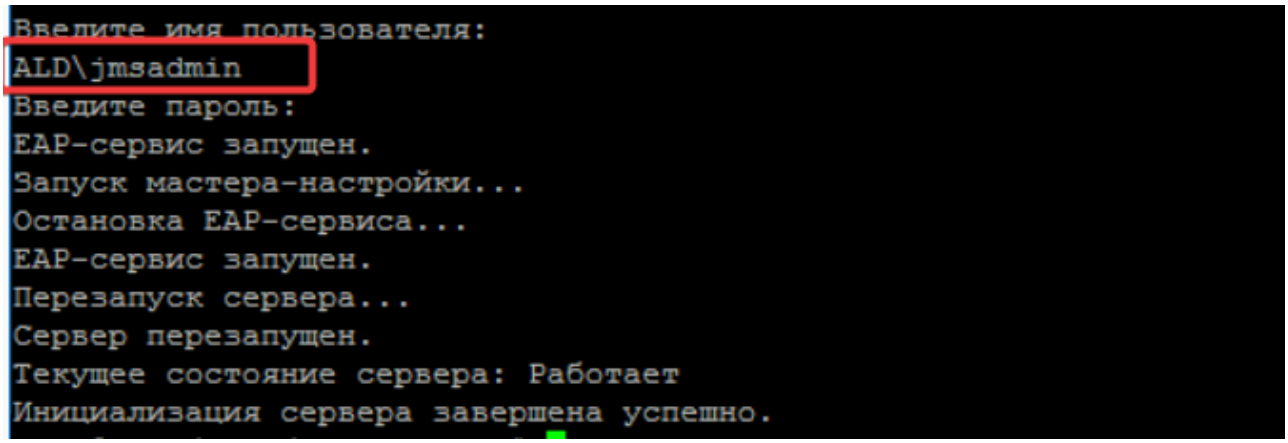
- ```
  sudo mkdir /opt/eap-engine/licenses/ -pv
  sudo cp /distrib/ald.sovint.ru.lic /opt/eap-engine/licenses/ -v
  ```

- Установка корневого сертификата домена:

```
sudo cp -v rootca.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

- Начальная конфигурация:

```
sudo Aladdin.EAP.Agent.Terminal server initialize -p
/distrib/InitialConfiguration.ini
```

- 


- ```
  systemctl status eap-engine
  Aladdin.EAP.Agent.Terminal server status
  ```

- Установить серверную часть веб-консоли JMS:

```
apt install -f /distrib/aladdin-eap-web-admin_4.1.0.6244_x64.deb
```

- `sudo tee /opt/eap-web-admin/appsettings.json < EOF`

```
{
  "Logging": {
    "LogLevel": {
      "Default": "Information",
      "Microsoft": "Warning",
      "Microsoft.Hosting.Lifetime": "Information"
    }
  },
  "AllowedHosts": "*",

  "Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "http://0.0.0.0:5000"
      }
    }
  },

  "WebAdminSettings": {
    "IntegrationApiUrl": "http://localhost:8120",
    "AuthenticationApiUrl": "http://localhost:8121",
    "WebAgentUrl": "http://localhost:5601",
    "ShowWebAgentError": false,
    "LicenseStatus": {
      "NotificationDaysCount": 30,
      "NotificationInterval": 600
    },
    "RetrySettings": {
      "Enabled": true,
      "RetryTimeout": 10000,
      "RetryCount": 10,
      "RetryStatusCodes": [ 503 ]
    },
    "UseActiveDirectoryVirtualListView": false,
    "DefaultActiveDirectoryMaxSizeLimit": 100,
    "SyncTokenSettings": {
      "CheckSyncTimeout": 120,
      "TotalSyncTimeout": 600
    }
  },

  "DataProtectionOptions": {
    "ApplicationName": "Aladdin.EAP.Admin.Web",
    "KeyLocation": "/var/aladdin/eap-engine/keys/",
    "KeyLifetimeDays": 90
  }
```

```
}
EOF
```

```
systemctl restart eap-web-admin
```

- ```
  mkdir /etc/aladdin/eap-web-admin/ssl
  cp -v /distrib/jms.pfx /etc/aladdin/eap-web-admin/ssl

  Aladdin.EAP.Agent.Terminal ssl enable --path /etc/aladdin/eap-web-admin/ssl/jms.pfx --password 1234567890
  ```

```
sed -i 's/"IntegrationApiUrl":.*/"IntegrationApiUrl":"https:\/\/jms.ald.sovint.ru:8120",/g' /etc/aladdin/eap-web-admin/appsettings.json
sed -i 's/"AuthenticationApiUrl":.*/"AuthenticationApiUrl":"https:\/\/jms.ald.sovint.ru:8121",/g' /etc/aladdin/eap-web-admin/appsettings.json
```

```
nano /etc/aladdin/eap-web-admin/appsettings.json
```

```
"Kestrel": {
  "Endpoints": {
    "Http": {
      "Url": "http://localhost:5001"
    },
    "Https": {
      "Url": "https://*:5000",
      "Certificate": {
        "Path": "/etc/aladdin/eap-web-admin/ssl/jms.pfx",
        "Password": "1234567890"
        }
      }
    }
  },
```

```
systemctl restart eap-web-admin
```

- ```
  sed -i 's/"AuthApiURL":.*/"AuthApiURL": https\/\/jms.ald.sovint.ru:8121/g' /etc/aladdin/jwa-service/appsettings.json
  sed -i 's/"ClientApiURL":.*/"ClientApiURL": https\/\/jms.ald.sovint.ru:8122/g' /etc/aladdin/jwa-service/appsettings.json
  ```

- ```
  sudo Aladdin.EAP.Agent.Terminal certificates install --path jms_enroll.pfx --password 1234567890
  ```
  ```

Установка JMS Web Agent

```
sudo apt install pcscd -y
sudo apt install -f ./jcpkcs11-2_2.9.0.874_al_x64.deb
sudo apt install -f ./aladdin-jms-web-agent_4.1.0.62.44_x64.deb
/opt/jms-client/Aladdin.JMS.WebAgent --jms-host jms.ald.sovint.ru —-
jms-web-
host jms.ald.sovint.ru
/opt/jms-client/jwa-service.sh bg
```

Импорт сертификатов

Настройка MSCA Proxy

Входящие порты: 6610, 6611 TCP

- Установить .NET 4.8 Framework https://go.microsoft.com/fwlink/?linkid=2088631
- Установить Aladdin.CAProxyService-1.0.0.4-x64

```
netsh http add sslcert ipport=0.0.0.0:6611
certhash=fd20805c859aedb31de3e12b3800db6c99ca7429
appid={670f608f-28ad-4724-8264-7b3c0eb2dfd6}
```

- Выполнить проверку работы сервиса: http://localhost:6610/api/ca/ping
- Создать пользователя
  - **ca_proxy_user**
- Создать группу
  - **CA_PROXY_GROUP**
  - включить в группу **CA_PROXY_GROUP** пользователя **ca_proxy_user**
- Запустить reg-файл

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Aladdin\CA Proxy Service\MSCAProxyWebApi]
"MSCAProxyWebApiAddresses"="http://*:6610;https://*:6611"
"AuthorizeAsGroupMember"="CA_PROXY_GROUP"
"AuthorizationGroupStore"="Machine"
```

- Перезапустить службу

```
net stop CAProxySvc_default
net start CAProxySvc_default
```

Настройка профилей JMS

Certificate Authority

Шаблон JMS Web Server

- **Certification Authority** → Certificate Templates → Manage
  - Web Server → Duplicate Template
    - General
      - Template display name: JMS Web Server
    - Request Handling
      - Allow private key to be exported
    - Subject Name:
      - Supply in the request
    - Extensions
      - Key Usage:
        - Digital Signature
        - Allow key exchange only with key ecryption (key encipherment)
    - Security:
      - Указать УЗ, которая сможет выпустить сертификат
        - Allow: Read, Write, Enroll
  - **Certification Authority** → Certificate Templates → New
    - JMS Web Server

Выпустить сертификат JMS Server

- certlm.msc Выпустить сертификат для JMS
  - create custom request
    - JMS Web Server
      - Subject
        - Common Name: jms.ald.sovint.ru
        - DNS: jms.ald.sovint.ru
      - Private Key
        - Key Options: Make private key exportable
      - Extensions
        - Key Usage: Digital Signature, Key Encipherment
  - Экспортировать сертификат в формате pxf (опцию Include all certificatation path if possible НЕ УКАЗЫВАТЬ!)
  - Так же, выгрузить корневой сертификат.

Выпустить сертификат MSCA Proxy

- certlm.msc Выпустить сертификат для JMS
  - create custom request
    - JMS Web Server
      - Subject

        - Common Name: mscaproxy.ald.sovint.ru
        - DNS: mscaproxy.ald.sovint.ru
    - Extensions
        - Key Usage: Digital Signature, Key Encipherment

Выпустить сертификат JMS Enrollment Agent Computer

- certlm.msc Выпустить сертификат для JMS
    - create custom request
        - JMS Enrollment Agent (Computer)
            - Subject
                - Common Name: jms.ald.sovint.ru
                - DNS: jms.ald.sovint.ru
- Экспортировать в pfx.

Domain Controller

- **certlm.msc** - Выпустить сертификат на Контроллеры домена по шаблону **Kerberos Authentication**
- **Group Policy Management**
    - Создать политику, действующую на компьютеры домена:
        - Computer Configuration → Policies → Windows Settings → Security Settings → System Services → Smart Card Removal Policy → Automatic
        - Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Interactive Logon: Smart Card Removal Behavior → Disconnect if a remote Remote Desktop Services session

Создание профилей JMS

- Выполнить привязку профилей по умолчанию:
    - Инициализация JaCarta PKI по умолчанию
    - Профиль выпуска по умолчанию
    - Профиль клиентского агента по умолчанию
- Создать профиль выпуска «Выпуск сертификатов - УЦ Microsoft CA»
    - Прокси сервер:
        - Адрес прокси-сервера: **https://ca.ald.sovint.ru:6611**
        - Логин: **ca_proxy_user**
    - Тип подписи запроса из консоли управления JMS: **Общий (подпись запроса на** сервере)
    - Шаблоны сертификатов
        - Пользователь: **JMSSmartcardUser**
        - Администратор: **JMSSmartcardUser**
    - Типы приложений: **PKI**
    - Криптопровайдер для генерации ключевой пары: **Microsoft Base Smart Card Crypto Provider**