
ORACLE®

Установка пользовательской аутентификации с использованием пользовательских сертификатов.

Игорь Лукьянов

Старший консультант
Oracle Application Server 10g

ORACLE

Использование интеграции - требования

Для успешной работы Вы должны быть знакомы с управлением инстанса инфраструктуры OAS 10G и иметь прединсталлированный OAS10G-сервер на одной из поддерживаемых аппаратных платформ и OS.

SSL-протокол.

1. SSL-протокол – индустриальный стандарт для защищенных сетевых коннекций
2. SSL защищает данные в течение их передачи на основе их криптования и алгоритмов защиты
3. Технология SSL базируется на механизмах криптования с открытыми ключами PKI.
4. OAS10G использует SSL для защиты передачи данных между пользователями и сервером приложений, а также для передачи данных между компонентами сервера приложений.

Установка переменных окружения.

```
%cd /home/oracle/infra
%export ORACLE_SID=infra
%export ORACLE_HOME=/home/oracle/infra
%export PATH=$PATH:$ORACLE_HOME/bin
```

Конфигурирование Oracle Process Management и Notification службы (OPMN) для использования с SSL.

%cd $ORACLE_HOME/opmn/conf

%cp opmn.xml opmn.xml.bak

Измените в opmn.xml для ias-component id=“HTTP”:

<…data id=“start-mode” value=“ssl-disabled” />

на

<…data id=“start-mode” value=“ssl-enabled” />

Перезагрузите OPMN:

%$ORACLE_HOME/opmn/bin/opmnctl reload

Конфигурирование ssl.conf - файла.

%cd $ORACLE_HOME/Apache/Apache/conf

%cp ssl.conf ssl.conf.bak

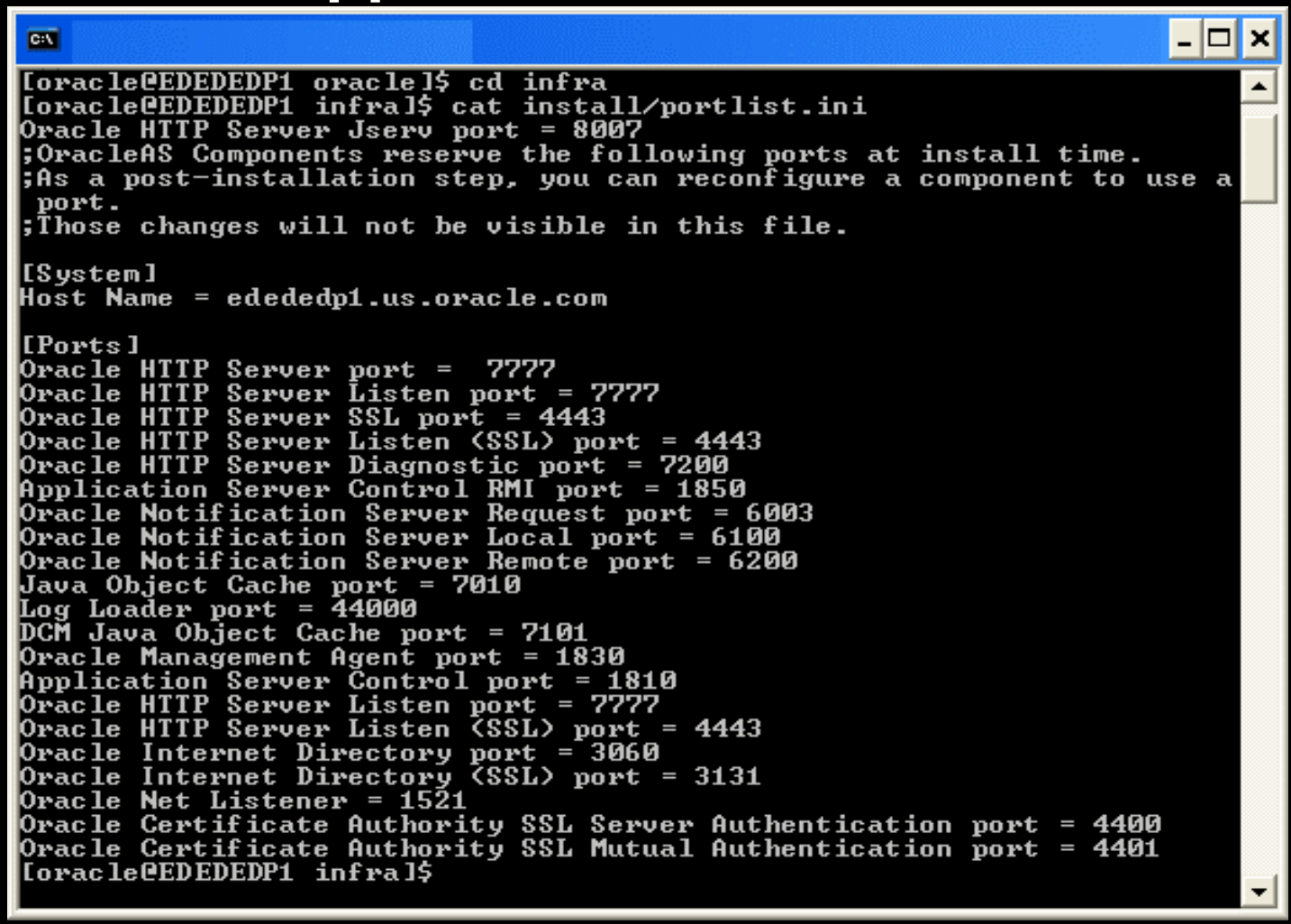
Отредактируйте ssl.conf – файл:

Внутри контейнера </VirtualHost> добавьте в конце:

RewriteEngine on

RewriteOptions inherit

Определите SSL-порт для HTTP-сервера через /home/oracle/infra/install/portlist.ini или Application Server Control.



```
[oracle@EDEDEDP1 oracle]$ cd infra
[oracle@EDEDEDP1 infra]$ cat install/portlist.ini
Oracle HTTP Server Jserv port = 8007
;OracleAS Components reserve the following ports at install time.
;As a post-installation step, you can reconfigure a component to use a
 port.
;Those changes will not be visible in this file.

[System]
Host Name = edededp1.us.oracle.com

[Ports]
Oracle HTTP Server port =  7777
Oracle HTTP Server Listen port = 7777
Oracle HTTP Server SSL port = 4443
Oracle HTTP Server Listen (SSL) port = 4443
Oracle HTTP Server Diagnostic port = 7200
Application Server Control RMI port = 1850
Oracle Notification Server Request port = 6003
Oracle Notification Server Local port = 6100
Oracle Notification Server Remote port = 6200
Java Object Cache port = 7010
Log Loader port = 44000
DCM Java Object Cache port = 7101
Oracle Management Agent port = 1830
Application Server Control port = 1810
Oracle HTTP Server Listen port = 7777
Oracle HTTP Server Listen (SSL) port = 4443
Oracle Internet Directory port = 3060
Oracle Internet Directory (SSL) port = 3131
Oracle Net Listener = 1521
Oracle Certificate Authority SSL Server Authentication port = 4400
Oracle Certificate Authority SSL Mutual Authentication port = 4401
[oracle@EDEDEDP1 infra]$
```

Переконфигурируйте SSO SSL порт.

%cd $ORACLE_HOME/sso/bin

%./ssocfg.sh https
<hostname.domain><OracleHTTPServerSSLport>:

Пример:

%./ssocfg.sh https scias.ru.oracle.com 4443

Переконфигурируйте SSO-сервер для использования с SSL:

%cd $ORACLE_HOME/sso/conf

%cp sso_apache.conf sso_apache.conf.bak

Добавьте следующие линии в конце sso_apache.conf:

<IfDefine SSL>

<location “/sso/auth”>

SSLRequireSSL>

</location>

<location “/sso/ChgPwdServlet”>

SSLRequireSSL (см. дальше)

Переконфигурируйте SSO-сервер для использования с SSL:

</location>

</IfDefine>

<IfModule mod_ossl.c>

Oc4jExtractSSL on

<location “/sso”>

SSLOptions +ExportCertData +StdEnvVars

</location>

</IfModule>

Перерегистрируйте Ваши SSO-приложения:

%$ORACLE_HOME/jdk/bin/java –jar
$ORACLE_HOME/sso/lib/ossoreg.jar –oracle_home_path
$ORACLE_HOME –site_name SSO –config_mod_osso TRUE
-mod_osso_url https://hostname.domain.com:4443
-update_mode CREATE –u root

Также перерегистрируйте Ваше Oracle Certification Authority (OCA):

%$ORACLE_HOME/jdk/bin/java –jar
$ORACLE_HOME/sso/lib/ossoreg.jar –oracle_home_path
$ORACLE_HOME –site_name OCA –config_mod_osso TRUE
-mod_osso_url https://hostname.domain.com:4400 -u root
-virtualhost –config_file
$ORACLE_HOME/Apache/Apache/conf/osso/oca/osso.conf

Рестартируйте Ваш Oracle HTTP сервер:

```
%$ORACLE_HOME/opmn/bin/opmnctl restartproc
    type=ohs
```

Переконфигурируйте orion-web.xml файл:

%cd $ORACLE_HOME/j2ee/OC4J_SECURITY/application-deployments/sso/web

%cp orion-web.xml orion-web.xml.bak

В контейнере </orion-web-app> в orion-web.xml в конце добавьте:

<jazn-web-app runas-mode="true" />

Переконфигурируйте policy.properties файл:

%cd $ORACLE_HOME/sso/conf

%cp policy.properties policy.properties.bak

В файле policy.properties замените:

1. DefaultAuthLevel = MediumSecurity

на

DefaultAuthLevel = MediumHighSecurity

2. MediumSecurity_AuthPlugin =
oracle.security.sso.server.auth.SSOServerAuth

на

MediumHighSecurity_AuthPlugin =
oracle.security.sso.server.auth.SSOX509CertAuth

Рестартируйте OC4J_SECURITY процесс:

%ORACLE_HOME/opmn/bin/opmnctl restartproc process-type=OC4J_SECURITY

После рестарта проверьте, что процесс OC4J_SECURITY работает:

%$ORACLE_HOME/opmn/bin/opmnctl status

Размещение пользовательского сертификата в Oracle Internet Directory:

Если Вы используете Oracle Certification Authority пользовательский сертификат размещается в Oracle Internet Directory автоматически.

Если Вы используете другое CA Вы должны разместить сертификат в OID пользуясь:

- Export NLS_LANG=AMERICAN_AMERICA.UTF8
- %$ORACLE_HOME/bin/ldapmodify –h ldaphost –p OracleInternetDirectoryport –D “directory_administrator” –w password –f file_name.ldif

Пример:

%ORACLE_HOME/bin/ldapmodify –h scias.ru.oracle.com –p 3060 –D “cn=orcladmin” –w qsR53_34!@ -f $ORACLE_HOME/file_name.ldif

Пример сертификата в 64-битной форме в файле формата ldif:

dn: cn=jsmith,cn=users,dc=realm1,dc=oracle,dc=com

changetype: modify

replace: usercertificate

usercertificate::MIIC3TCCAkYCAgP3MA0GCSqGSIb3DQEBBAUAMIG8M
QswCQ

YDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEXMBUGA1UE
BxMOUmVkd29vZCBTaG9yZXMxGzAZBgNV

BAoTEk9yYWNsZSBDb3Jwb3JhdGlvbjEfMB0GA1UECxMWV2ViIFNpbm
dsZSBTaWduLU9uLCBTVDEeMBwGA1

UEAxMVQ2VydGlmaWNhYoEHmF4gomtc4mxSKh/zAgMBAAEwDQYJKo
ZIhvcNAQEEBQADgYEAKwXoCLDRqmK1

Y9LQtljLnCaIJKUZmS1Qj+bhu/lHeZLGHg4TJg3O2XVA5u/VxwjLeGBqLX
y2z7o3RujNKx2CVx6p/0Hkjn

w4w6KVau2hcBgC9m4kzUGhHJ9b65v/zx7dlUKyJr4RF+IJhJg4/oYXxLrY
Hp5NAkHP4htT0gqCXil=


Вопросы
Ответы


ORACLE®