Инструкция по настройки Битрикс для портала Итилиум

Данная инструкция предназначена для администраторов системы Итилиум. В инструкции рассказывается, как настроить сервер с Битрикс, развернутый на CentOS7, чтобы можно было использовать сквозную доменную аутентификацию на портале Итилиум.

Термины и обозначения

Итилиум – развернутая информационная база Итилиум версии 4.6.1.2 или выше.
AD – служба каталогов Active Directory.
Портал Итилиум – развернутая система Bitrix с установленным модулем «Портал Итилиум» и подключенная к системе Итилиум.
Сквозная доменная аутентификация – способ аутентификации на веб-ресурсе или в приложении, при котором у пользователя не запрашивается пароль, а используется информация о текущей учетной записи в операционной системе, под которой работает пользователь.
Битрикс – развернутая на сервере с CentOS7 система «1С-Битрикс: Управление сайтом» версии 18.0 или выше, или «1С-Битрикс24» (только версия для установки на собственный сервер, облачная версия «1С-Битрикс24» не поддерживается).

Что нужно сделать

Для работы портала Итилиум необходимо выполнить настройку, чтобы веб-сервер создавал переменную окружения PHP $_SERVER[”REMOTE_USER”].

Как это сделать

Необходимая настройка может быть выполнена только на веб-сервере Apache версии 1.3 и выше.

Мы рассмотрим веб-сервер apache с модулем mod_auth_ntlm_winbind.so

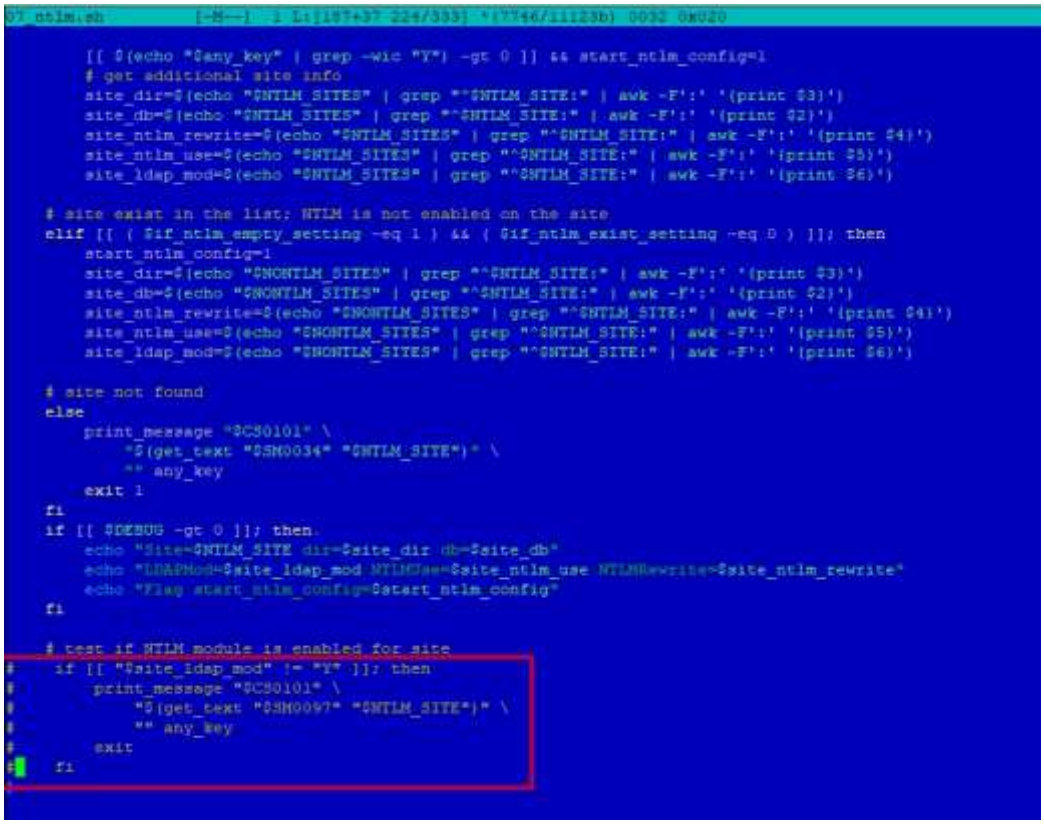
Исходные данные для рассматриваемого примера:

Домен:	itilium-dc-test.mycompany.ru
Имя машины, где установлен Битрикс:	itilium-portal
Адрес сайта Битрикс:	itilium-portal.mycompany.ru

Удобнее всего настройку выполнить при помощи веб-окружения Битрикс.

1) Для работы редакций 1С-Битрикс без модуля модуля AD/LDAP (Старт, Малый бизнес, Бизнес) необходимо модифицировать файл /opt/webdir/bin/menu/06_site/07_ntlm.sh (сохраните его резервную копию)

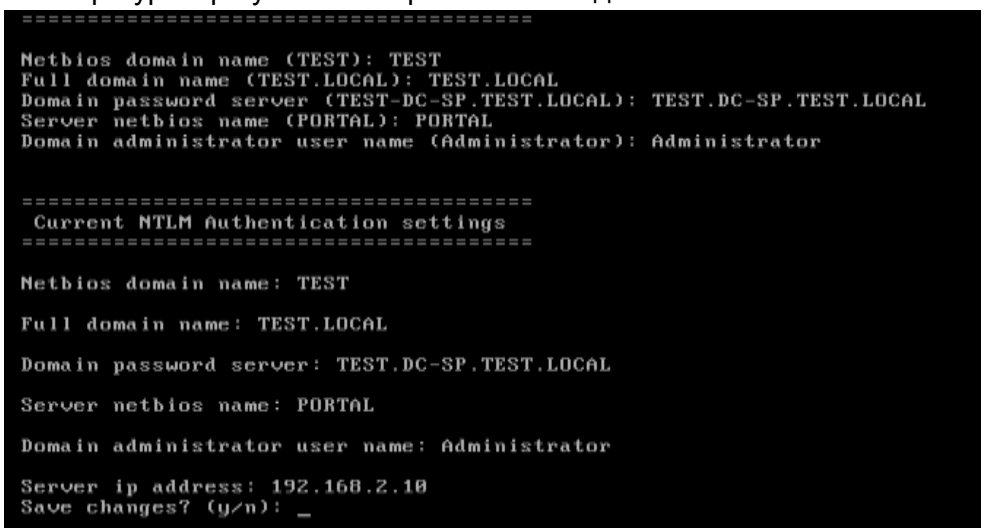
Закомментировать выделенные строки (в версии Bitrix virtual appliance version 7.5 это строки 219-224), поставив в начале строки #:



После этого запустить веб-окружение:
sudo /root/menu.sh
выбрать последовательно

6. Configure pool sites
    7. Configure NTLM auth for sites
        1. Configure NTLM settings for the sit

На запросы конфигуратора указать запрашиваемые данные



Пример в нашем случае:

Domain : ITILIUM-DC-TEST.MYCOMPANY.RU
LDAP Server : itil-dc-1.itilium-dc-test.mycompany.ru:389
Realm : dc=ITILIUM-DC-TEST,dc=MYCOMPANY,dc=RU
KDC : 10.32.1.23

После подтверждения корректности введенных данных мастер настроит и запустит все необходимые службы, а также подключит виртуальную машину в домен.

Проверить, что компьютер успешно введен в домен можно командой:
net ads testjoin

2) Создать\изменить конфигурационный файл для веб-сайта, который слушает внешний порт напрямую (без проксирование через nginx). В качестве конфигурационного файла можно использовать файл сайта созданный при помощи “Битрикс веб-окружения”. Красным отмечены необходимые настройки: прослушивание внешнего порта.

Пример файла:
/etc/httpd/bx/conf/bx_ext_**itilium-portal.mycompany.ru**.conf

```
# site: itilium-portal.mycompany.ru
<IfModule !auth_ntlm_winbind_module.c>
        LoadModule auth_ntlm_winbind_module modules/mod_auth_ntlm_winbind.so
</IfModule>
Listen 8091
<VirtualHost *:8091>
        ServerName  itilium-portal.mycompany.ru
   ServerAlias www.itilium-portal.mycompany.ru
        ServerAdmin webmaster@localhost
   DocumentRoot  /home/bitrix/ext_www/itilium-portal.mycompany.ru
   KeepAlive On

   ErrorLog logs/itilium-portal_error_log
   LogLevel warn
   CustomLog logs/itilium-portal_access_log combined

   <IfModule mod_rewrite.c>
        #Nginx should have "proxy_set_header HTTPS YES;" in location
        RewriteEngine On
        RewriteCond %{HTTP:HTTPS} =YES
        RewriteRule .* - [E=HTTPS:on,L]
   </IfModule>

   <Directory />
        Options FollowSymLinks
        AllowOverride None
   </Directory>

   <DirectoryMatch .*\.svn/.*>
       Require all denied
   </DirectoryMatch>

   <DirectoryMatch .*\.git/.*>
        Require all denied
   </DirectoryMatch>

   <DirectoryMatch .*\.hg/.*>
        Require all denied
   </DirectoryMatch>

   <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru>
```

```
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        DirectoryIndex index.php index.html index.htm
#       Require all granted


    AuthName "NTLM Authentication thingy"
    NTLMAuth on
        NTLMAuthHelper "/usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp"
        NTLMBasicAuthoritative on
        AuthType NTLM
        Require valid-user


        php_admin_value session.save_path /tmp/php_sessions/ext_www/itilium-portal.mycompany.ru
        php_admin_value upload_tmp_dir   /tmp/php_upload/ext_www/itilium-portal.mycompany.ru
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/cache>
        AllowOverride none
        Require all denied
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/managed_cache>
        AllowOverride none
        Require all denied
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/local_cache>
        AllowOverride none
        Require all denied
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/stack_cache>
        AllowOverride none
        Require all denied
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/upload>
        AllowOverride none
        AddType text/plain
php,php3,php4,php5,php6,phtml,pl,asp,aspx,cgi,dll,exe,ico,shtm,shtml,fcg,fcgi,fpl,asmx,pht
        php_value engine off
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/upload/support/not_image>
        AllowOverride none
        Require all denied
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/images>
        AllowOverride none
        AddType text/plain
php,php3,php4,php5,php6,phtml,pl,asp,aspx,cgi,dll,exe,ico,shtm,shtml,fcg,fcgi,fpl,asmx,pht
        php_value engine off
    </Directory>

    <Directory /home/bitrix/ext_www/itilium-portal.mycompany.ru/bitrix/tmp>
        AllowOverride none
        AddType text/plain
php,php3,php4,php5,php6,phtml,pl,asp,aspx,cgi,dll,exe,ico,shtm,shtml,fcg,fcgi,fpl,asmx,pht
```

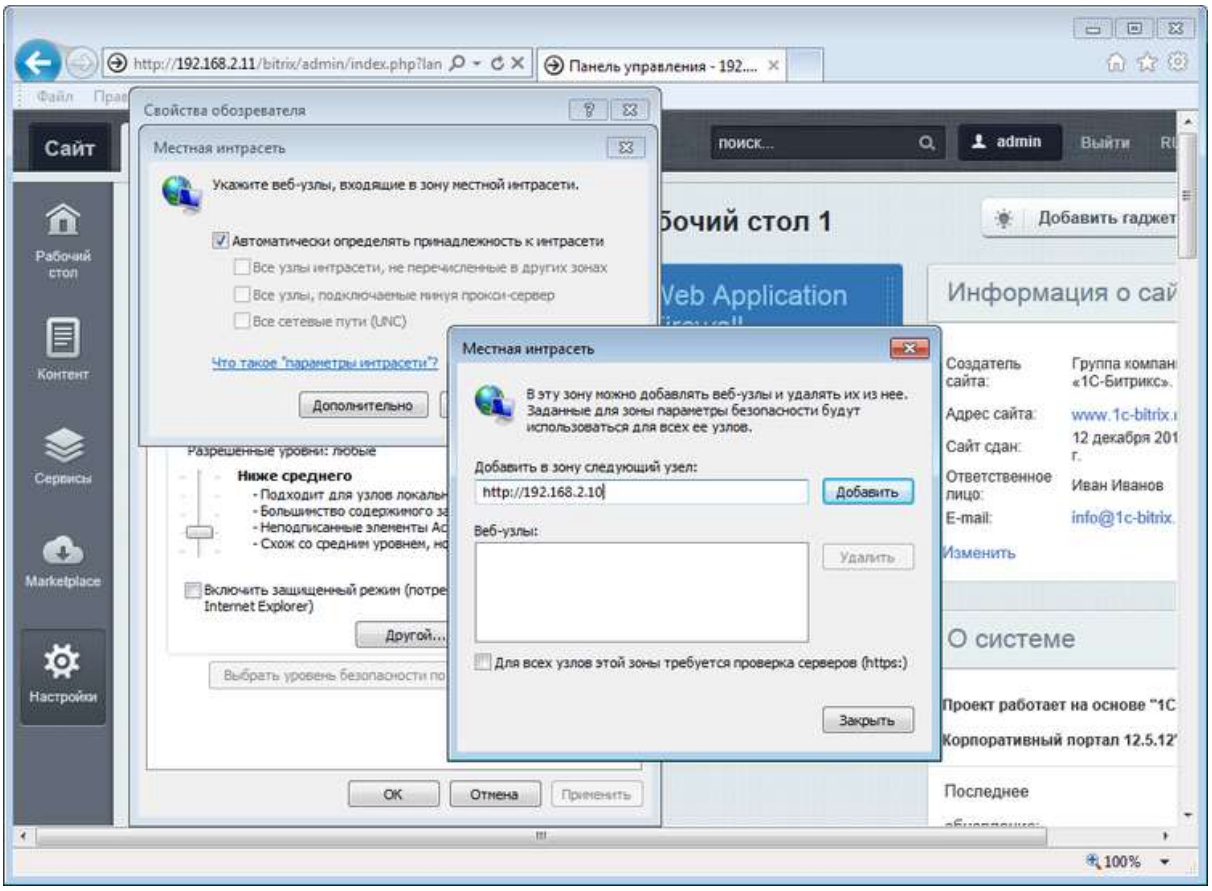
```
        php_value engine off
    </Directory>

</VirtualHost>
```

3) Открыть порт сайта в файрволе
   В нашем примере это порт 8091

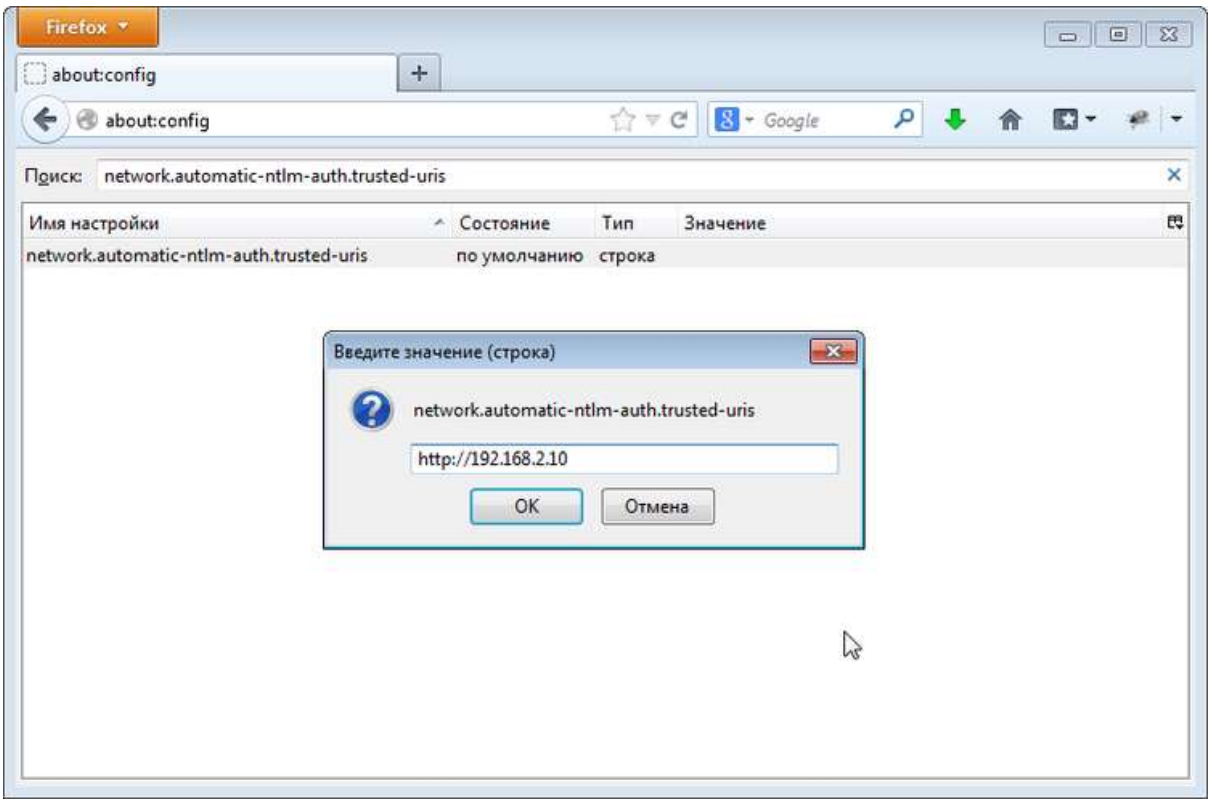
   iptables -I INPUT -p tcp --dport 8091 -j ACCEPT
   service iptables save

4) Настройка NTLM-авторизации в браузерах

- **Internet Explorer**
  Для успешной NTLM-авторизации нужно, чтобы веб-сервер находился в зоне **Local Intranet** (при необходимости нужно добавить):



- **Mozilla Firefox**:
  Добавить веб-сервер к списку доверенных URI для автоматической NTLM-авторизации (через параметр network.automatic-ntlm-auth.trusted-uris на странице Firefox: about:config)



5) Если используется лес доменов - вносим настройку в samba, файл /etc/samba/smb.conf

winbind separator = \\

winbind enum users = yes

winbind enum groups = yes

winbind use default domain = no

После этого необходимо перезагрузить сервис:

service smb restart

service winbind restart

Настройка завершена.

В случае возникновения проблем

Проверить:

1) Настройка samba.
   /etc/samba/smb.conf

```
# configure active directory connection for NTLM auth
[global]
        workgroup = ITILIUM-DC-TEST
        server string = ITILIUM-PORTAL.MYCOMPANY.RU server
        security = ads

        realm = ITILIUM-DC-TEST.MYCOMPANY.RU
        netbios name = ITILIUM-PORTAL

        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

        winbind enum users = yes
        winbind enum groups = yes

        idmap config * : range = 10000-40000
        idmap config * : backend = tdb

        template homedir = /home/%D/%U
        template shell = /bin/bash

        encrypt passwords = yes
        password server = itilium-dc-test.mycompany.ru
        winbind use default domain = yes
        restrict anonymous = 2
        client use spnego = yes
        client ntlmv2 auth = yes
        winbind separator = +

        log file = /var/log/samba/log.%m
        log level = 2 passdb:5 auth:10 winbind:2
        max log size = 200
```

2) Если авторизация не работает проверить логи apache
   [:error] [pid 4340] (20014)Internal error: [client 10.32.1.115:62451] ntlm_auth reports Broken Helper: BH NT_STATUS_UNSUCCESSFUL NT_STATUS_UNSUCCESSFUL

   [:error] [pid 68917] (2)No such file or directory: [client 10.32.1.115:65377] couldn't spawn child ntlm helper process: ntlm_auth

   Убедиться что существует группа *wbpriv*
   cat /etc/group
   Если нет, добавить:
   groupadd wbpriv
   usermod -a -G wbpriv apache
   usermod -a -G wbpriv bitrix

   Если группа существовала выполнить команды:
   chgrp wbpriv /var/lib/samba/winbindd_privileged
   ln -s /var/lib/samba/winbindd_privileged/pipe /var/run/samba/winbindd_privileged/pipe
   service httpd restart

3) Настройка kerberos
/etc/krb5.conf

```
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = ITILIUM-DC-TEST.MYCOMPANY.RU
    dns_lookup_realm = false
    dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = yes

[realms]
    ITILIUM-DC-TEST.MYCOMPANY.RU = {
            kdc = itilium-dc-test.mycompany.ru
            admin_server = itilium-dc-test.mycompany.ru
}

[domain_realm]
    .itilium-dc-test.mycompany.ru = ITILIUM-DC-TEST.MYCOMPANY.RU
    itilium-dc-test.mycompany.ru = ITILIUM-DC-TEST.MYCOMPANY.RU
```

Проверить авторизацию на контроллере домена
/usr/bin/ntlm_auth --username=*yourname*
service winbind status
service winbind start