RUNA WFE. Клиент-оповещатель. Руководство администратора.

(Конфигурирование системы для использования TasksNotifier для Windows).

Версия 2.1

Оглавление

Настройка NTLM аутентификации....1
Настройка клиентской части....2
Последовательность действий:....2
Настройка безопасности JVM....3
Настройка серверной части....4
Последовательность действий:....4
Как запустить клиент-оповещатель....5

Настройка NTLM аутентификации

Для включения системы “беспарольной” аутентификации, используя аккаунт пользователя, зарегистрированного в Windows домене, необходимо:

- добавить NTLM login модуль в файл $(DIST_ROOT)/server/default/conf/login_module.properties. Например, ru.runa.af.authenticaion.NTLMLoginModule=SUFFICIENT
- Настроить имя домена в файле $(DIST_ROOT)/server/default/conf/ntlm_support.properties. Например, domain=RUNA
- Включить поддержку NTLM в этом же файле. Например, ntlm_supported=true

Зайдя на страницу сервера, где установлена система,: http://<servername>/wfe/ntlmlogin.do (NTLM аутентификация может также работать поверх HTTPS) пользователи, зарегистрированные в указанном домене и имеющие права на вход в систему, пройдут аутентификацию.

Для отключения поддержки NTLM достаточно отключить параметры, указанные в п.п. 1) и 3).

После изменения параметров NTLM необходимо перегрузить сервер.

Настройка Kerberos аутентификации

Замечание. В данном разделе все имена и принципалы пользователей и серверов case-sensitive.

Настройка TasksNotifier (приложения, сообщающего о появившихся заданиях)

Настройка клиентской части

Замечание. Клиентское приложение (TaskNotifier) собрано с жестко указанными принципалами сервера – WFTestUser. Для смены значения принципалов необходима пересборка приложения.

Последовательность действий:

1. На контроллере домена Внести в следующий ключ реестра параметр

- Для Windows Server 2003 и Windows 2000 SP4

ключ: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
параметр: allowtgtsessionkey=dword:0x01
- Для Windows XP SP2
ключ: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos
параметр: allowtgtsessionkey=dword:0x01

Замечание. После внесения параметра необходима перезагрузка.
Описание проблемы, которая решается при помощи данного действия:
http://java.sun.com/j2se/1.5.0/docs/guide/security/jgss/tutorials/Troubleshooting.html глава "javax.security.auth.login.LoginException: KrbException: KDC has no support for encryption type (14) - KDC has no support for encryption type".

2. На Workflow серевере создать/отредактировать файл конфигурации Kerberos krb5.ini
Файл должен находиться в %SystemRoot% и иметь имя krb5.ini.
Обязательно следует указать в качестве алгоритмов криптования следующие:

```
[libdefaults]
default_tkt_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
default_tgs_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
permitted_enctypes = des-cbc-md5 des-cbc-crc des3-cbc-sha1
```

Детальное описание файла конфигурации Kerberos http://web.mit.edu/kerberos/www/krb5-1.4/krb5-1.4.3/doc/krb5-admin/krb5.conf.html.[1]

3. Проинсталлировать на клиенте JRE5.0, (находится http://java.sun.com/j2se/1.5.0/download.jsp)
4. Необходимо создать произвольную папку на клиенте, имя которой не содержит пробелов. Далее в данном документе будем обозначать эту папку - $(NOTIFIER_ROOT). Из файла-архива \\Workflow_comp\releases\notifier\task-notifier-2.0<...>.zip необходимо распаковать в эту папку файлы rtn.jar и runa_tasks.exe.
5. Находящийся в \\Workflow_comp\releases\notifier\task-notifier-2.0<...>.zip файл swt-win32-3138.dll (эта .dll используется native графической библиотекой swt в случае операционной системы Windows) необходимо скопировать на клиентский компьютер и путь к нему включить в переменную среды Path.
6. После настройки серверной части клиентское приложение можно будет активизировать, запустив на выполнение файл $(NOTIFIER_ROOT)\runa_tasks.exe (файл запускает виртуальную машину Java и передает ей соответствующие ссылки на классы, находящиеся в rtn.jar.

Замечание. Настройки build'a приложения, сообщающего о появившихся заданиях описаны в документе «RUNA WFE. Руководство разработчика. Версия 2.0” в разделе «Настройка «толстого» клиента».

Настройка безопасности JVM

Включить security manager. Для включения security manager'a для всех локально запускаемых приложений необходимо определить переменную окружения _JAVA_OPTIONS и установить ее значение -Djava.security.manager
После этого на все локально запускаемые приложения будут накладываться ограничения security manager'a по умолчанию. Эти ограничения описываются в файле $JAVA_HOME\lib\security\java.policy. Формат этого файла описан http://java.sun.com/j2se/1.5.0/docs/guide/security/PolicyFiles.html. Список возможных полномочий используемых security manager'ом – http://java.sun.com/j2se/1.5.0/docs/guide/security/permissions.html.

Пример политики (файла java.policy) дающий классам (в том числе и из JAR архивов) из директории D:\tmp все полномочия и не дающим никаких полномочий классам (в том числе и из JAR архивов) из любых других директорий файловой системы:

1 Пример конфигурационного файла krb5.ini прилагается.

```
// Standard extensions get all permissions by default

grant codeBase "file:${{java.ext.dirs}}/*" {
	permission java.security.AllPermission;
};

// default permissions granted to all domains

grant {
	// Allows any thread to stop itself using the java.lang.Thread.stop()
	// method that takes no argument.
	// Note that this permission is granted by default only to remain
	// backwards compatible.
	// It is strongly recommended that you either remove this permission
	// from this policy file or further restrict it to code sources
	// that you specify, because Thread.stop() is potentially unsafe.
	// See "http://java.sun.com/notes" for more information.
	permission java.lang.RuntimePermission "stopThread";

	// allows anyone to listen on un-privileged ports
	permission java.net.SocketPermission "localhost:1024-", "listen";

	// "standard" properies that can be read by anyone

	permission java.util.PropertyPermission "java.version", "read";
	permission java.util.PropertyPermission "java.vendor", "read";
	permission java.util.PropertyPermission "java.vendor.url", "read";
	permission java.util.PropertyPermission "java.class.version", "read";
	permission java.util.PropertyPermission "os.name", "read";
	permission java.util.PropertyPermission "os.version", "read";
	permission java.util.PropertyPermission "os.arch", "read";
	permission java.util.PropertyPermission "file.separator", "read";
	permission java.util.PropertyPermission "path.separator", "read";
	permission java.util.PropertyPermission "line.separator", "read";

	permission java.util.PropertyPermission "java.specification.version", "read";
	permission java.util.PropertyPermission "java.specification.vendor", "read";
	permission java.util.PropertyPermission "java.specification.name", "read";

	permission java.util.PropertyPermission "java.vm.specification.version", "read";
	permission java.util.PropertyPermission "java.vm.specification.vendor", "read";
	permission java.util.PropertyPermission "java.vm.specification.name", "read";
	permission java.util.PropertyPermission "java.vm.version", "read";
	permission java.util.PropertyPermission "java.vm.vendor", "read";
	permission java.util.PropertyPermission "java.vm.name", "read";
};

grant codeBase "file:/D:/tmp/*" {
	permission java.security.AllPermission;
};
```

Настройка серверной части

Последовательность действий:

1. Включить Kerberos login модуль в файл $(DIST_ROOT)/server/default/conf/login_module.properties.

Например, ru.runa.af.authenticaion.KerberosLoginModule=SUFFICIENT.
Настроить принципалы сервера и пользователя от имени которого осуществляется аутентификация в файле $(DIST_ROOT)/server/default/conf/kerberos_module.properties.

- principal – имя сервиса, который осуществляет аутентификацию (В текущей реализации WFTestUser@RUNA.RU)
- serverPrincipal - принципалы пользователя от имени которого осуществляется аутентификация сервера (фактически это логин пользователя)

2. Для сервера необходимо выполнить те же настройки, что и для клиентской машины.

3. Для пользователя, от имени которого осуществляется аутентификация в AD, необходимо включить DES криптование. Описание
http://www.microsoft.com/windows2000/en/advanced/help/default.asp?url=/windows2000/en/advanced/help/dsadmin_concepts_accounts.htm.

4. На Workflow сервере создать Kerberos keytab в котором содержится информация необходимая для аутентификации этого пользователя используя утилиту ktab из состава JDK 5.0. Например

ktab -k file:///c:/winnt/krb5.keytab -a WFTestUser@RUNA.RU

(В текущей реализации надо использовать имя WFTestUser@RUNA.RU)

5. Синхронизировать вермя на контроллере домена, workflow сервере и клиенте.
Детальное описание утилиты http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/ktab.html.

Как запустить клиент-оповещатель

Установите в af_delegate.properties ссылку на RUNA WFE сервер.

Установите swt-win32-3232.dll в директорию, ссылка на которую находится в переменной окружения Path.

Запустите javaw -cp .;rtn.jar ru.runa.notifier.PlatformLoader

javaw -cp .;rtn.jar ru.runa.notifier.PlatformLoader

Замечание. Можно не использовать переменную окружения Path. В этом случае положите swt-win32-3232.dll в ту же директорию, что и rtn.jar.
Запустите javaw -Djava.library.path=. -cp .;rtn.jar ru.runa.notifier.PlatformLoader
или runa_tasks.exe