IBM Platform Symphony RFE 89932 readme file

About setting AES128 key for Pluggable Authentication Module (PAM) plug-in

The PAM plug-in uses a static AES128 key to encrypt passwords between the client and management hosts. This fix provides documentation and a sample about how to use own AES128 key for encryption. The source code in this fix is for sample purpose only.

Readme file for: IBM® Platform Symphony
Product/Component Release: 7.1 Fix Pack 1
Update Name: Enhancement pack
Fix ID: sym-7.1-build435881-citi
Publication date: 30 December 2016
Last modified date: 27 February 2017

1. Scope

Applicability	
Operating system	RHEL 6.x or RHEL 7.x 64-bit
Symphony version	7.1 Fix Pack 1
Cluster types	This feature applies to Platform Symphony 7.1 Fix Pack 1 clusters

2. Configuration of this patch

1) Prerequisites

To compile the PAM plug-in, following packages are required to install in your development environment.

compat-libstdc++
gcc-c++
libstdc++
pam-devel
zlib-devel

To apply this fix, you must have a Platform Symphony 7.1 Fix Pack 1 cluster.

2) Installation files

The package includes the following files:

File name	Description
`symsetup7.1_lnx26-lib23-x64_build435881.tar.gz`	The package that contains the new feature for Linux x86_64 for Platform Symphony 7.1 Fix Pack 1

3) Change key and get PAM plug-in

a. Get package

Download the `symsetup7.1_lnx26-lib23-x64_build435881.tar.gz` package and decompress the package on the development environment with the following command:

```
>tar zxvf symsetup7.1_lnx26-lib23-x64_build435881.tar.gz
```

b. Change AES128 key and build the PAM plug-in

1. Open the `symsetup7.1_lnx26-lib23-x64_build435881/plugins/egodefault/sec_ego_ext_cipher.c` file.
2. Set your AES128 key using the variables `server_public_k` and `server_private_k`. The AES128 key that the PAM plug-in uses to encrypt passwords is defined in these two variables. These two variables must be set with the same key.
3. Change the `prefix` value before building the plug-in.
    a. Open the `Makefile.inc` file:

```
symsetup7.1_lnx26-lib23-x64_build435881/3rdparty/icu/3.2/linux2.6-glibc2.3-x86_64/lib/icu/3.2/Makefile.inc
```

    b. Change the `prefix` value:

```
prefix = ${HOME}/symsetup7.1_lnx26-lib23-x64_build435881/3rdparty/icu/3.2/linux2.6-glibc2.3-x86_64/
```

    where **${HOME}** is the location of the decompressed tar.gz in your environment.

    For example, If `symsetup7.1_lnx26-lib23-x64_build435881.tar.gz` is decompressed under `/home`, then prefix value is:

```
prefix = /home/symsetup7.1_lnx26-lib23-x64_build435881/3rdparty/icu/3.2/linux2.6-glibc2.3-x86_64/
```

4. Build the PAM plug-in:

```
>cd symsetup7.1_lnx26-lib23-x64_build435881
>make
```

5. Get PAM plug-in library and binary and configuration file

```
plugins/egodefault/sec_ego_ext_co.so
plugins/pam/egostashpass-pam
plugins/pam/sec_ego_ext_pam.so
plugins/pam/pamauth.conf
```

4) Installation procedure

a. Before installation

Log on to the management host as the cluster administrator and run:

```
>egosh service stop all
>egosh ego shutdown all
```

b. Installation steps

1. Back up the `sec_ego_ext_pam.so` file on all management hosts if it exists in the cluster.
2. Back up the `sec_ego_ext_co.so` file on all client hosts if it exists in the cluster.

c. Deploy the new PAM plug-in

1. Copy the `sec_ego_ext_pam.so` file to the `$EGO_LIBDIR` directory on all management hosts.
2. Copy the `sec_ego_ext_co.so` file to following directory:

   ```
   Symphony compute hosts: $EGO_LIBDIR
   Symphony client: $SOAM_HOME/lib64
   Symphony DE: $SOAM_HOME/7.1/linux2.6-glibc2.3-x86_64/ego_lib64
   ```

3. Copy the plug-in configuration file `pamauth.conf` to the `$EGO_CONFDIR` directory on all management hosts.
4. Copy the `egostashpass-pam` utility to the `$EGO_BINDIR` directory on the management host.

d. Configuration

1. Edit the `$EGO_CONFDIR/pamauth.conf` file to set values for mandatory parameters.

   Set the mandatory parameter `PAM_ADMIN` as the PAM account that should be mapped to the EGO user called `Admin`.

   Set the parameter `PAM_SERVICE` to the PAM policy file located under the `/etc/pam.d/` directory.

   Here is an example `pamauth.conf` file:

   ```
   # Mandatory parameters
   # PAM_ADMIN=<pam-account-name>
   # PAM account that should be mapped to EGO 'Admin' user.
   PAM_ADMIN=egoadmin
   # PAM_SERVICE=<pam-service-name>
   # PAM Service file (under /etc/pamd.) defining the
   # PAM policy to be used for EGO.
   PAM_SERVICE=sshd
   ```

2. Change the password of the `Admin` user in EGO using the utility `egostashpass-pam`.

   The password should be the same as the password use for the `PAM_ADMIN` account specified in the `pamauth.conf` file (in step 1). EGO needs to save the password of this account as it uses this password to generate credential for EGO Service Controller and other EGO services.

3. Edit the `$EGO_CONFDIR/ego.conf` file on management hosts to modify the value of the `EGO_SEC_PLUGIN` and `EGO_SEC_CONF` parameters as follows:

   ```
   EGO_SEC_PLUGIN=sec_ego_ext_pam
   EGO_SEC_CONF=plug-in-configuration-directory,created-ttl,plug-in-
   log-level,plug-in-log-directory
   ```

   Here is an example of `EGO_SEC_CONF` parameter:

```
EGO_SEC_CONF=/opt/egoshare/kernel/conf,0,INFO,/opt/egoshare/kerne
l/log
```

All the server side messages will be logged to the `ego_ext_plugin_server.log` file in the `plug-in-log-directory`.

4. Edit the `ego.conf` file on client hosts to modify the value of the `EGO_SEC_PLUGIN` parameter as follows:

   ```
   EGO_SEC_PLUGIN=sec_ego_ext_co
   ```

   The `EGO_SEC_CONF` parameter is optional on client hosts.

   Specify this parameter if log messages are required from the client side plug-in. The format is same as the format specified in step 3. All client side messages will be logged to the `ego_ext_plugin_client.log` file in the `plug-in-log-directory`.

e. After installation

1. Start the cluster using the following command:

   ```
   >egosh ego start all
   ```

2. Run the following command to map the PAM account to the EGO account after logging in as the `Admin` user:

   ```
   >egosh user add
   ```

f. Uninstallation

1. Shut down the cluster using the following commands:

   ```
   >egosh service stop all
   >egosh ego shutdown all
   ```

2. Restore the backup file `sec_ego_ext_pam.so` on all management hosts.

3. Restore the backup file `sec_ego_ext_co.so` on all compute and client hosts.

3. Copyright and trademark information