Readme for IBM® Spectrum Symphony RFE 101420

Readme file for: IBM Spectrum Symphony
Product/Component Release: 7.2
Fix ID: sym-7.2-build447463-citi
Publication date: April 14, 2017

This interim fix enhances Kerberos user authentication through the GSS-Kerberos plug-in to provide Microsoft Windows Active Directory (AD) integration, enabling you to consolidate Windows and Linux systems in your IBM Spectrum Symphony cluster.

Scope

Applicability	
Operating systems	Management hosts: • RHEL 6.5 64-bit Compute hosts: • RHEL 6.5 64-bit • Windows 2008 R2 64 bit Client hosts: • RHEL 6.5 64-bit • Windows 2008 R2 64 bit
Product version	IBM Spectrum Symphony 7.2

Limitations and know issues	
Limitations	• When logon with user in different domain against current host with trust, ensure domain be included as part of user name like “aduser@EXAMPLE.COM”. • If you enable AD users to be loaded automatically to the EGO user namespace by setting `ENABLE_AD_USERS_MANAGE=Y`, ensure: ✓ The “use_fully_qualified_names” parameter in the `/etc/sssd/sssd.conf` file must be configured as “False”. ✓ AD domain users must not already be defined in the EGO database.
Out of scope	This interim fix does not support the following functions when Kerberos authentication is enabled: • Logons to IBM Spectrum Symphony from Linux compute hosts in another domain with no trust. • Windows management hosts. • CLI on Windows. • WSDL API. • VEMKD and PEM Kerberos authentication on Windows. • Client authentication using TGT.

Installation and configuration

1. Prerequisites

To apply this interim fix, you must meet the following prerequisites:

- IBM Spectrum Symphony 7.2 must be installed on hosts in your cluster.
- The Windows AD domain must be installed and correctly configured; all hosts must be joined to the corresponding domain.

- Kerberos, the System Security Services Daemon (SSSD), and the Network Time Protocol (NTP) must be installed and configured correctly on all Linux hosts in your cluster.

2. Packages

This interim fix includes the following installation packages:

Package name	Description
sym-7.2.0.0_x86_64_build447463.tar.gz	Package for Linux management and compute hosts.
symclnt-7.2.0.0.x86_64_build447463.tar.gz	Package for Linux client hosts.
symde-7.2.0.0_x86_64_build447463.tar.gz	Package for Linux Developer Edition hosts.
egocore-3.6.0.0_build447463.msp	Package for Windows compute hosts.
soamcore-7.2.0.0_build447463.msp	Package for Windows compute hosts.
symde-7.2.0.0_build447463.msp	Package for Windows Developer Edition hosts.
symclnt-7.2.0.0_build447463.msp	Package for Windows client hosts.

3. Installation

Follow these steps to install this interim fix on hosts in your cluster:

Before installation

a. Log on to the master host as the cluster administrator, disable all applications, and shut down the cluster:

```
$ soamcontrol app disable all
$ egosh service stop all
$ egosh ego shutdown all
```

b. On all hosts, back up the following configuration file:

```
ego.conf
```

c. On Linux management and compute hosts, back up the following file:

```
$EGO_TOP/3.6/linux-x86_64/lib/sec_ego_gsskrb.so
$EGO_TOP/soam/7.2/linux-x86_64/lib64/libsoambase.so
```

d. On Linux client hosts, back up the following file:

```
$SOAM_HOME/lib64/sec_ego_gsskrb.so
$SOAM_HOME/lib64/libsoambase.so
```

e. On Linux Developer Edition hosts, back up the following file:

```
$SOAM_HOME/7.2/linux-x86_64/ego_lib64/sec_ego_gsskrb.so
$SOAM_HOME/7.2/linux-x86_64/lib64/libsoambase.so
```

f. On Windows compute hosts, back up the following files:

```
%EGO_TOP%\3.6\lib\sec_ego_sspikrb.dll
%EGO_TOP%\3.6\lib\sec_ego_sspikrb.pdb
%EGO_TOP%\soam\7.2\w2k3_x64-vc7-psdk\lib64\soambase.dll
%EGO_TOP%\soam\7.2\w2k3_x64-vc7-psdk\lib64\soambase.lib
%EGO_TOP%\soam\7.2\w2k3_x64-vc7-psdk\lib64\soambase.pdb
```

g. On Windows client hosts, back up the following files:

```
%SOAM_HOME%\lib64\sec_ego_sspikrb.dll
%SOAM_HOME%\lib64\soambase.dll
%SOAM_HOME%\lib64\soambase.lib
%SOAM_HOME%\lib64\soambase.pdb
```

h. On Windows Developer Edition hosts, back up the following files:

```
%SOAM_HOME%\7.2\w2k3_x64-vc7-psdk\ego_lib64\sec_ego_sspikrb.dll
%SOAM_HOME%\7.2\w2k3_x64-vc7-psdk\lib64\soambase.dll
%SOAM_HOME%\7.2\w2k3_x64-vc7-psdk\lib64\soambase.lib
%SOAM_HOME%\7.2\w2k3_x64-vc7-psdk\lib64\soambase.pdb
```

i. On all management hosts, clean up the GUI work directory and clear the browser cache. Delete all subdirectories and files in the following directories:

NOTE: If you configured the `WLP_OUTPUT_DIR` parameter and set `APPEND_HOSTNAME_TO_WLP_OUTPUT_DIR` to `true` in the `$EGO_CONFDIR/wlp.conf` file, clean up the `$WLP_OUTPUT_DIR/WEBGUI_hostname/gui/workarea/*` directory. If you configured the `WLP_OUTPUT_DIR` parameter and set `APPEND_HOSTNAME_TO_WLP_OUTPUT_DIR` to `false` in the `$EGO_CONFDIR/wlp.conf` file, clean up the `$WLP_OUTPUT_DIR/gui/workarea/*` directory.

```
$ rm -rf $EGO_TOP/gui/work/*
$ rm -rf $EGO_TOP/gui/workarea/*
$ rm -rf $EGO_TOP/kernel/rest/workarea/*
```

Installation

Log on to the host OS as the cluster administrator, then complete the steps corresponding to your host type:

Installing on Linux hosts:

a. On management and compute hosts, download the `sym-7.2.0.0_x86_64_build447463.tar.gz` file and decompress the package:

```
$ tar zxfo sym-7.2.0.0_x86_64_build447463.tar.gz -C $EGO_TOP
```

b. On client hosts, download the `symclnt-7.2.0.0.x86_64_build447463.tar.gz` file and decompress the package:

```
$ tar zxfo symclnt-7.2.0.0.x86_64_build447463.tar.gz -C $SOAM_HOME
```

c. On Developer Edition hosts, download the `symde-7.2.0.0_x86_64_build447463.tar.gz` file and decompress the package:

```
$ tar zxfo symde-7.2.0.0_x86_64_build447463.tar.gz -C $SOAM_HOME
```

Installing on Windows hosts:

- To perform an interactive installation, copy the Windows package to the corresponding hosts and double-click the `.msp` package.
- To perform a silent installation:

  a. On Windows compute hosts, download the `egocore-3.6.0.0_build447463.msp` and `soamcore-7.2.0.0_build447463.msp` file and install the package using the following command:

  ```
  C:\>msiexec /update <Sym_package_name_path> /l*v <Sym_install_log>
  /norestart /quiet REINSTALLMODE=omus
  ```

  where:

  - `Sym_package_name_path` is the fully qualified file name of the `.msp` package for this interim fix.
  - `Sym_install_log` is the log that captures details of the upgrade.

  For example, to update a Windows 64-bit Windows compute host, enter:

  ```
  C:\>msiexec /update C:\egocore-3.6.0.0_build447463.msp /l*v
  updateSym.log /norestart /quiet REINSTALLMODE=omus

  C:\>msiexec /update C:\soamcore-7.2.0.0_build447463.msp /l*v
  updateSym.log /norestart /quiet REINSTALLMODE=omus
  ```

  b. On Windows client hosts, download the `symclnt-7.2.0.0_build447463.msp` file and install the package using the following command:

  ```
  C:\>msiexec /update C:\symclnt-7.2.0.0_build447463.msp /l*v
  updateSym.log /norestart /quiet REINSTALLMODE=omus
  ```

  c. On Windows Developer Edition hosts, download the `symde-7.2.0.0_build447463.msp` file and install the package using the following command:

  ```
  C:\>msiexec /update C:\symde-7.2.0.0_build447463.msp /l*v
  updateSym.log /norestart /quiet REINSTALLMODE=omus
  ```

After installation

a. Enable Kerberos user authentication as described in the “Configuration" section.

b. Start the cluster and enable application:

```
$ egosh ego start all
```

```
$ soamcontrol app enable <appName>
```

Uninstallation

- To uninstall this interim fix from management and Linux compute hosts:

a. Log on to the master host as the cluster Administrator, disable all applications, and shut down the cluster:

```
$ soamcontrol app disable all
$ egosh service stop all
$ egosh ego shutdown all
```

b. Restore all the files that you backed up during installation on all hosts.

- To uninstall this interim fix from Linux client hosts:

  Recover all the files that you backed up during installation on client hosts.

- To uninstall this interim fix from Linux Developer Edition hosts:

  a. Log on to the Linux Developer Edition host as the cluster Administrator, shutdown IBM Spectrum Symphony Developer Edition processes:

  ```
  $ soamshutdown
  ```

  b. Restore all the files that you backed up during installation on Linux Developer Edition hosts.

  c. Start IBM Spectrum Symphony Developer Edition on Linux hosts:

  ```
  $ soamstartup
  ```

- To uninstall this interim fix from Windows hosts:

  - On Windows compute hosts, complete these steps:

    a. Get the Windows compute host `.msp` package for this interim fix (`egocore-3.6.0.0_build447463.msp` and `soamcore-7.2.0.0_build447463.msp`).

    b. From the IBM Spectrum Symphony 7.2 installation package, extract the `.msi` file with the same prefix as the interim fix package (`egocore-*`):

    ```
    C:\>sym-7.2.0.0.exe --extract <directory_to_extract_to>
    ```

    c. Roll back the interim fix:

    ```
    C:\>msiexec /uninstall <Sym_SP_path> /package <Sym_msi_path>
    /norestart /quiet /l*v <Sym_rollback_log>
    ```

    where:

    - `Sym_SP_path` is the fully qualified file name of the `.msp` interim fix package (`egocore-3.6.0.0_build447463.msp`,`soamcore-7.2.0.0_build447463.msp`).
    - `Sym_msi_path` is the fully qualified file name of the `.msi` file that extracted in **step b**.
    - `Sym_rollback_log` is the name of the log file that captures details of the rollback.

      For example:

      ```
      C:\>msiexec /uninstall C:\egocore-3.6.0.0_build447463.msp /package
      C:\egocore-3.6.0.0.msi /norestart /quiet /l*v rollbackSym.log
      ```

      ```
      C:\>msiexec /uninstall C:\soamcore-7.2.0.0_build447463.msp
      /package C:\soamcore-7.2.0.0.msi /norestart /quiet /l*v
      rollbackSym.log
      ```

  - On Windows client hosts, use the following command to uninstall this interim fix:

    ```
    C:\>msiexec /uninstall C:\symclnt-7.2.0.0_build447463.msp /package
    C:\symclnt-7.2.0.0.msi /norestart /quiet /l*v rollbackSym.log
    ```

  - On Windows Developer Edition hosts, use the following command to uninstall this interim fix:

```
C:\>msiexec /uninstall C:\symde-7.2.0.0_build447463.msp /package
C:\symde-7.2.0.0.msi /norestart /quiet /l*v rollbackSym.log
```

After uninstallation

Start the cluster and enable application:

```
$ egosh ego start all
$ soamcontrol app enable <appName>
```

Configuration

User authentication with security plug-ins is cluster-level configuration and requires all hosts in the cluster to use the same authentication mechanism. To enable GSS-Kerberos authentication in the Spectrum Symphony cluster, you must enable the GSS-Kerberos plug-in on all Linux hosts and enable the SSPI-Kerberos plug-in on all Windows hosts.

1. Enabling the GSS-Kerberos plug-in on management hosts

a. On each management host, modify the `$EGO_CONFDIR/ego.conf` file to use the GSS-Kerberos plug-in as follows:

- **`EGO_SEC_PLUGIN`:** Set the GSS-Kerberos plug-in for authentication to the Spectrum Symphony cluster:

  `EGO_SEC_PLUGIN=sec_ego_gsskrb`

- **`EGO_SEC_CONF`:** Specify the plug-in configuration in the format `<plug-in-configuration-directory,created-ttl,plug-in-log-level,plug-in-log-directory>`, where:

  - `plug-in-configuration-directory` specifies the location of the `sec_ego_gsskrb.conf` file (which is created in the next step).
  - `created-ttl` specifies the time-to-live duration for the authentication token sent from the client to server. Set this value to 0 or empty (indicating that the default value of 24 hours must be used).
  - `plug-in-log-level` specifies the plugin's log level. Valid values are: DEBUG, INFO, WARN, or ERROR. As a best practice, set the log level as ERROR or WARN. A lower level causes too many messages to be logged, making it harder to troubleshoot if required.
  - `plug-in-log-directory` specifies the absolute path to the directory containing the plug-in logs.

  For example:

  `EGO_SEC_CONF="/opt/EGO/kernel/conf,0,ERROR,/opt/EGO/kernel/log"`

  You can choose to configure only the location of the `sec_ego_gsskrb.conf` file and leave the other values to take defaults. For example:

  `EGO_SEC_CONF=”/opt/EGO/kernel/conf”`

- **`EGO_SEC_KRB_SERVICENAME`:** Specify the Kerberos principal name for the authentication server. The service principal can be a cluster-wide principal name.

To use a cluster-wide principal name, use a valid Kerberos principal name as its value. For example:
`EGO_SEC_KRB_SERVICENAME=sym72service/cluster1`

For more information on configuring the GSS-Kerberos plug-in, see https://www.ibm.com/support/knowledgecenter/SSZUMP_7.2.0/security/kerberos_auth_linux.html.

b. Edit the `sec_ego_gsskrb.conf` file in the directory specified by the `EGO_SEC_CONF` parameter, and define the following parameters in the file:

- **`REALM`**: Specify the MIT Kerberos realm name, which will be used as the realm of both user principal and service principal.

  For example:

  `REALM=EXAMPLE.COM`

- **`KRB5_KTNAME`:** Specify the absolute path to the keytab file containing one or more keys for the service principal, which is defined in the `EGO_SEC_KRB_SERVICENAME` parameter

  For example:

  `KRB5_KTNAME=/tmp/service.keytab`

- **`KERBEROS_ADMIN`:** Specify the Kerberos principal that will map to the built-in cluster administrator (“Admin”). All management hosts must use the same value for this parameter.

  For example:

  `KERBEROS_ADMIN=egoadmin`

  -or-

  `KERBEROS_ADMIN=egoadmin@EXAMPLE.COM`

  While you can add the Kerberos realm in the value, it is not required. It is good practice to define the realm only in the `sec_ego_gsskrb.conf` file.

  When you use the “Admin” user account to log on to Spectrum Symphony, the user account will be mapped to the specified Kerberos principal. You would then use the password of the Kerberos principal to log in to the cluster.

- **`KINITDIR`:** Specify the absolute path to the MIT Kerberos tool **kinit**, which is used to generate a TGT for the user principal when logging on. The MIT kinit is by default at `/usr/bin`. Only MIT Kerberos **kinit** is allowed; others (such as Java **kinit**) are not supported.

  For example:

  `KINITDIR=/usr/bin`

- **`ENABLE_AD_USERS_MANAGE`:** Optionally, specify `Y` to enable or `N` to disable AD users to be automatically added to the EGO database. By default, the parameter is not configured.

For more information on configuring the `sec_ego_gsskrb.conf` file, see https://www.ibm.com/support/knowledgecenter/SSZUMP_7.2.0/security/kerberos_auth_linux.html.

2. Enabling the GSS-Kerberos plug-in on Linux compute/Developer Edition/client hosts

a. On each compute, Developer Edition and client host, modify the **`EGO_SEC_PLUGIN`**, **`EGO_SEC_CONF`** and **`EGO_SEC_KRB_SERVICENAME`** parameters in the `ego.conf` file as configured on management hosts. Find the `ego.conf` file under `$EGO_CONFDIR` on compute, client and Developer Edition hosts.

For example:

```
EGO_SEC_PLUGIN=sec_ego_gsskrb
EGO_SEC_CONF=”/opt/EGO/kernel/conf”
EGO_SEC_KRB_SERVICENAME=sym72service/cluster1
```

b. Edit the `sec_ego_gsskrb.conf` file in the directory specified by the `EGO_SEC_CONF` parameter, and define the **`REALM`** and **`KINITDIR`** parameters in the file as configured on management hosts.

Optionally, define the **`KERBEROS_ADMIN`** parameter. If you define this parameter, use the same value as on management hosts. When this parameter is defined on compute hosts or Developer Edition hosts, you can log on to the cluster as the “Admin” user with the password of the `KERBEROS_ADMIN` principal (for example, “egoadmin”). When this parameter is not defined on compute hosts and its value on management hosts is not “Admin”, you cannot use the “Admin” user to log on from the compute host or Developer Edition host. To log on as the “Admin” user, you must use the principal defined by the `KERBEROS_ADMIN` parameter on management hosts (“egoadmin” in this example) as the user name.

For example:

```
REALM=EXAMPLE.COM
KERBEROS_ADMIN=egoadmin
KINITDIR=/usr/bin
```

3. Enabling the SSPI-Kerberos plug-in on Windows compute/Developer Edition/client hosts

a. Modify the `%EGO_CONFDIR%/ego.conf` file on all Windows compute, Developer Edition and client hosts to use the SSPI-Kerberos plug-in as follows:

- **`EGO_SEC_PLUGIN`:** Set the SSPI-Kerberos plug-in for authentication to the IBM Spectrum Symphony cluster.

  ```
  EGO_SEC_PLUGIN=sec_ego_sspikrb
  ```

- **`EGO_SEC_CONF`**: Specify the SSPI-Kerberos plug-in configuration in the format `<plug-in-configuration-directory,created-ttl,plug-in-log-level,plug-in-log-directory>`, similar to the **`EGO_SEC_CONF`** parameter configured on Linux hosts. Enclose the value within double quotes (“).

  For example:

  ```
  EGO_SEC_CONF="C:\SymphonyClient\Client72\conf,0,ERROR,C:\
  SymphonyClient\Client72\conf"
  ```

- **`EGO_SEC_KRB_SERVICENAME`:** Specify the Kerberos principal name for the authentication server, like the **`EGO_SEC_KRB_SERVICENAME`** parameter configured on Linux hosts.

For more information on configuring the SSPI-Kerberos plug-in, see https://www.ibm.com/support/knowledgecenter/SSZUMP_7.2.0/security/kerberos_auth_windows.html.

b. Edit the `sec_ego_gsskrb.conf` file in the directory specified by the `EGO_SEC_CONF` parameter and define the following parameters in the file:

- **`REALM`**: Specify the MIT Kerberos realm name, which will be used as the realm of the service principal.

  For example:

  ```
  REALM=EXAMPLE.COM
  ```

- **KERBEROS_ADMIN**: Specify the AD user or the Kerberos principal that will map to the user name of the built-in cluster administrator (Admin). When you use the “Admin” user account to log on, the user account will be mapped to the specified AD user or Kerberos principal.

  For example:

  ```
  KERBEROS_ADMIN=egoadmin
  ```

  The `KERBEROS_ADMIN` parameter is optional. If you choose to define this value, use the same value as on management hosts, except for realm or domain. If you choose not to configure this value and its value configured on management hosts is not “Admin”, you cannot use the “Admin” user account to log on from the client host. To log on as the Admin user, you must use the principal defined by the `KERBEROS_ADMIN` parameter on management hosts or the AD user with the same name as the Kerberos principal (“egoadmin” in this example) as the user name.

  You can include the domain of the AD user or the realm of the Kerberos principal in the value. If the value is an AD user with domain, ensure that the domain is the same as the host located AD domain. If the value is a Kerberos principal with realm, ensure that the realm is the same as the value of the `REALM` parameter.

  If the value does not contain realm or domain information, it is treated as an AD user. You would then use the password of the AD user when using the “Admin” user to log on.

- **DOMAIN**: Optionally, specifies the Windows domain name. This parameter takes effect if Windows SSPI get Windows host domain failed.

For more information on configuring the `sec_ego_gsskrb.conf` file, see https://www.ibm.com/support/knowledgecenter/SSZUMP_7.2.0/security/kerberos_auth_windows.html.

Feature usage

This section describes how to enable and use Kerberos authentication with Windows AD in the Spectrum Symphony cluster and makes the following assumptions about your cluster for illustration purposes:

- Your cluster includes two AD domains **SYMAD1.COM** and **SYMAD2.COM** and an external two-way trust exists between them. The corresponding realm is **SYMAD1.COM** and **SYMAD2.COM**.
- Your cluster setup is as follows:
  - Management and compute hosts are joined to **SYMAD1.COM**.
  - Linux client host **symclient1** (Developer Edition host working as client) is joined to **SYMAD1.com**.
  - Linux client host **symclient2** (Developer Edition host working as client) is joined to **SYMAD2.com**.
  - Windows client host **symclient3** (Developer Edition host working as client) is joined to **SYMAD1.com**.
- Two user accounts ‘**egoadmin**’ and ‘**ad1tester**’ exist in SYMAD1.COM domain. One service principal called “**vemkd**” exists in the SYMAD1.COM domain. The service principal is added to keytab “/tmp/service.keytab” on the master host.
- User account called ‘**ad2tester**’ exists in SYMAD2.COM domain.
- SYMAD1.COM and SYMAD2.COM are configured in the `/etc/krb5.conf` Kerberos file.
- SSSD is correctly configured on each Linux hosts.
- Enable Kerberos authentication as described in the “Configuration” section. The following steps are repeated for completeness:

- Enable the GSS-Kerberos plug-in on management hosts:
  a. Configure the `$EGO_CONFDIR/ego.conf` file on management hosts. For example:

     ```
     EGO_SEC_PLUGIN=sec_ego_gsskrb
     EGO_SEC_CONF="/EGOShare/kernel/conf,0,ERROR,/opt/EGO/kernel/log"
     EGO_SEC_KRB_SERVICENAME=vemkd/cluster1
     ```

  b. Edit the `sec_ego_gsskrb.conf` file under the directory specified by the `EGO_SEC_CONF` parameter and configure the file. For example:

     ```
     REALM=SYMAD1.COM
     KRB5_KTNAME=/tmp/service.keytab
     KERBEROS_ADMIN=egoadmin
     KINITDIR=/usr/bin
     ```

- Enable the GSS-Kerberos plug-in on Linux compute hosts and client hosts:
  a. Configure the `$EGO_CONFDIR/ego.conf` file on all Linux compute/client hosts. For example:

     ```
     EGO_SEC_PLUGIN=sec_ego_gsskrb
     EGO_SEC_CONF="/opt/EGO/kernel/conf,0,ERROR,/opt/EGO/kernel/log"
     EGO_SEC_KRB_SERVICENAME=vemkd/cluster1
     ```

  b. Edit the `sec_ego_gsskrb.conf` file under the directory specified by the `EGO_SEC_CONF` parameter on all Linux compute/client hosts and configure the file. For example:

     ```
     REALM=SYMAD1.COM
     KERBEROS_ADMIN=egoadmin
     KINITDIR=/usr/bin
     ```

- Enable the SSPI-Kerberos plug-in on Windows client host:
  a. Configure the `%EGO_CONFDIR%/ego.conf` file on Windows client host. For example:

     ```
     EGO_SEC_PLUGIN=sec_ego_sspikrb
     EGO_SEC_CONF="C:\Program
     Files\IBM\SpectrumComputing\SymphonyClient\Client72\conf,0,ERROR,C:\
     Program Files\IBM\SpectrumComputing\SymphonyClient\Client72\log"
     EGO_SEC_KRB_SERVICENAME=vemkd/cluster1
     ```

  b. Edit the `sec_ego_gsskrb.conf` file under the directory specified by the `EGO_SEC_CONF` parameter on Windows client host and configure the file. For example:

     ```
     REALM=SYMAD1.COM
     KERBEROS_ADMIN=egoadmin
     ```

- Start the cluster and enable applications:

  ```
  $ egosh ego start all
  $ soamcontrol app enable <appName>
  ```

- From management host in SYMAD1.COM domain, check to confirm that AD users can log on to the IBM Spectrum Symphony cluster:
  a. Log on as the “Admin” user. For example:

     ```
     $ egosh user logon -u Admin -x egoadminAD
     ```

b. Add the user “ad1tester” to EGO user namespace.

   If “`ENABLE_AD_USERS_MANAGE=Y`” is configured in `sec_ego_gsskrb.conf` file, the AD user already loaded to EGO user database automatically. If not, you need to add AD user “ad1tester” to the EGO user database manually. For example:

   ```
   $ egosh user add -u ad1tester -x 111
   ```

   Notes: When adding the user, you are not required to provide the same password in the AD. Any random string is sufficient, do not use this password for user logon.

c. Assign a role for the “ad1tester” user account. For example:

   ```
   $ egosh user assignrole -u ad1tester -r CONSUMER_ADMIN -p
   /SymTesting/Symping72
   ```

d. Log on as AD user “ad1tester”. For example:

   ```
   $ egosh user logon -u ad1tester -x passAD
   ```

- Log on to Linux client host **symclient1** in SYMAD1.COM and run workload to confirm that Kerberos authentication works:

  a. Log on as “Admin” user:

     ```
     $ soamlogon -u Admin -x egoadminAD
     ```

     NOTE: The “Admin” user is mapped to the Kerberos principal configured by the `KERBEROS_ADMIN` parameter; ensure that you use the password of the Kerberos principal.

  b. Run some sample Symphony command to view applications:

     ```
     $ soamview app
     ```

  c. Run the **symping** tool as “Admin”. For example:

     ```
     $ symping -u Admin -x egoadminAD
     ```

  d. Run **symping** as “ad1tester”. For example:

     ```
     $ symping -u ad1tester -x passAD
     ```

- Log on to Linux client host **symclient2** in another domain SYMAD2.COM with trust and run workload to confirm that Kerberos authentication works:

  a. Log on as “Admin” user. For example:

     ```
     $ soamlogon -u Admin –x egoadminAD
     ```

     NOTE: The “Admin” user is mapped to the Kerberos principal configured by the `EGO_SEC_KRB_SERVICENAME` parameter; ensure that you use the password of the Kerberos principal.

  b. Run the **symping** tool. For example:

     ```
     $ symping -u Admin -x  egoadminAD
     ```

  c. Run the **symping** tool. For example:

     ```
     $ symping -u egoadmin@SYMAD2.COM -x egoadminAD
     ```

  d. Add another domain SYMAD2.COM user to the EGO database. When adding the user, you are not required to provide the same password in AD; any random string is sufficient, do not use this password for user logon. For example:

     ```
     $ egosh user add -u ad2tester -x 111
     ```

  e. Assign role for the “ad2tester” user account. For example:

```
$ egosh user assignrole -u ad2tester -r CONSUMER_ADMIN -p
/SymTesting/Symping72
```

f. Run symping as “ad2tester”:

```
$ symping -u ad2tester@SYMAD2.COM -x passAD
```

NOTE: Domain name must be included when logon by user in another domain with trust.

- Log on to Windows client host **symclient3** in SYMAD1.COM domain using an AD user and run workload:
  a. Run **symping** as “Admin”:

```
$ symping -u Admin -x  egoadminAD
```

```
$ symping -u egoadmin -x egoadminAD
```

  b. Run **symping** as “ad1tester”:

```
$ symping -u ad1tester –x passAD
```

- Launch a web browser and log in to the management console.
  a. Log on as user “Admin” and password “egoadminAD”.
  b. Log on as user “ad1tester” and password “passAD”.

Best practices

When configuring and using Kerberos user authentication, take note of the following best practices:

- Do not include realm or domain information when configuring the `KERBEROS_ADMIN` and `EGO_SEC_KRB_SERVICENAME` parameters. The realm for Kerberos principal is configured by parameter `REALM` in the `sec_ego_gsskrb.conf` file, and the domain for AD user is the domain that the Windows host belongs to. You are not required to specify the two parameters.
- Use `ERROR` or `WARN` log level for the plug-in log. Many authentication events occur in the Spectrum Symphony cluster and all authentication servers and clients log to the two log files. With a low log level, too many messages will be recorded in the log.

Troubleshooting

When the GSS-Kerberos and SSPI-Kerberos plug-ins are enabled, use the following logs for troubleshooting:

- **Plug-in logs**: All errors that occur during authentication and errors caused by misconfiguration in the `sec_ego_gsskrb.conf` file are logged to the log files, according to the specified log level. Find the logs in the directory specified by the `EGO_SEC_CONF` parameter in the `$EGO_CONFDIR/ego.conf` file. All client messages are logged to the `ego_gssKerberos_plugin_client.log` file, and all server messages are logged to the `ego_gssKerberos_plugin_server.log` file. For both client and server, the logs that are generated during plug-in initialization are recorded in the `ego_gssKerberos_plugin_server.log` file. Use the Process ID in each message to distinguish logs for the different clients and servers.
- **Daemon’s logs**: All errors that occur before and after authentication in the plug-in and errors caused by parameters defined in the `$EGO_CONFDIR/ego.conf` file is logged to the Spectrum Symphony daemons logs (VEMKD, EGOSC and so on).

- **KDC log** (`krb5kdc.log` defined in `/etc/krb5.conf`): The KDC log records any errors when processes send AS_REQ and TGS_REQ to the KDC.

Copyright and trademark information