Readme File for IBM® Spectrum Symphony RFE 106792

Readme file for: IBM Spectrum Symphony
Product/Component Release: 7.2.0.2
Fix ID: sym-7.2.0.2-build493482-ms
Publication date: June 14, 2018

When your cluster is set up for GSS-Kerberos authentication, this enhancement enables you to log on and submit workload on compute/client hosts that use the default security plug-in by configuring the new `ACCEPT_DEFAULT_CLIENT` parameter in IBM Spectrum Symphony 7.2.0.2.

1. Scope

Before you install this enhancement in your cluster, note the following requirements:

Applicability	
Operating systems	RHEL 6.x, 7.x 64-bit
Product version	IBM Spectrum Symphony 7.2.0.2
Kerberos Version	MIT Kerberos version 1.10 or higher

2. Installation

Follow the instructions in this section to download and install this enhancement in your cluster.

Prerequisites

- Before applying this fix, IBM Spectrum Symphony 7.2.0.2 must be installed.
- Before enabling this configuration, your Kerberos environment must be set up.

Packages

File name	Description
`sym-7.2.0.2_x86_64_build493482.tar.gz`	Package for Linux management and compute hosts.
`symclnt-7.2.0.2.x86_64_build493482.tar.gz`	Package for Linux client hosts.

Before installation

1. 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
   ```

2. On all hosts in the cluster, back up the following configuration file:

   `$EGO_CONFDIR/ego.conf`

3. On each management and compute host, back up the following file:

   `$EGO_TOP/3.6/linux-x86_64/lib/sec_ego_gsskrb.so`

4. On each Linux client host, back up the following file:

   `$SOAM_HOME/lib64/sec_ego_gsskrb.so`

Installing on management and compute hosts

1. Log on to the host OS as the cluster administrator.

2. On each Linux management and compute host, download the `sym-7.2.0.2_x86_64_build493482.tar.gz` package and decompress it to the top-level installation directory:

   ```
   $ tar zxfo sym-7.2.0.2_x86_64_build493482.tar.gz -C $EGO_TOP
   ```

3. Verify that the permissions and ownership of the files are the same as they were before applying the fix. Update any file permissions or ownership as required.

Installing on client hosts

1. Log on to the host OS as the cluster administrator.
2. On each Linux client host, download the `symclnt-7.2.0.2.x86_64_build493482.tar.gz` file and decompress to the top-level installation directory:

   ```
   $ tar zxfo symclnt-7.2.0.2.x86_64_build493482.tar.gz -C $SOAM_HOME
   ```

3. Verify that the permissions and ownership of the files are the same as they were before applying the fix. Update any file permissions or ownership as required.

3. Configuration and usage

This section describes how to log on and submit workload on client/compute hosts that use the default security plug-in while GSS-Kerberos plug-in is configured on management hosts.

1. Enable Kerberos authentication on Linux management hosts in your cluster. See "Enabling Kerberos authentication on Linux hosts" topic in the online IBM Knowledge Center.
2. Modify the `$EGO_CONFDIR/sec_ego_gsskrb.conf` file to enable GSS-Kerberos authentication for the client that uses the default security plug-in by defining the **`ACCEPT_DEFAULT_CLIENT`** parameter. Valid values are `Y` (enabled) or `N` (disabled). Default is `N`.

   `ACCEPT_DEFAULT_CLIENT=Y`

3. Start the cluster and enable applications:

   ```
   $ egosh ego start
   ```

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

4. From a Linux compute host that uses the default security plug-in, log on and run a client application (for example, `symping`) as follows:

   a. Log on to the cluster as an EGO user by using the "`egosh user logon`" command:

      ```
      $ egosh user logon –u Admin –x Admin
      ```

   b. Log on as an EGO user by using the "`soamlogon`" command:

      ```
      $ soamlogon –u Admin –x Admin
      ```

   c. Run `symping` as an EGO user:

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

5. From a Linux client host that uses the default security plug-in, run a client application (for example, `symping`) as an EGO user:

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

4. Uninstallation

Follow the instructions in this section to uninstall this enhancement in your cluster, if required:

Uninstalling on management and compute hosts

1. 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
   ```

2. On each management and compute host, restore all the files that you backed up during installation.
3. Start the cluster:

   ```
   $ egosh ego start all
   ```

Uninstalling on client hosts

On each client host, restore the file that you backed up during installation.

5. Copyright and trademark information