Readme File for Universal User Group Support with SSPI plug-in in IBM® Spectrum Symphony

Readme file for: IBM Spectrum Symphony
Product/Component Release: 7.2.0.1
Fix ID: sym-7.2.0.1-build473417-bmo
Publication date: November 16, 2017

This update enhances the SSPI-Kerberos plug-in in IBM Spectrum Symphony 7.2.0.1 to support Microsoft Active Directory (AD) Universal User Groups. This update is based on the RFE with Fix ID sym-7.2.0.1-build459298-bmo, which implements Kerberos-based single sign-on for Windows through the SSPI-Kerberos plug-in.

Scope 3
Installation 3
System requirements 3
Packages 3
Installing on Windows management hosts 3
Configuration and usage 4
Prerequisites and considerations 4
Configuring universal user groups 4
Verifying universal user groups 5
Uninstallation 6
Troubleshooting 6
Copyright and trademark information 7

1. Scope

This scope of this update is identical to the scope specified for sym-7.2.0.1-build459298-bmo. For details, see the Readme File.

2. Installation

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

System requirements

Windows x86_64 hosts

Packages

Package name	Description
`sym-7.2.0.1-egocore-3.6.0.1_build473417.msp`	Packages for Windows management hosts.
`sym-7.2.0.1-soammgmt-7.2.0.1_build473417.msp`	

Installing on Windows management hosts

This enhancement applies only to Windows management hosts. To install this enhancement, download and install the `sym-7.2.0.1-egocore-3.6.0.1_build473417.msp` and `sym-7.2.0.1-soammgmt-7.2.0.1_build473417.msp` packages on each management host in your cluster as follows:

a. Log on to the master host as the cluster admin (the AD user specified in the `KERBEROS_ADMIN` parameter in the `sec_ego_sspikrb.conf file`), disable your applications, and stop all system services:

```
> soamcontrol app disable all
> egosh service stop all
```

If the cluster admin is not the AD user specified as the cluster administrator when IBM Spectrum Symphony was installed, launch the command prompt as that cluster administrator and shut down the cluster; otherwise, run the following command directly to shut down the cluster:

```
> egosh ego shutdown all
```

b. On each Windows management host, back up the following files:

```
%EGO_CONFDIR%\sec_ego_sspikrb.conf
```

c. Install this enhancement on each management host as follows:

- For an interactive installation, copy the `sym-7.2.0.1-egocore-3.6.0.1_build473417.msp` and `sym-7.2.0.1-soammgmt-7.2.0.1_build473417.msp` packages to each management host, double-click each .msp package, and follow the prompts.
- For a silent installation:

1. Copy the `sym-7.2.0.1-egocore-3.6.0.1_build473417.msp` and `sym-7.2.0.1-soammgmt-7.2.0.1_build473417.msp` packages to each management host.
2. Install the packages using the following commands:

   ```
   C:\>msiexec /update C:\sym-7.2.0.1-egocore-
   3.6.0.1_build473417.msp /l*v updateSymCore.log /norestart /quiet
   REINSTALLMODE=omus
   ```

   ```
   C:\>msiexec /update C:\sym-7.2.0.1-soammgmt-
   7.2.0.1_build473417.msp /l*v updateSymMgmt.log /norestart /quiet
   REINSTALLMODE=omus
   ```

   The command syntax is as follows:

   ```
   > 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 enhancement.
   - <*sym_install_log*> is the log file for the upgrade.

3. Configuration and usage

Prerequisites and considerations

Before configuring universal user groups, ensure that the cluster has been configured as described in the “Configuration and usage” section in the Readme File for sym-7.2.0.1-build459298-bmo.

Take note of the following considerations for universal user groups:

- When a universal user group is configured in IBM Spectrum Symphony, ensure that at least one active Global Catalog located DC exists in the group-located forest, which can serve the universal user group information retrieval request.
- Loading users and groups with the same name from different domains is not recommended. Identical user names or user group names under different domains are treated as the same user or user group for authorization purposes. When this happens, a user “domainA\userA” is granted permissions when a user “domainB\userA” is granted permissions. The same behavior applies for user groups.

Other considerations are similar to sym-7.2.0.1-build459298-bmo.

Configuring universal user groups

On each management host, modify the following parameters in the `%EGO_CONFDIR%/sec_ego_sspikrb.conf` file for universal user groups:

- **`INCLUDED_USERGROUP`**: To load some universal user groups, add the groups in the format *`domain-name1`*`\`*`groupname1`*,*`domain-name2`*`\`*`groupname2,….`* Ensure that you use the NETBIOS domain name.

  For example:
  `INCLUDED_USERGROUP=ADDOMAIN1\globalgroup1,ADDOMAIN2\globalgroup2,ADDOMAIN1\universalgroup1,ADDOMAIN2\universalgroup2`

- **`EXCLUDED_USERGROUP`**: To exclude some universal user groups, add the groups in the format *`domain-name1`*`\`*`groupname1`*,*`domain-name2`*`\`*`groupname2,….`* Ensure that you use the NETBIOS domain name.

For example:
`EXCLUDED_USERGROUP=ADDOMAIN1\globalgroup3,ADDOMAIN1\universalgroup3`

As a best practice, use this parameter or the `INCLUDED_USERGROUP` parameter to limit the users or user groups you want to load to IBM Spectrum Symphony. You can only configure one of the two parameters; if both are configured, neither parameter take effect.

- **`USERLOAD_DOMAIN`**: After configuring universal user groups in the `INCLUDED_USERGROUP` or `EXCLUDED_USERGROUP` parameter, specify the group domain. Ensure that you use the NETBIOS domain name.

  For example:
  `USERLOAD_DOMAIN=ADDOMAIN1,ADDOMAIN2`

- (Optional) Remove the `LOAD_USERS_FROM_GROUP` parameter as its configuration no longer takes effect.

Verifying universal user groups

This section makes the following assumptions for illustration purposes:

- Management hosts are located in domain ad1.test.com. Another domain ad2.test.com is in the same forest as domain ad1.test.com but in different trees.
- A universal user group AD1\uGroup1 is configured in the `INCLUDED_USERGROUP` parameter. This group contains users from domains in the tree of ad1.test.com and domains in the tree of ad2.test.com.
- The following users exist in group AD1\uGroup1: AD1\userA and AD2\userB.

Follow these steps to test whether universal user groups are loaded to IBM Spectrum Symphony and whether the correct roles and permissions are assigned:

1. Start the cluster, start all services, and enable applications:

   ```
   > egosh ego start all
   ```

   ```
   > soamcontrol app enable appName
   ```

2. Log on to a management host as the cluster administrator (the AD user specified as the `KERBEROS_ADMIN`). Check whether the expected users and user groups are loaded successfully:

   ```
   > egosh user list –l
   ```

   The group AD1\uGroup1 will show in the format @AD1\ugroup1; all users in the AD1\uGroup1 group will show, such as AD1\userA and AD2\userB.

3. Check users in the AD1\uGroup1 group:

   ```
   > egosh user list –g AD1\uGroup1
   ```

   All users in the group AD1\uGroup1 – AD1\userA and AD2\userB – will show.

4. Assign the “Consumer Admin” role to the AD1\uGroup1 group:

   ```
   > egosh user assignrole -u AD1\uGroup1 -r "Consumer Admin" -p /
   ```

   Check roles and permissions of the AD1\uGroup1 group and user AD2\userB:

   ```
   > egosh user roles4user -u @AD1\uGroup1
   ```

   ```
   > egosh user roles4user -u AD2\userB
   ```

   ```
   > egosh user permissions4user -u @AD1\uGroup1
   ```

   ```
   > egosh user permissions4user -u AD2\userB
   ```

Both the AD1\uGroup1 group and user AD2\userB are assigned the “Consumer Admin” role successfully and inherit all the permissions of the “Consumer Admin” role.

5. Log on to a compute host in the ad2 domain as user AD2\userB and submit the **symping** application:

   ```
   > symping -u "" -x ""
   ```

   The user can run **symping** successfully.

4. Uninstallation

If required, follow these steps to uninstall this enhancement:

a. Log on to the master host as the cluster administrator (the AD user specified in the `KERBEROS_ADMIN` parameter in `sec_ego_sspikrb.conf`), disable applications, and stop all system services:

   ```
   > soamcontrol app disable all
   ```

   ```
   > egosh service stop all
   ```

   If the cluster administrator is not the AD user specified as the cluster administrator when IBM Spectrum Symphony was installed, launch the command prompt as that cluster administrator and shut down the cluster; otherwise, run the following command directly to shut down the cluster:

   ```
   > egosh ego shutdown all
   ```

b. To roll back from the Windows Control Panel, go to **Control Panel > Programs and Features > View installed updates**, click `Update for Symphony 7.2.0.1 (build “473417”)` and click **Uninstall**.

c. To roll back from the IBM Spectrum Symphony command prompt, enter the following commands:

   ```
   C:\> msiexec /uninstall {50F98099-0EFB-459D-B1B4-346ED8D85E7F} /package
   {90B5C3E7-18A8-473C-929B-F9101A58E256} /norestart /quiet /l*v
   sym_rollbackcore.log
   ```

   ```
   C:\> msiexec /uninstall {1AC60925-4437-40C9-90F3-CE142E973C89} /package
   {403A5A97-7878-40D1-8C25-873F0F6BA8A5} /norestart /quiet /l*v
   sym_rollbackmgmt.log
   ```

   The command syntax is as follows:

   ```
   > msiexec /uninstall <interim_fix_code> /package <product_code>
   /norestart /quiet /l*v <rollback_log>
   ```

   where:

   - *<interim_fix_code>* is the identifier of the .msp package for this enhancement.
   - *<product_code>* is the identifier of the .msi file in the product installation package.
   - *<rollback_log>* is the name of the log file to capture details of the rollback.

d. On each management host, restore the following files from your backup:

   ```
   %EGO_CONFDIR%\sec_ego_sspikrb.conf
   ```

5. Troubleshooting

All errors that occur when users and groups (including universal user groups) are loaded to IBM Spectrum Symphony are logged to the plug-in’s server logs file

`ego_sspiKerberos_plugin_server.log`. If any user or group is not loaded as expected, use this log to locate the reasons for the error.

6. Copyright and trademark information