IBM® Platform Symphony

Best practices

Configuring AD SSO for Platform Symphony API

Xiaoping Zheng
IBM, Software Defined Systems
QA, Platform Symphony

Issued: April 2015

Contents

Configuring AD SSO for Platform Symphony API

The ADD SSO feature is intended for configuring a normal domain user that has full access to user and group account information and is applicable to Platform Symphony 6.1.1 and 7.1 on Windows.

Prerequisites

Before completing the steps in this topic, ensure that the normal domain user meets the following prerequisites:

1. The domain user must have full access to user and group account information. To do this, follow these steps:

    a. Open the Active Directory Users and Computers Microsoft Management Console by clicking Run, typing dsa.msc, and clicking OK.

    b. From the View menu, select Advanced Features.

    c. Select the Users list.

    d. Double-click your domain user.

    e. Select the Security tab.

    f. Select Full Control Permissions for Everyone.

    g. Click Apply.

2. The domain user is a domain administrator (that is, the domain user must belong to the local Administrator group).

Before configuring AD single sign-on, ensure you have the following prerequisites:

1. For all hosts (management, compute, and client), the AD single sign-on API is supported on Windows only. (Note that this is different from the AD support on Platform Symphony; the single sign-on feature is limited to Windows only for all hosts.)
2. The service principal name (SPN) must be configured correctly.
3. The SPN is the name by which a client uniquely identifies a service instance.

Use the setspn a command in the format setspn a service_name/host

DomainUser, where:

– service_name can be sd or vemkd.

– host is the fully-qualified host name (with domain suffix) of the host.

For example, sd/host.domain.com.

For failover, set the SPN for the target service on all management hosts in the cluster.

Use the AD_SPN_SERVICENAME field in the adauth.conf file, in the format AD_SPN_SERVICENAME=service_name/{host}, where service_namecan be sd or vemkd.

Note that here, host is not a variable.

For example, sd/{host} or vemkd/{host}.

Steps

1. On every host, edit the adauth.conf file to set the values of the parameters in the following table:

   Notes:

   For management hosts and compute hosts the adauth.conf file is under $EGO_CONFDIR.

   For client hosts, add an adauth.conf file under $SOAM_HOME\conf.

Parameter	Mandatory or optional	Description
AD_SSO	Mandatory to enable SSO	Enables SSO on all hosts, management, compute, and client hosts. Valid values: Y N (default) If SSO is enabled on management hosts (AD_SSO=Y), compute or client hosts can use the original AD plug-in or use SSO (requires AD_SSO=Y on compute or client hosts). If AD_SSO is not enabled on management hosts, compute hosts or client hosts cannot use the SSO feature even if AD_SSO=Y on the compute or client hosts.
AD_SPN_SERVICENAME	Mandatory if SSO is enabled	Specifies a service principal name by which a client uniquely identifies an instance of a service. Valid format: service_name/{host} where, service_name can be sd or vemkd. Note that here, host is not

		a variable. For example, sd/{host}. If SSO is enabled (AD_SSO=Y), but AD_SPN_SERVICENAME is not defined, the AD plug-in does not load successfully.
AD_ADMIN	Mandatory	Specifies the AD user admin on management hosts. On other hosts, use an asterisk (*) as a placeholder for the parameter.

2. On every host, edit the ego.conf file to set the values of the parameters in the following table:

Notes:

For management hosts and compute hosts the ego.conf file is under $EGO_CONFDIR.

For client hosts, the ego.conf file is under $SOAM_HOME\conf.

Parameter	Mandatory or optional	Description
EGO_SEC_PLUGIN	sec_ego_ext_ad	Specifies the AD plug-in.
EGO_SEC_CONF	For management and compute hosts: $EGO_TOP\kernel\conf,0, DEBUG,$EGO_TOP \kernel\log For client hosts: $SOAM_HOME\conf,0, DEBUG,$SOAM_HOME \log	Specifies settings for the AD plug-in in this format: <plug-in_configuration_directory, created-ttl, plug-in_log_level, plug-in_log_directory> All server-side messages are logged to ego_ext_plugin_server.log in the plugin-log directory. All client-side messages are logged to ego_ext_plugin_client.log in the plugin-log directory.

3. Map the domain administrator password to the cluster administrator's password:

```
# egostashpass-AD
```

4. On all the management hosts, start the LIM process as the domain administrator:

a. Click Start > Run.

b. Enter services.msc and click OK.

c. Locate Platform LIM, right-click the service, and click Properties.

d. Click the Log on tab.

e. Select This account and enter details for the domain administrator.

f. Click OK.

5. Ensure that the VEMKD, SD, and RS services run as the same user set up in the setspn command.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

Without limiting the above disclaimers, IBM provides no representations or warranties regarding the accuracy, reliability or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any recommendations or techniques herein is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Anyone attempting to adapt these techniques to their own environment does so at their own risk.

This document and the information contained herein may be used solely in connection with the IBM products discussed in this document.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.