CONFIGURING SSO FOR SHAREPOINT DOCUMENTS WITH KERBEROS/SPNEGO AUTHENTICATION

Overview

Configuring IBM® Content Analytics with Enterprise Search (ICA) to support single sign-on (SSO) authentication for secure search of Microsoft SharePoint documents involves the following steps:

- Installing ICA on WebSphere® Application Server (WAS). For installation instructions, see the fix pack readme file.
- Ensuring that Kerberos/SPNEGO-based application SSO is configured correctly between the SharePoint and ICA application servers. Verify that when you move from one application to the other in your web browser that you are not prompted to log in.
- Configuring the target SharePoint server, Internet Information Server, and Active Directory to allow Kerberos token propagation for the WAS instance that resides in the ICA server.
- Deploying a web service that is bundled with ICA on the SharePoint server.

After completing these steps, you can create a SharePoint crawler and configure the crawler to support secure search through SSO authentication.

SharePoint server configuration for Kerberos

The SharePoint server must be configured to use Kerberos authentication. Because the crawler requires NTLM authentication, the SharePoint server must support both the Kerberos/SPNEGO and NTLM protocols. Otherwise, the SharePoint crawler is not able to collect documents.

To configure the SharePoint server, see the section about Implementing Windows Authentication Methods in the following document, *Plan authentication methods (SharePoint Server 2010)*:

http://technet.microsoft.com/en-us/library/cc262350.aspx#section9

After setting up the server authenticaton, you must configure the client. The client must be in a domain member machine, and must log in as a domain user.

During configuration, it's important to understand the concept of Service Principal Name (SPN) on IIS. For assistance, see the following document, *How to use SPNs when you configure Web applications that are hosted on Internet Information Services*:

http://support.microsoft.com/kb/929650

In a later configuration task, the name of the SPN that is assigned to the SharePoint server (IIS) will be needed. You might want to make a note of the SPN in this step.

When you finish this configuration task, you can log in to SharePoint without being prompted for credentials; you are recognized as the domain user that you used for Windows OS login.

WebSphere Application Server configuration to enable SPNEGO-based application SSO

Before configuring secure search SSO with Kerberos authentication, application SSO between the SharePoint and ICA servers must be configured properly. Because ICA is installed on WAS, this task involves configuring WAS to enable SPNEGO-based SSO.

For detailed procedures about configuring WAS, see the following information:
http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/csec_SPNEGO_explain.html

http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_SPNEGO_config.html

During the configuration task, it's important to enable the "Enable delegation of Kerberos credentials" capability. This function allows the ICA security processor to reuse the user's Kerberos credential, which is used for logging in to WAS, to access the SharePoint server on behalf of the user.

When you finish this configuration task, you can log in to WAS without being prompted for credentials; you are recognized as the domain user that you used for Windows OS login. You can move from a page hosted by WAS to a page on the SharePoint server without any authenticatoin challenges.

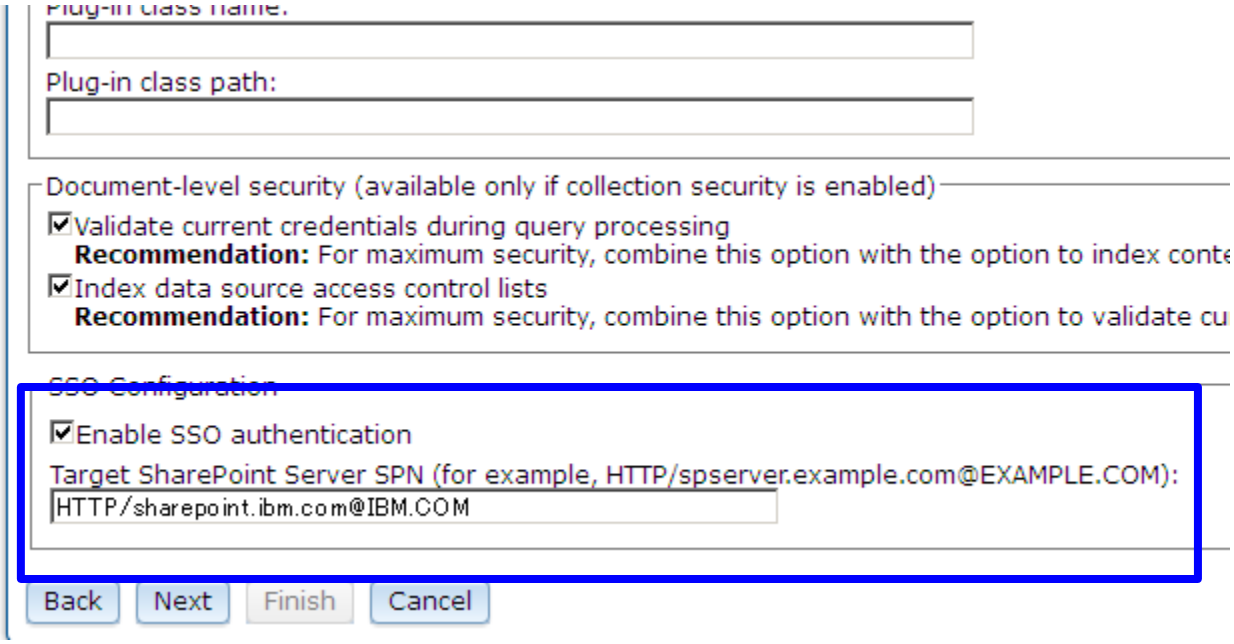
Web service deployment

Before you configure a SharePoint crawler, you must deploy provided web services on the SharePoint server. These web services enable support for several functions, including farm-aware crawling and secure search. For instructions, see the following topic:

http://pic.dhe.ibm.com/infocenter/analytic/v3r0m0/topic/com.ibm.discovery.es.ad.doc/iiysacspwebsvc.htm

ICA SharePoint crawler configuration to enable SPNEGO-based secure search SSO

If the environment meets the preceding pre-requisites, ICA is now ready to be configured. To create a SharePoint crawler that supports SPNEGO authentication for secure search processing, select the "Enable SSO authentication" check box on the first page of the SharePoint crawler creation panel (the crawler properties) and specify the SharePoint server's SPN.



This is the only difference between SSO and non-SSO cases. You can create an index with the same procedures that you use for indexing other secure collections.

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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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.

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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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.

Trademarks

IBM, the IBM logo, ibm.com, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.