IBM Endpoint Manager for Software Use Analysis

Version 9.1 (includes update 9.0.1, 9.0.1.1 and 9.0.1.2)

Security Guide

IBM Endpoint Manager for Software Use Analysis

Version 9.1 (includes update 9.0.1, 9.0.1.1 and 9.0.1.2)

Security Guide

Security Guide

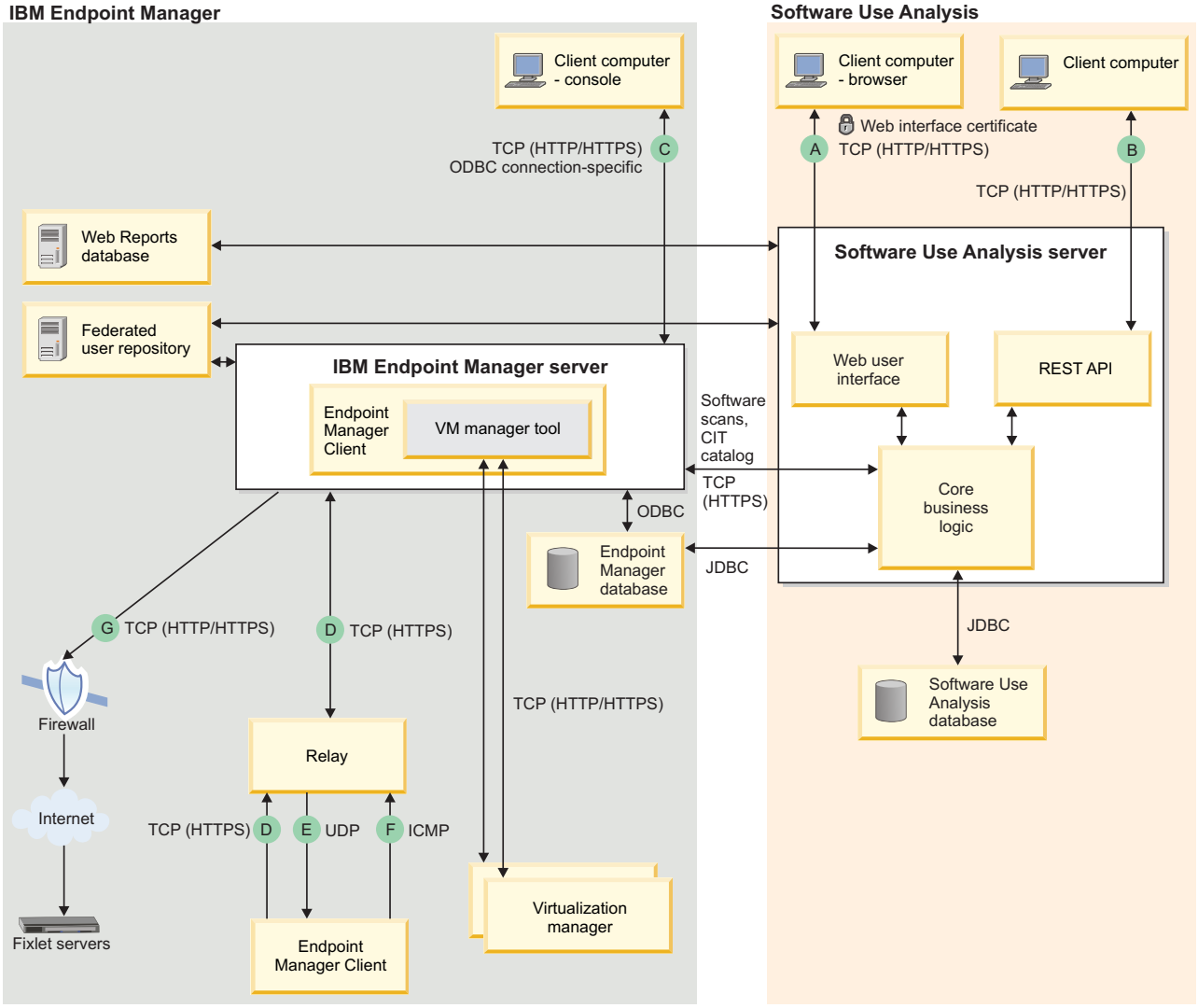
This edition applies to version 9.0.1.2 of IBM Endpoint Manager for Software Use Analysis (product number 5725-F57) and to all subsequent releases and modifications until otherwise indicated in new editions.

Security

You can configure different security features to adequately protect business assets and resources in the data model when using Software Use Analysis.

Flow of data

There are several different interactions that occur between the components of the Software Use Analysis infrastructure and between the user and tool.



Software Use Analysis domain

Interaction	Type	Connection	Description
A	Web browser data traffic	Port	By default, the web browser connects to the Software Use Analysis server using port 9081 (HTTPS). You can disable the SSL/TLS connection tunnelling.
		Origination	The web browser connects to the Software Use Analysis server.
B	REST API data traffic	Port	By default, the web browser connects to the Software Use Analysis server using port 9081 (HTTPS). You can disable secure connection.
		Origination	A client that uses REST API connections.

IBM® Endpoint Manager domain

Interaction	Type	Connection	Description
C	IBM Endpoint Manager Console data traffic	Port	Consoles connect to root server using HTTPS 52311 for all interactions
		Origination	The IBM Endpoint Manager console connects to the RootServer service.
		Network controls:	There is a "refresh rate" for each IBM Endpoint Manager console user (default 15 seconds)
D	Gather, post, download	Port	Port 52311 is configurable by the Endpoint Manager administrator at installation time.
		Origination	The Endpoint Manager client initiates the request to the Endpoint Manager relay or server.
		Network controls:	• Configurable bandwidth throttling to Endpoint Manager relay or clients • Configurable gather interval. The default is *1* per day per fixlet site. • Configurable minimum time to wait between posts. The default is *15* seconds. • Configurable temporal distribution (spread out downloads over time) per action • The ability to set "policy" to prevent computers from downloading files if they are not pointed at the proper Endpoint Manager relay
E	UDP “new information” message	Port	Port 52311 is configurable by the Endpoint Manager administrator at installation time.
		Origination	The UDP messages are sent from the Endpoint Manager clients' immediate “parent”, which can be either an Endpoint Manager relay or server.
		Network controls:	• Configurable limit of the number of UDP messages sent at one time from an Endpoint Manager relay • Configurable limit of the amount of time to wait after sending UDP messages from an Endpoint Manager relay

Interaction	Type	Connection	Description
F	Relay selection	Port	The ICMP protocol does not use a port.
		Origination	Each Endpoint Manager client sends progressive “rounds” of ICMP packets to each relay with increasing TTLs until an Endpoint Manager relay responds. For example, in a network of 2 relays, one 1 hop away and one 2 hops away, the Endpoint Manager client sends an ICMP message to both with TTL 1 and receives 2 “time exceeded” messages from the local router. The Endpoint Manager client then sends an ICMP message to both relays with TTL 2 and receives one “time exceeded” message and one reply message. The Endpoint Manager client then chooses the relay that is one hop away.
		Network controls	• Relay auto-selection can be disabled. • Configurable interval for when the Endpoint Manager clients perform auto-selection • Configurable limit on the maximum number of ICMP packets to send out in a time interval • Configurable limit on the maximum number of “rounds” to send out during relay auto-selection
G	New data download from external IBM fixlet servers	Port	80 (typically); possibly 21, 443
		Origination	The Endpoint Manager server connects to the IBM fixlet servers
		Network controls	There is a configurable interval that the Endpoint Manager server checks for new fixlet messages.

The following database protocols are used:

- ODBC
- JDBC

Security configuration scenarios

When you configure security settings, ensure that the combination of security modes that you set up on the side of Endpoint Manager and Software Use Analysis is supported.

Legend:

- ✔ - the mode is enabled
- ANY - the mode is either enabled or disabled

Table 1. Security configuration scenarios

Endpoint Manager		Software Use Analysis		Endpoint Manager on Windows and MSSQL	Endpoint Manager on Linux and DB2
Enhanced security	SHA1	TLS 1.2	SP800-131a		
	✔	✔		Supported	Supported
✔		✔		Supported	Supported
✔	✔	✔		Supported	Supported
	✔			Supported	Supported
✔				Supported	Supported
✔	✔			Supported	Supported
✔		✔	✔	Not supported	Supported

Table 1. Security configuration scenarios (continued)

Endpoint Manager		Software Use Analysis		Endpoint Manager on Windows and MSSQL	Endpoint Manager on Linux and DB2
Enhanced security	SHA1	TLS 1.2	SP800-131a		
✔	✔	✔	✔	Not supported	Supported
	✔	✔	✔	Not supported	Not supported
	✔		✔	Not supported	Not supported
✔			✔	Not supported	Not supported
✔	✔		✔	Not supported	Not supported
		ANY	ANY	Not supported	Not supported

Configuring secure communication

A digital certificate is a signed public key that is accompanied by information about the key owner. The public key always has a private key that is associated with it. The Software Use Analysis server can use SSL if the server possesses both the certificate and the private key that is associated with it. Security of your access to the web console of Software Use Analysis depends on the security of the digital certificate, and its private key, that the server uses for protecting the communication. By default, SSL is enabled on the server. However, the initial configuration is based on a temporary self-signed certificate and is not intended to be used in the production environment. The initial certificate should be replaced with a server certificate that is signed by a certificate authority (CA) that you trust.

Before you begin

- Enabling or disabling the use of SSL changes the web address of the Software Use Analysis server. After you perform one of those actions, you must run a data import so that the web address is updated for the fixlets that use it to download files from the Software Use Analysis server.

Procedure

1. In the top navigation bar, click **Management** > **Server Settings**.
2. Select **Use SSL**. The Certificate subsection opens.
3. Optional: Select **Use TLS 1.2**.

   Important:
   - To use TLS 1.2, ensure that your browser supports TLS 1.2, and that it is enabled.
   - To fulfill all the requirements for SP800-131 compliance, see: Enabling SP800-131 compliance.
4. Provide information about the security certificate.
   - If you have a certificate that is provided by a certificate authority (CA):
     a. Select **Import a PEM encoded private key and certificate**.
     b. Click **Browse** to locate the private key in the computer file system.
     c. In the **Private key password** field, enter the password for the key.
     d. Click **Save**.

     Note: The certificate and the key must be PEM-encoded.

- If you want to generate a new self-signed certificate and use it with the server:

  Restriction: A self-signed certificate contains a public key, information about the owner of the certificate, and the owner's signature. Because such a certificate is signed by its own private key, it does not provide means to verify the origin of the certificate through a trusted certificate authority.

  a. Select **Generate a self-signed certificate**.
  b. Specify the certificate subject *common name*. The common name must correspond to the DNS name of the Software Use Analysis server.
  c. In the **Expiration Date** field, enter the date when the certificate expires.
  d. Click **Save**.

  Note: Most of browsers display a warning message when a self-signed certificate is used.

5. Restart the server.

Assuring compliance with federal encryption standards

You can configure Software Use Analysis to be compliant with the Federal Information Processing Standard requirements that are related to encryption.

Federal Information Processing Standard 140-2

Federal Information Processing Standards (FIPS) are standards and guidelines that are issued by the National Institute of Standards and Technology (NIST) for federal government computer systems.

Government agencies and financial institutions use Federal Information Processing Standard (FIPS) to ensure that the products conform to specified security requirements. For more information about these standards, see the NIST website.

FIPS 140-2 is the standard that defines the security requirements for cryptographic modules that are used within a system that handles sensitive but unclassified information. Compliance with the FIPS 140-2 standard has two aspects that affect Software Use Analysis: the algorithms that are used to manage sensitive data must be FIPS-approved and a FIPS-approved implementation must be used when data is transmitted with the SSL/TLS.

Software Use Analysis uses the FIPS 140-2 approved cryptographic providers for cryptography:

- IBMJCEFIPS (certificate 376)
- IBMJSSEFIPS (certificate 409)
- IBM Crypto for C (ICC) (certificate 384)

The certificates are listed on the NIST web site.

Configuring the server to achieve FIPS compliance

You can assure compliance with the FIPS 140-2 standard by modifying the configuration properties for the underlying application server.

Procedure

1. Edit your `java.security` file that is in the following directory: *installation_dir*`/jre/lib/security/`. Put the

com.ibm.crypto.fips.provider.IBMJCEFIPS before the **IBMJCE** one in the provider list. Ensure that the list is correctly numbered.

2. Add the **-Dcom.ibm.jsse2.usefipsprovider=true** property to the `jvm.options` file. The property allows the Java™ Secure Socket Extension (JSSE2) provider to run in FIPS 140-2 mode.

   Note: Your certificates must be at least 1024 bytes in size and can be signed with a DSA or RSA signature algorithm. You can use the IBM keytool utility to generate a compatible key pair.

3. To use the TLS protocol, configure secure communcation.

   A number of ciphers are supported by FIPS 140-2. The default SSL configuration automatically enables the FIPS 140-2 compliant ciphers when JSSE is running in FIPS mode. You can enable specific ciphers by listing them in the **enabledCiphers** attribute of the SSL configuration.

SP800-131 compliance

SP800-131 requires longer key lengths and stronger cryptography. The specification also provides a transition configuration to enable users to move to a strict enforcement of SP800-131.

The transition configuration also enables users to run with a mixture of settings from both FIPS140-2 and SP800-131. SP800-131 can be run in two modes, transition and strict. The transition mode is offered to give you a setting to move your environment to SP800-131 strict mode. In transition mode, it is optional to use the SP800-131 required certificates and to set the protocol to SP800-131.

The following requirements must be fulfilled to allow for the strict enforcement of SP800-131:

- The use of the TLS version 1.2 protocol for the Secure Sockets Layer (SSL) context.
- Certificates must have a minimum length of 2048 bytes. An Elliptic Curve (EC) certificate requires a minimum size of 244-bit curves.
- Certificates must be signed with a signature algorithm of SHA256, SHA384, or SHA512. Valid signature algorithms include:
  - SHA256 with RSA
  - SHA384 with RSA
  - SHA512 with RSA
  - SHA256 with ECDSA
  - SHA384 with ECDSA
  - SHA512 with ECDSA
- SP800-131 approved cipher suites.

For more information about the SP800-131 standard, see the web site run by National Institute of Standards and Technology.

Enabling SP800-131 compliance

You can set up a Software Use Analysis profile to meet the SP800-131 requirement that is originated by the National Institute of Standards and Technology (NIST).

Procedure

You can configure Software Use Analysis to run in SP800-131 strict or transition mode.

- To configure the product to run in *strict mode*:
  1. Ensure that your server certificates meet the criteria for SP800-131.

     For more information about SP800-131, see the National Institute of Standards and Technology Special Publication 800-131A.
  2. Modify your SSL configuration to use the TLS version 1.2 protocol.
  3. Enable the Java Secure Socket Extension (JSSE) to run in SP800-131 strict mode: set the system property **com.ibm.jsse2.sp800-131** to *strict*. The property must be set in the `jvm.options` file, which is in the *installation_dir*`/wlp/usr/servers/server1` directory.

     Example:

     ```
     -Dcom.ibm.jsse2.sp800-131=strict
     ```

  Note: If your server certificates do not meet the criteria for SP800-131 or if the TLS version 1.2 protocol is not used, then after you restart the server you are not able to connect to Software Use Analysis. In this event, you can remove the **com.ibm.jsse2.sp800-131** property from the `jvm.options` file, or set the property to *transition*.
- To configure the product to run in *transition mode*, enable JSSE to run in SP800-131 transition mode by setting the system property **com.ibm.jsse2.sp800-131** to *transition*. The property must be set in the `jvm.options` file, which is in the *installation_dir*`/wlp/usr/servers/server1` directory.

  Example:

  ```
  -Dcom.ibm.jsse2.sp800-131=transition
  ```

Managing a certificate

The self-signed certificate that is provided with Software Use Analysis is not intended to be used in the production environment. Replace it with a certificate that is signed by a certificate authority (CA) of your choice.

To have a certificate, you need to generate a private key, a public key, and a certificate signing request (CSR) that is associated with the public key. Next, a certificate authority must sign this request. There are two ways to get a certificate signing request signed. You can either send it to an existing certificate authority (CA), such as Entrust, Verisign, or the CA of your organization, or you can create a private CA.

Using an existing certificate authority

You can use an existing certificate authority (CA) to sign your certificate signing request (CSR). The root certificates of popular CAs are imported into new web browsers by default.

Procedure

1. To generate a new private key and a certificate signing request (CSR), open the command-line console and enter the following commands:

   ```
   openssl genrsa -out key_name.key key_strength -sha256
   ```

   Note: Add the `-des3` option to have a password-protected key, for example:
   `openssl genrsa -des3 -out key_name.key key_strength -sha256`

```
openssl req -new -key key_name.key -out csr_name.csr
```

Where:

csr_name
: Is the name of the CSR file you want to create.

key_name
: Is the name of the new key.

key_strength
: Is the strength of the key that is measured in the number of bits.

sha256
: Is the signature hash algorithm.

For example:

```
openssl genrsa -out privateKey.key 2048 -sha256
openssl req -new -key privateKey.key -out csr.csr
```

The certificate request is created. The certificate signing request (CSR) functions as a temporary placeholder for the signed certificate until you import the certificate into the keystore in the Server Settings panel. The certificate must now be signed by a certificate authority (CA) to complete the process of generating a signed certificate for the server.

2. Send the certificate signing request (CSR) to an external certificate authority (CA) for signing.
3. When the certificate authority (CA) returns the certificate, import it together with the private key.

Creating a private certificate authority

You can create a private certificate authority (CA) and use it for signing the certificate signing request (CSR). A private CA can be created on any computer with an operating system that supports openSSL.

Before you begin

Secure communication depends on the security of the root certificate of the certificate authority (CA). Apply appropriate security measures to protect your private CA.

Procedure

1. Create a private certificate authority (CA) and a certificate:
   a. To create a private CA, run the following commands:

```
mkdir ca
```

```
openssl req -new -newkey rsa:key_strength -nodes
-out path_to_csr.csr -keyout path_to_keyfile.key -sha256
```

Where:

key_strength
: Is the strength of the key that is measured in the number of bits.

path_to_csr
: Is the path to the CSR.

path_to_keyfile
: Is the path to the CA key file.

For example:

```
openssl req -new -newkey rsa:2048 -nodes -out ca/ca.csr -keyout ca/ca.key -sha256
```

b. To create a certificate for your private CA, run the following command:

```
openssl x509 -signkey path_to_keyfile.key -days
number_of_days -req -in path_to_csr.csr
-out path_to_ca_cert.arm -sha256
```

Where:

path_to_keyfile
Is the path to the CA key file.

number_of_days
Is the number of days the certificate is to be valid.

path_to_csr
Is the path to the CSR.

path_to_ca_cert
Is the path to CA certificate file.

For example:

```
openssl x509 -signkey ca/ca.key -days 7300 -req -in ca/ca.csr
-out ca/ca.arm -sha256
```

2. Generate a private key and a certificate signing request (CSR).
3. Sign the certificate signing request (CSR):

```
openssl x509 -req -days 7300 -in path_to_csr -CA ca/ca.arm
-CAkey path_to_keyfile -out cert.arm -set_serial 01 -sha256
```

Where:

path_to_csr
Is the path to the CSR file that you created.

path_to_keyfile
Is the path to the CA key file that you created.

cert.arm
Is the produced server certificate.

ca.arm Is the CA certificate that you must use to sign the CSR.

For example:

```
openssl x509 -req -days 7300 -in csr.csr -CA ca/ca.arm
-CAkey ca/ca.key -out cert.arm -set_serial 01 -sha256
```

The newly created file `ca.arm` contains the root certificate of your private certificate authority (CA). The certificate `cert.arm` and private key `privateKey.key` can now be imported in the Server Settings panel.

Authenticating users with LDAP

Software Use Analysis supports authentication through a Lightweight Directory Access Protocol server. To use this feature, you must configure the Software Use Analysis server.

Configuring Directory Servers

To use LDAP for authentication of Software Use Analysis users, you must create a directory that the application would link to.

Before you begin

- You must have the Manage Directory Servers n permission to perform this task.

Procedure

1. In the top navigation bar, click **Management** > **Directory Servers**.
2. To create an LDAP connection, click **New**.
3. Enter a name for the new directory, select an LDAP server for authentication from the list and enter the name of a **Search Base**.
4. If values of your LDAP server are different from the default, select **Other** from the **LDAP Server** list and enter values of filters and attributes of your LDAP server.

   Important: The default values might need to be modified in particular for openLDAP servers due to various implementations of openLDAP.
5. Enter a name and a password for the authenticated user.
6. If your LDAP server uses Secure Socket Layer protocol, select **SSL** check box. If you require no user credential, select **Anonymous Bind** check box.
7. In the **Host** area, provide the host name on which LDAP server is installed.
8. Enter the **Port**.
9. To verify whether all of the provided entries are valid, click **Test Connection**.
10. Click **Create**.

    You configured a system link to an authentication system.
11. Optional: To add a backup LDAP server, in the **Primary Server** tab click `add backup server` link.
    a. Enter backup LDAP server's host and IP.
    b. Click **Test Connection** to verify whether all of the provided entries are valid.
    c. Click **Save** to confirm the changes.
12. Optional: To edit the directory, click its name. Click **Save** to confirm the changes.
13. Optional: To delete the created directory, click its name. Then, in the upper left of the window click **Delete**.

Linking users to directories

To complete an authentication process through LDAP, you must create a user that would link to the created directory.

Before you begin

You must have the Manage Users permission to perform this task.

Procedure

1. In the top navigation bar, click **Management** > **Users**.
2. To create a user, click **New**.
3. In the **User Name** field, type the name of an existing user of an LDAP server.
4. From the list, select a **Computer Group** to which the user would be assigned.
5. From the **Authentication Method** list, select the name of an LDAP directory.

6. Click **Create**.
7. Optional: To delete the created user, click its name. Then, in the upper left of the window click **Delete**.

   Note: The deleted user cannot be re-created.

What to do next

To confirm authentication, log in to the Software Use Analysis server with the credentials of the LDAP user that you created in Software Use Analysis.

User provisioning

After configuring a Directory Server, you can integrate its users with Software Use Analysis using the LDAP protocol. With user provisioning, you can integrate whole groups of users instead of linking each of them separately.

Before you begin

- Configure a Directory Server.

Procedure

1. Log in to Software Use Analysis.
2. In the top navigation bar, click **Management** > **User Provisioning**.
3. Click **New** to create a new user provisioning rule.
4. In Group Names, start typing the name of a group of users from your Directory Server and then choose one of the autofilled results.
5. In Roles, select the roles that will be assigned to the new users.
6. In Computer Group, select the computer group to which the new users will be assigned.
7. Click **Create**.

Results

You integrated your Directory Server users with Software Use Analysis. For each of the integrated users, Software Use Analysis creates a corresponding match in its user registry and uses your Directory Server as a source for password verification.

Integrating users with Web Reports

You can use the Web Reports component to allow your Lightweight Directory Access Protocol (LDAP) and Web Reports users to access Software Use Analysis.

Before you begin

Install the Web Reports component. The component is typically installed together with your IBM Endpoint Manager server but you can also add it to your environment at any time. To do so, start the installation of IBM Endpoint Manager and choose to install only Web Reports.

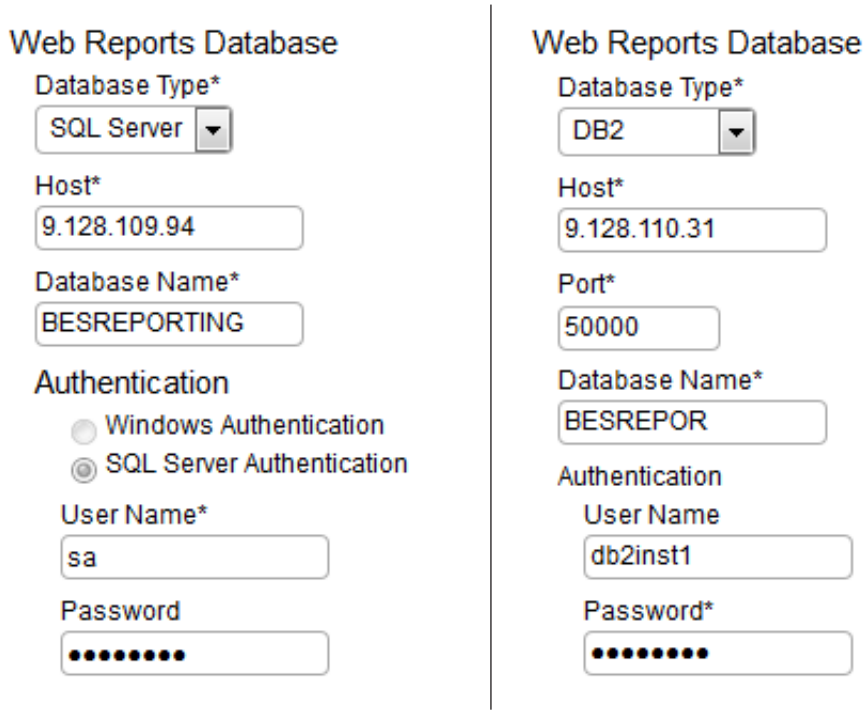
About this task

One of the Web Reports capabilities is integrating with an LDAP directory. This integration allows you to view information about your LDAP users through Web Reports and to grant them right privileges to access your IBM Endpoint Manager environment. If you create an entry for each user in Software Use Analysis, they

will be linked between the application and Web Reports. The linked users can then access Software Use Analysis with the same credentials that are specified in Web Reports. Whenever you change the credentials in Web Reports, they will also be valid in Software Use Analysis with no additional configuration.

Procedure

1. Connect your Software Use Analysis server to the Web Reports database.
   a. Log in to Software Use Analysis.
   b. In the navigation bar, click **Management** > **Data Sources**.
   c. Click on your data source and fill in the connection parameters for the Web Reports database. The required information will differ depending on the type of the database that you use. For more information, see the following examples.



2. Each of your Web Reports users must be manually added to Software Use Analysis. After your complete this action, the users will be linked with their equivalents in Web Reports:
   a. In Software Use Analysis, click **Management** > **Users**.
   b. Click **New** to create a new user.
   c. Enter the user name that corresponds with a Web Reports user name.
   d. Select the appropriate roles. The roles are not integrated between the applications and must be selected manually for each user.
   e. In the Authentication Method, choose **Web Reports**.
   f. Click **Create**.
   g. Repeat this action for each of your Web Reports users.

Results

The created user is linked with its equivalent in Web Reports. You can now use it to log in to Software Use Analysis by using the same password that is specified in

Web Reports. Whenever you change this password in Web Reports, it will also be valid for logging in to Software Use Analysis.

Relays

Relays lighten both upstream and downstream burdens on the server. Rather than communicating directly with a server, clients can instead be instructed to communicate with designated relays, considerably reducing both server load and client and server network traffic.

Relays work by:

- Relieving downstream traffic.
- Reducing upstream traffic.
- Reducing congestion on low-bandwidth connections.
- Reducing the load on the server.

Relays are an absolute requirement for any network with slow links or more than a few thousand clients. For more information about Relays, see IBM Endpoint Manager infocenter.

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 character set (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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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
2Z4A/101
11400 Burnet Road
Austin, TX 79758 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 information 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.

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, and ibm.com 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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks 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.

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Printed in USA