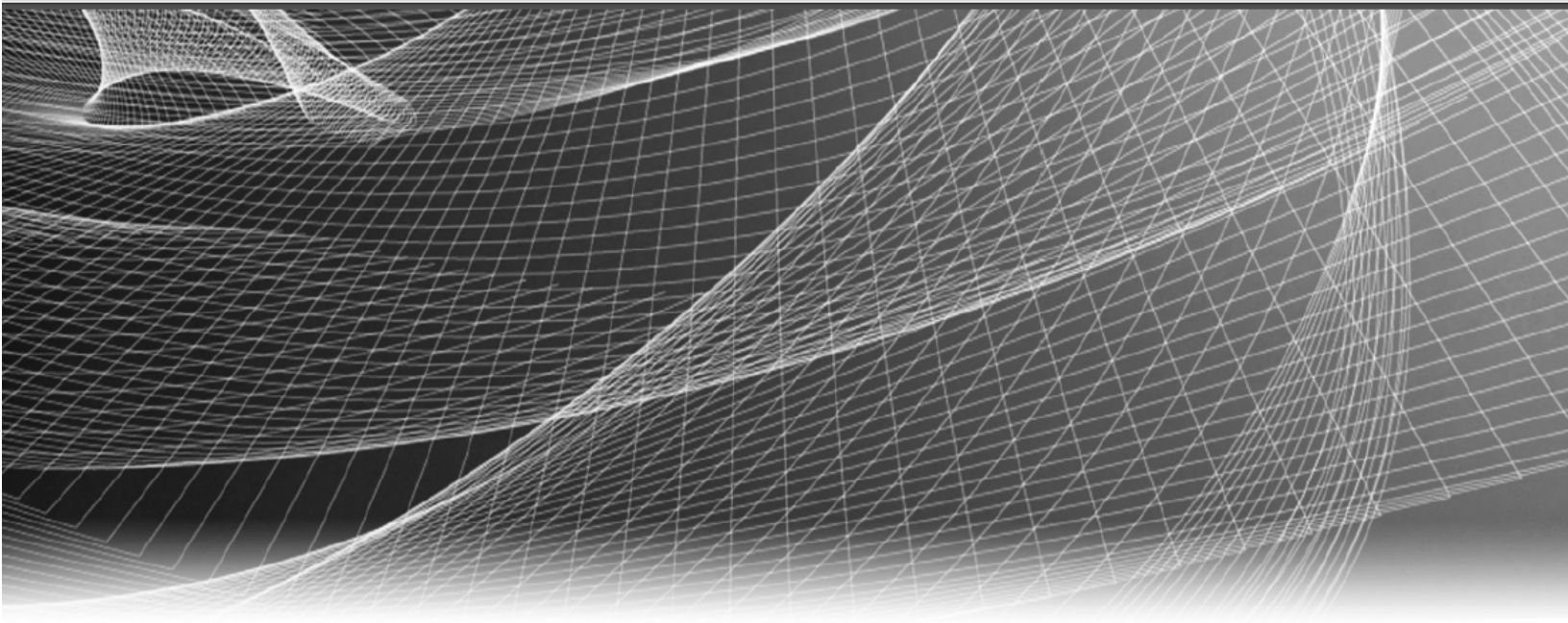


RSA Security Analytics

IPDB Extractor Service Configuration Guide

for Version 10.6.5

RSA EMC²

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

October 2017

Contents

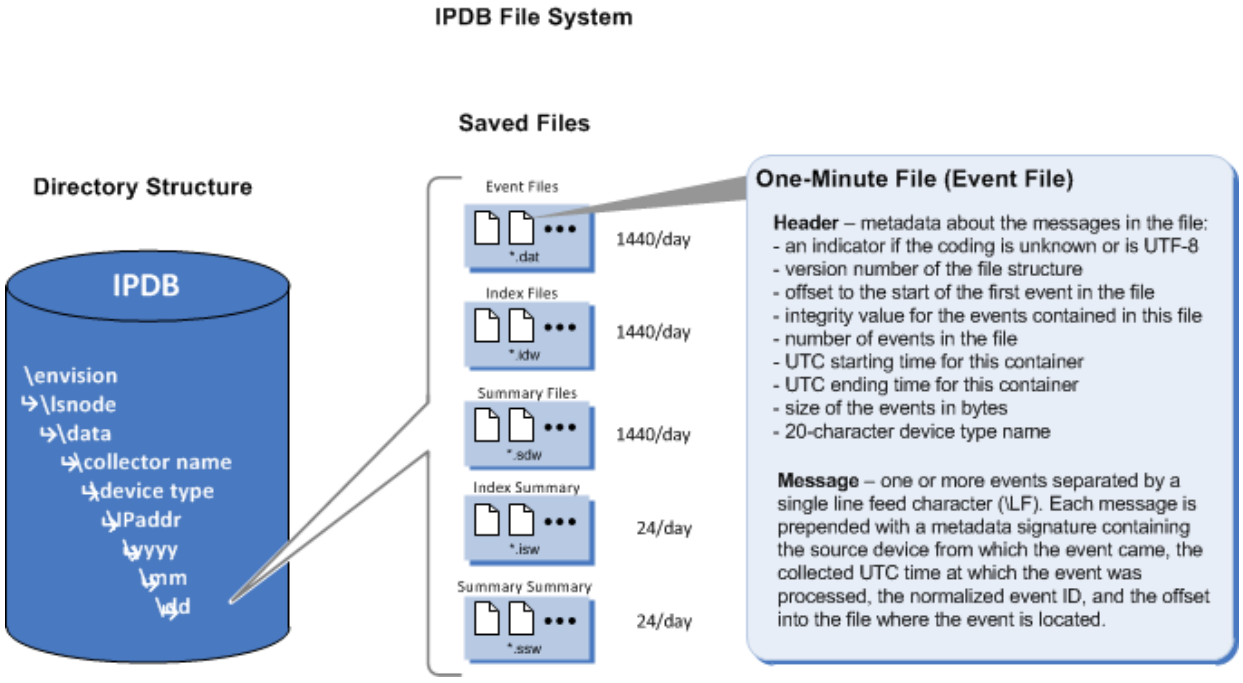
IPDB and the IPDB Extractor Service

This topic introduces the IPDB Extractor service and its role in the Reporting Module. You can choose the Internet Protocol Database (IPDB) as the source of your data when generating reports in the RSA Security Analytics Reporting module. The IPDB Extractor service sends data from the IPDB to the Reporting Engine. The IPDB is the repository for both normalized and raw event messages. It stores all collected messages in a file system organized by event source (service), IP address, and time (year/month/day) with index files to facilitate searches (report and queries).

Note: The IPDB Extractor only supports Content 2.x Event Sources.

You can use the Live Manual Resource Deployment dialog to deploy the latest content to the IPDB Extractor service. Deployment stores the IPDB Extractor service content in /etc/netwitness/ng/envision/etc directory. The content consists of:

- The service xml for all service types that RSA supports.
- The **ipaddr.tab** file - IP address file.
- The **ecat.ini** file.
- The **table-map.xml** file - envision content to NetWitness meta map.



Configure the IPDB Extractor Service

This topic is a set of procedures for configuring IPDB Extractor service. Steps required for configuration are presented in the order that the administrator performs the steps. After this configuration is complete, analysts and operators can report data in IPDB.

Table of Contents

Step 1. Mount the IPDB

This topic describes how to configure the Internet Protocol Database (IPDB) Extractor service to make it available as a data source for the Reporting Engine.

The Internet Protocol Database (IPDB) Extractor service facilitates the use of the RSA enVision IPDB event source database as a data source for the Reporting Engine. Before you can use the IPDB as a Reporting Engine data source, you must mount it to your Security Analytics environment and include the mounting instructions in the `/etc/fstab` file so that the IPDB is mounted automatically in the future.

In this release, Security Analytics:

- Supports two IPDB deployment types:
  - On an ES Appliance.
  - On a separate Network Attached Storage (NAS) device.
- Does not support an IPDB that runs on a Direct Attached Storage (DAS) device.

Note: In a RSA enVision multi-site environment, each site requires a different IPDB extractor instance running on a different appliance (virtual or physical) to integrate with that site's IPDB data source.

Mount an IPDB Running on an ES Appliance

You must complete the following tasks to mount an IPDB running on an ES appliance:

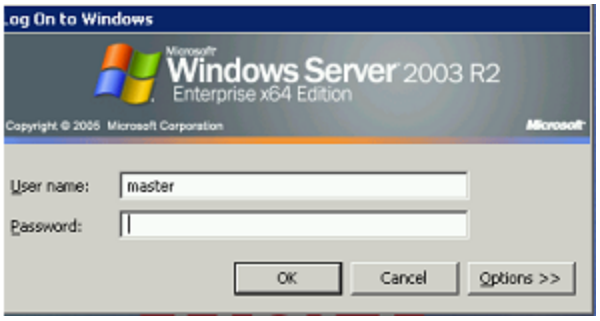
- Task 1 - Log on to the ES Appliance.
- Task 2 - Create a System User in Active Directory and share the IPDB directory and csd directories.
- Task 3 - Note the Reporting Engine Broker and configure the firewall.
- Task 4 - Configure the IPDB and device location file.
- Task 5 - (Optional) If the IPDB has multiple storage locations, map them.

Note: The examples in these tasks use Microsoft Windows 2003. If you have a different version of Windows, the screens and navigation to these screens may differ.

Task 1 - Log on to the ES Appliance

Log on to the ES Appliance to mount an IPDB that resides on that ES Appliance.

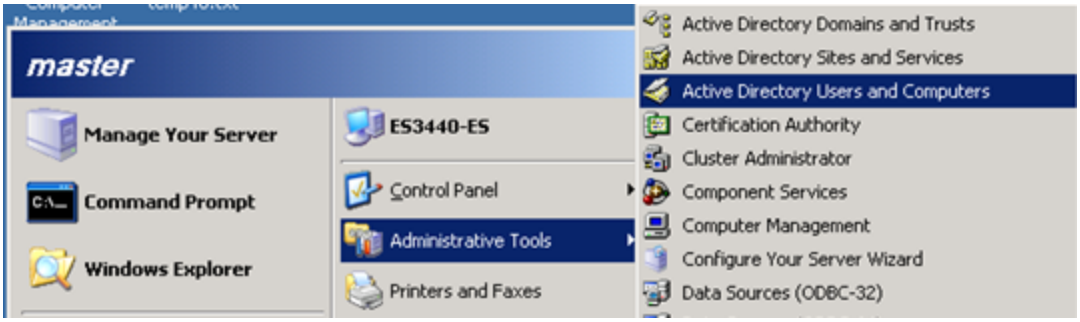
Note: You must use the RSA enVison master account credentials to log on to the ES Appliance.



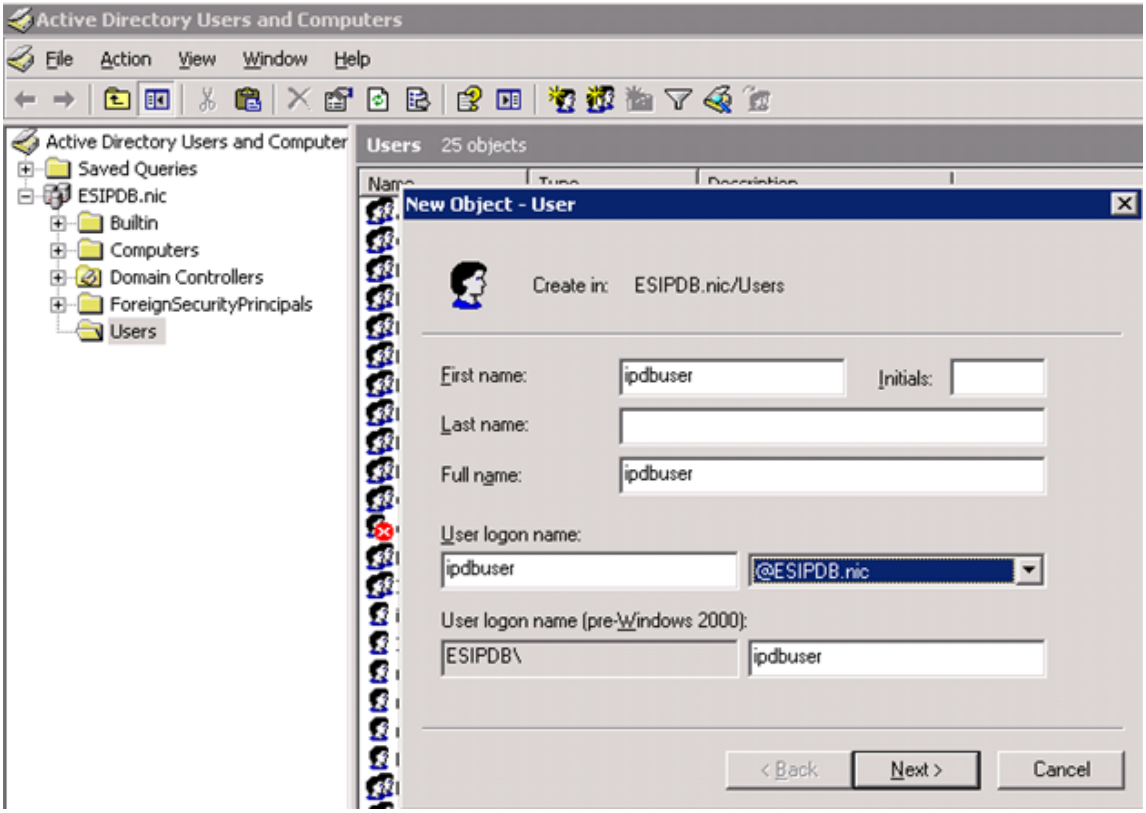
Task 2 - Create a System User in Active Directory and Share the IPDB and CSD Directories

To create a system user in Active Directory with read-only permission to the IPDB directory:

1. Go to the Active Directory folder.



2. Create a new system user in Active Directory.



3. Share the IPDB directory (for example, **e:\nic\lsnode\data**):

   The installation program downloads the **lockdown.zip** file that contains the **doit.bat** script to the Broker appliance. The **doit.bat** script gives you the ability to share the IPDB. Sharing exports the folder so that you can access it from Linux in your Security Analytics environment.

   a. Copy the **lockdown.zip** from the **/etc/netwitness/ng/envision** directory on the Broker to the ES appliance.

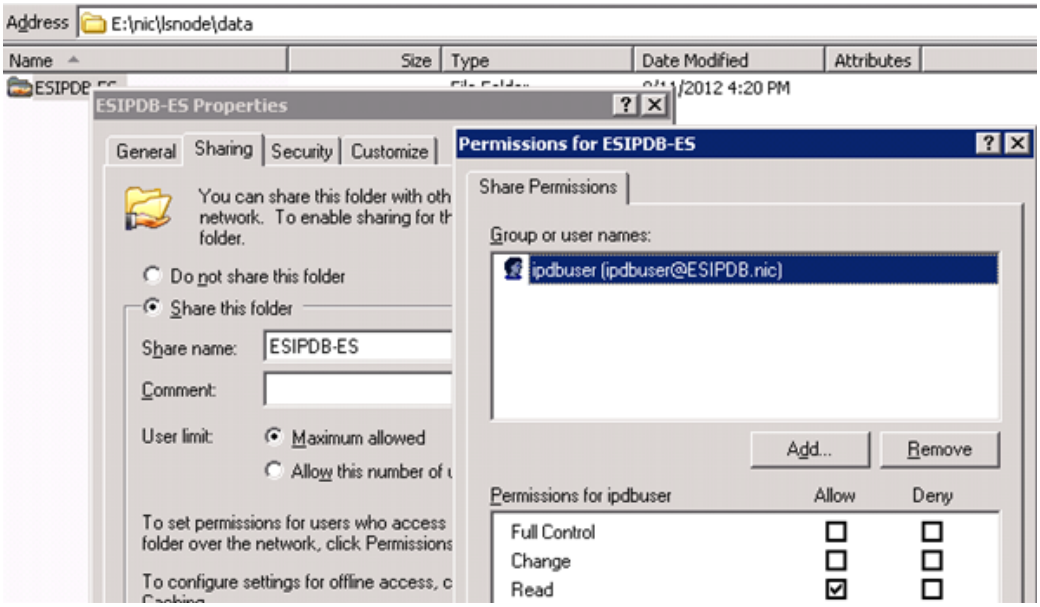
   b. Extract all the files from the **lockdown.zip**.

   c. Run the **doit.bat** script on the ES appliance.

   d. Right-click the IPDB directory (for example, **e:\nic\lsnode\data**).

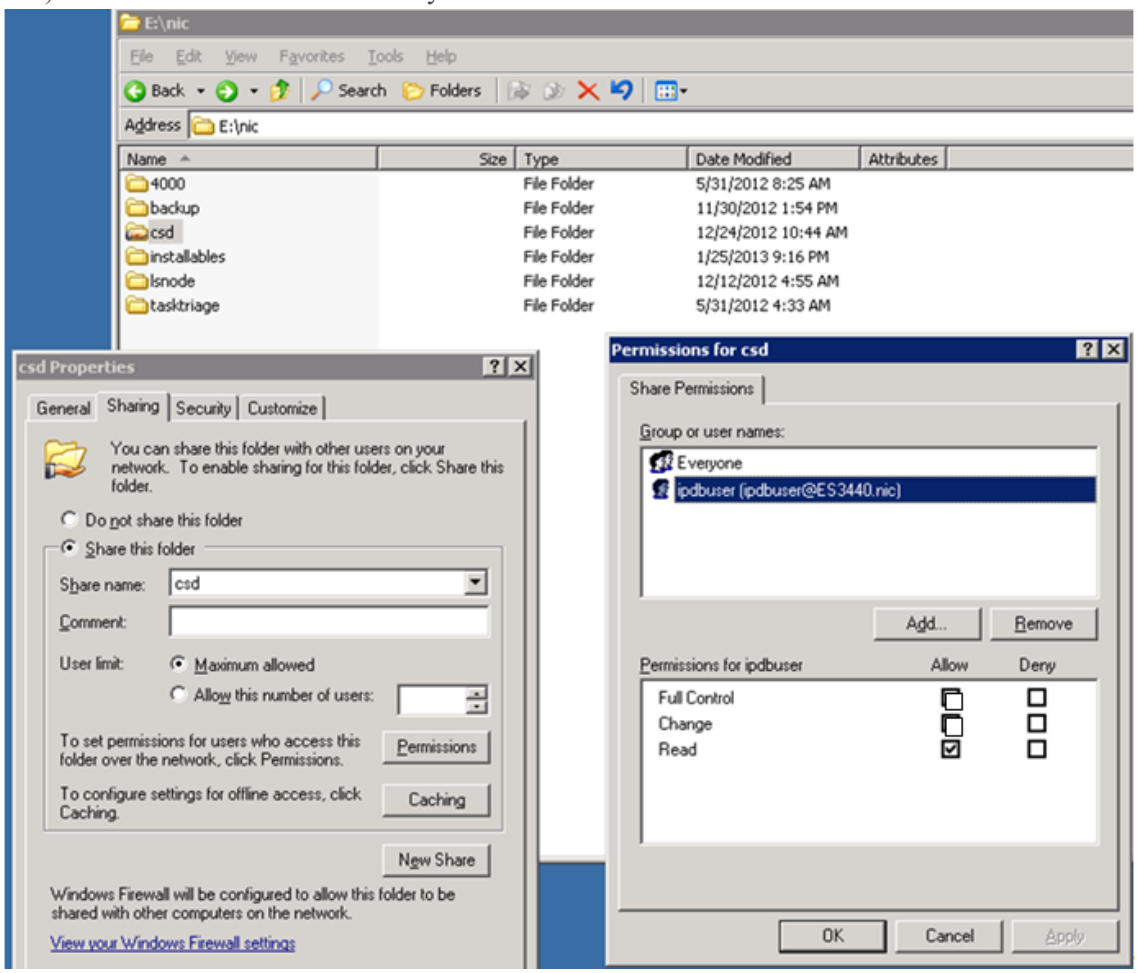
   e. Select **Read** access in the **Share Permissions** tab to give the new user (for

example,ipdbuser@ESIPDB.nic) read access to the IPDB directory.



4. Share the **csd** directory (for example **e:\nic\csd**).
   a. Right-click the **csd** directory (for example, **e:\nic\csd**).
   b. Select **Read** access in the **Share Permissions** tab to give the new user (for example,

csd) read access to the **csd** directory.



Task 3 - Note the Reporting Engine Broker and Configure Firewall

To note the IP address of the Broker for subsequent configuration and to configure the firewall:

1. Write down the IP address of the Broker appliance on which you want to run the Reporting Engine.
2. Configure the firewall so that the Broker running the Reporting Engine has access to the shared directory on the ES Appliance.

Task 4 - Configure the IPDB and Device Location File

To configure the IPDB and device location file:

1. Update the **/etc/fstab** to create the Mount Point for the IPDB:
   a. Run the following command to allow the use of a password file for credentials:
   yum install cifs-utils

   The cifs-utils package installs on the appliance.

   b. Do one of the following to insert the IPDB mount point directory in the **/etc/fstab** file:

   - If you do not use a credentials file:
     //1.1.1.1/ESIPDB-ES /var/netwitness/ipdbextractor/ipdb/ cifs auto,nouser,noexec,ro, username=*username*, password=*credentials-of-ipdb-user* 0 0
   - If you use a credentials file:
     //1.1.1.1/ESIPDB-ES /var/netwitness/ipdbextractor/ipdb/ cifs auto,nouser,noexec,ro,credentials=/root/cred 0 0

   You can create a credential file to provide the username and password for the IPDB-USER. The contents of the file would be:

   username=*username*
   password=*password*

   c. Do one of the following to insert the csd mount point directory in the **/etc/fstab** file:

   - If you do not use a credentials file:
     //1.1.1.1/csd /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro, username=*username*, password=*credentials-of-ipdb-user* 0 0
   - If you use a credentials file:
     //1.1.1.1/csd /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,credentials=/root/cred 0 0

2. Type **mount -a**.

Task 5 - (Optional) For IPDB with Multiple Map Storage Locations, Map Multiple Storage Locations

To map storage locations for an IPDB with multiple storage locations:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select an IPDB Extractor service.

3. In the toolbar, select **View > Explore**.

   Security Analytics displays the IPDB Extractor parameter folder tree.

4. Right-click **/ipdbextractor/config/storage.mapping** in the parameter folder tree.

5. Enter **e:\nic\lsnode~storage1,d:\seclocation~storage2** for the value.

6. Restart the IPDB Extractor service.

7. On the Broker appliance, create **storage1** and **storage2** directories in the **ES** directory. In addition, you need to change the mount points in the **/etc/fstab** to reflect the multiple storage directories. For example:

   //1.1.1.1/storage1 /var/netwitness/ipdbextractor/ipdb/storage1 cifs auto,nouser,noexec,ro,credentials=/root/creds 0 0

   //1.1.1.1/storage2 /var/netwitness/ipdbextractor/ipdb/storage2 cifs auto,nouser,noexec,ro,credentials=/root/creds 0 0

Note: In this example, **storage1** is a shared name given to **e:\nic\lsnode\data** on an ES appliance with an IP address of ***1.1.1.1.*** Similarly **storage2** is shared name given to **d:\alternate-storage\data** on the same appliance. In addition, when you have multiple storage locations, the mapped storage locations on a Broker appliance become their respective node names on the ES or the NAS (that is **storage1** and **storage2** are created in the **/var/netwitness/ipdbextractor/ipdb/** directory on the Broker appliance

Mount an IPDB Running on a Network Attached Storage Device

You must complete the following tasks to mount an IPDB running on a NAS:

- Task 1 - Create an IPDB and csd read-only user.
- Task 2 - Physically connect to the NAS.
- Task 3 - Configure the IPDB and device location file.
- Task 4 - (Optional) If the IPDB has multiple storage locations, map them.

Task 1 - Create an IPDB and CSD Read-Only User

Access the NAS Administrative controller and create a read-only user to the IPDB and the **csd** directories on the NAS.

Task 2 - Physically Connect to the NAS

Physically connect the NAS to the Broker Appliance running the Reporting Engine through a private switch. You must apply an IP address to the ethernet point to which you attach the NAS (for example, 10.203.2.*x* where **x** is greater than 60).

Task 3 - Configure the IPDB and Device Location File

Both the IPDB and the device location file reside on a Network Attached Storage (NAS) device in an LS appliance deployment. The device location file (**.dir**) resides on **vol0** share and the IPDB resides in **vol1/vol2/vol3** depending on how you set up the IPDB for your environment.

To configure the IPDB and Device Location File:

1. Update the **/etc/fstab** to create the mount point for the IPDB:
   a. Run the following command to allow the use of a password file for credentials:
   yum install cifs-utils

   The cifs-utils package installs on the appliance.

   b. Do one of the following to insert the IPDB mount point directory in the **/etc/fstab** file:

   - If you do not use a credentials file:

     //1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1/ cifs auto,nouser,noexec,ro,prefixpath=/nic/lsnode/LSIPDB-LC1/data/LSIPDB-LC1, username=*username*, password=*credentials-of-ipdb-user* 0 0

   - If you use a credentials file:

     //1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1/ cifs auto,nouser,noexec,ro,prefixpath=/nic/lsnode/LSIPDB-LC1/data/LSIPDB-LC1,credentials=/root/cred 0 0

     You can create a credential file to provide the username and password for the IPDB-USER. The contents of the file would be:

     username=*username*
     password=*password*

     To verify that the IPDB mounted properly, make sure that the **/var/netwitness/ipdbextractor/ipdb** directory contains the ***NODENAME*** followed by various device type.

   - If you have multiple LCs:

     //1.1.1.1/LSIPDB-LC1 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1 cifs auto,nouser,noexec,ro, username=*username*, password=*credentials-of-ipdb-user* 0 0

//1.1.1.1/LSIPDB-LC2 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC2 cifs auto,nouser,noexec,ro, username=*username*, password=*credentials-of-ipdb-user* 0 0

c. Do one of the following to insert the csd mount point directory in the **/etc/fstab** file:

- If you do not use a credentials file:

  //1.1.1.1/vol0 /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,prefixpath=/nic/csd, username=*username*, password=*credentials-of-ipdb-user* 0 0

- If you use a credentials file:

  //1.1.1.1/vol0 /var/netwitness/ipdbextractor/devicelocation cifs auto,nouser,noexec,ro,prefixpath=/nic/csd,credentials=/root/cred 0 0

  To verify that the device location file mounted properly, make sure that the **/var/netwitness/ipdbextractor/devicelocation/global/local/directory** contains device location file.

2. Type **mount -a**.

Task 4 - (Optional) For IPDB with Multiple Map Storage Locations, Map Multiple Storage Locations

To map storage locations for an IPDB with multiple storage locations:

1. In the Security Analytics, select **Administration > Services**.
2. In the **Services** grid, select an IPDB Extractor service.
3. In the toolbar, select **View > Config**.

   Security Analytics displays the IPDB Extractor **General** configuration parameters tab.
4. Under **IPDB Extractor Configuration**, in the **Mapping of storage location to mount point** parameter, enter **\\1.1.1.1\vol1\nic\lsnode\LSIPDB-LC1~storage1,\\1.1.1.1\vol2\nic\lsnode\LSIPDB-LC1~storage2** for the configuration value.
5. Restart the IPDB Extractor service.
6. On the Broker appliance, create **storage1** and **storage2** directories in the **LSIPDB-LC1**directory. In addition, you need to change the mount points in the **/etc/fstab** to reflect the multiple storage directories. For example:

   //1.1.1.1/vol1 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1/storage1 cifs auto,nouser,noexec,ro,prefixpath=/nic/lsnode/LSIPDB-LC1/data/LSIPDB-LC1,credentials=/root/cred 0 0

//1.1.1.1/vol2 /var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1/storage2 cifs auto,nouser,noexec,ro,prefixpath=/nic/lsnode/LSIPDB-LC1/data/LSIPDB-LC1,credentials=/root/cred 0 0

Note: In this example, **storage1** is a shared name given to **\\1.1.1.1\vol1\nic\lsnode\LSIPDB-LC1** on a **NAS** with an IP address of **1.1.1.1**. Similarly **storage2** is shared name given to **\\1.1.1.1\vol2\nic\lsnode\LSIPDB-LC1** on the same appliance. In addition, when you have multiple storage locations, the mapped storage locations on a Broker appliance become their respective node names on the NAS (that is **storage1** and **storage2** are created in the **/var/netwitness/ipdbextractor/ipdb/LSIPDB-LC1** directory on the Broker appliance.

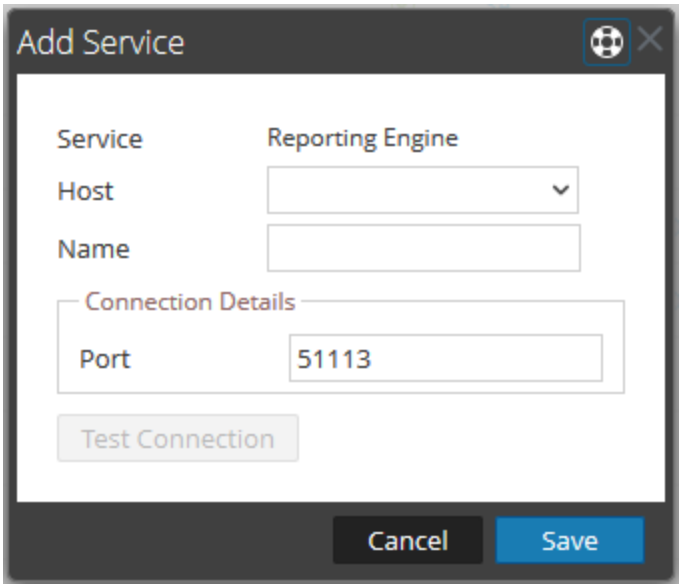
Step 2. Associate a Reporting Engine with an IPDB

This topic describes the procedure for associating the IPDB to a Reporting Engine. To associate an IPDB Extractor service with a Reporting Engine, you must add the Reporting Engine service and its associated IPDB Extractor service to the same Broker host. Add or Update a Host topic in the Host and Services Configuration Guide provides the general steps to add a Broker host.

You must add the Reporting Engine service and its associated IPDB Extractor service to the same Broker host.

1. Add the Reporting Engine service to the Broker host.

   When you add a Reporting Engine service, by default the **Reporting Engine service** defaults to the correct Port (**51113**) as shown below:



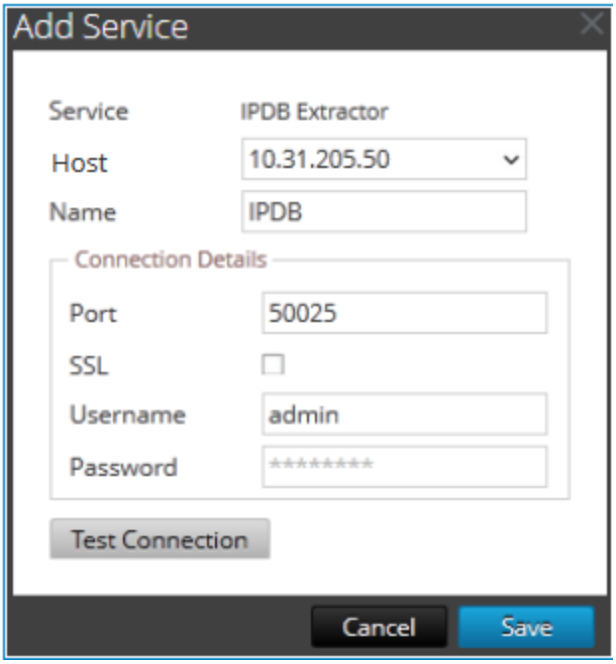
   The Reporting Engine service is added to the Broker host 10.31.205.50:

2. Add the IPDB Extractor service.

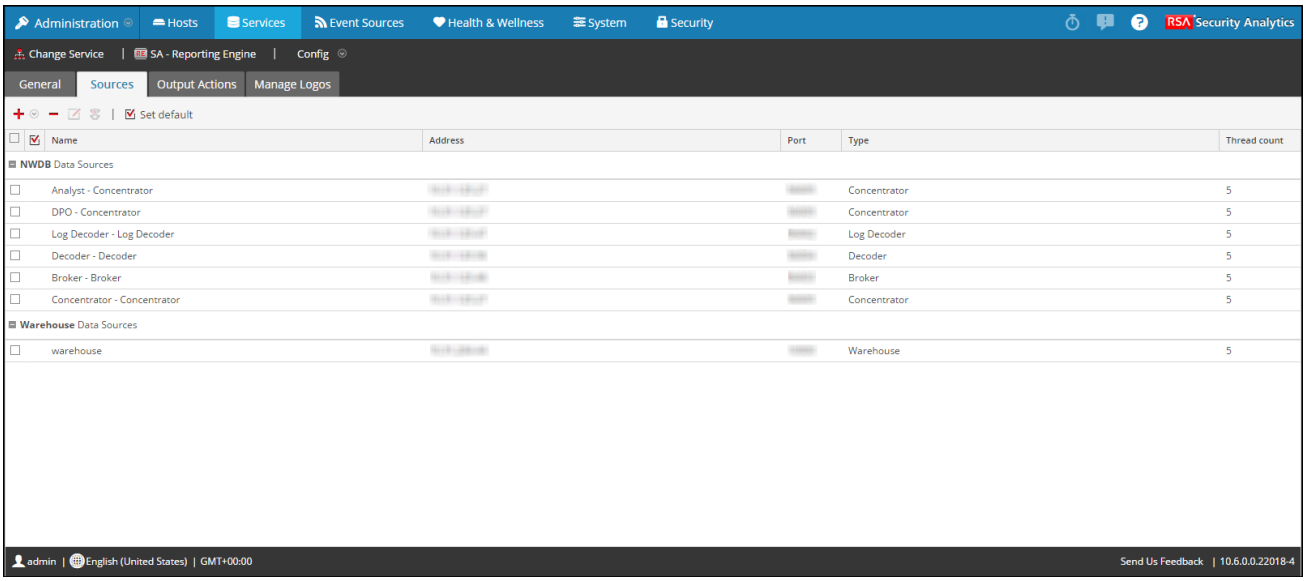
   When you add the IPDB extractor service, by default the service defaults to the Port (50025 for non-SSL and 56025 for SSL). By default SSL is set to off. If you want to use SSL, you must set the **SSL** parameter on the **System Configuration** section of the Services Config View - IPDB Extractor Configuration and restart the IPDB Extractor service.

   Note: You must ensure that the correct native port of the IPDB Extractor service is specified and if required replace the default port with the correct port. After you upgrade, you must verify that the IPDB Extractor service port to depict the correct native port.

3. The IPDB Extractor service is added to the Broker host **10.31.205.50**:



4. In the Security Analytics, select **Administration** > **Services**.
5. For a **Reporting Engine** in the **Actions** column, click  **> View > Config** and click the **Sources** tab.
6. In the Sources tab, add an IPDB Extractor service as a data source.



Note: If you add multiple IPDB Extractor services to the same Reporting Engine then you must ensure that the Use Sqlite Filter option is same for all the services. If the Sqlite Filter initialization fails for any of the IPDB Extractor services, you must turn OFF the Use Sqlite Filter option for all the IPDB Extractor Services associated with the Reporting Engine.

Step 3. (Optional) Map Multiple Storage Locations

This topic describes how to map multiple storage locations for the IPDB Extractor.
The General tab for an IPDB Extractor in the Service Config view provides a way to map the storage location to mount point.

Procedure

To map multiple storage locations for the IPDB:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the Services view page, select the **IPDB Extractor** service.
3. In the **Actions** column, click  **> View > Config**.

   The Service Config view is displayed with the IPDB Extractor Service General tab open.
4. In the **IPDB Extractor Configuration** panel, in the **Mapping of storage location to mount point** field, enter the mapping location for the IPDB.
5. Click **Apply**.

Step 4. Reset nwipdbadptr postgreSQL User Password

This topic describes the steps to reset the password for nwipdbadptr postgreSQL user (Component of the IPDB Extractor service). The IPDB Adaptor is a component of the IPDB Extractor service. **nwipdbadptr** is the postgreSQL database user that the IPDB Adaptor needs to get event meta data for the Reporting module.

There are two tasks that you must complete to configure the IPDB Adaptor:

- Reset the default password for the nwipdbadptr user.
- Add the IPDB Adaptor to the Reporting Engine.

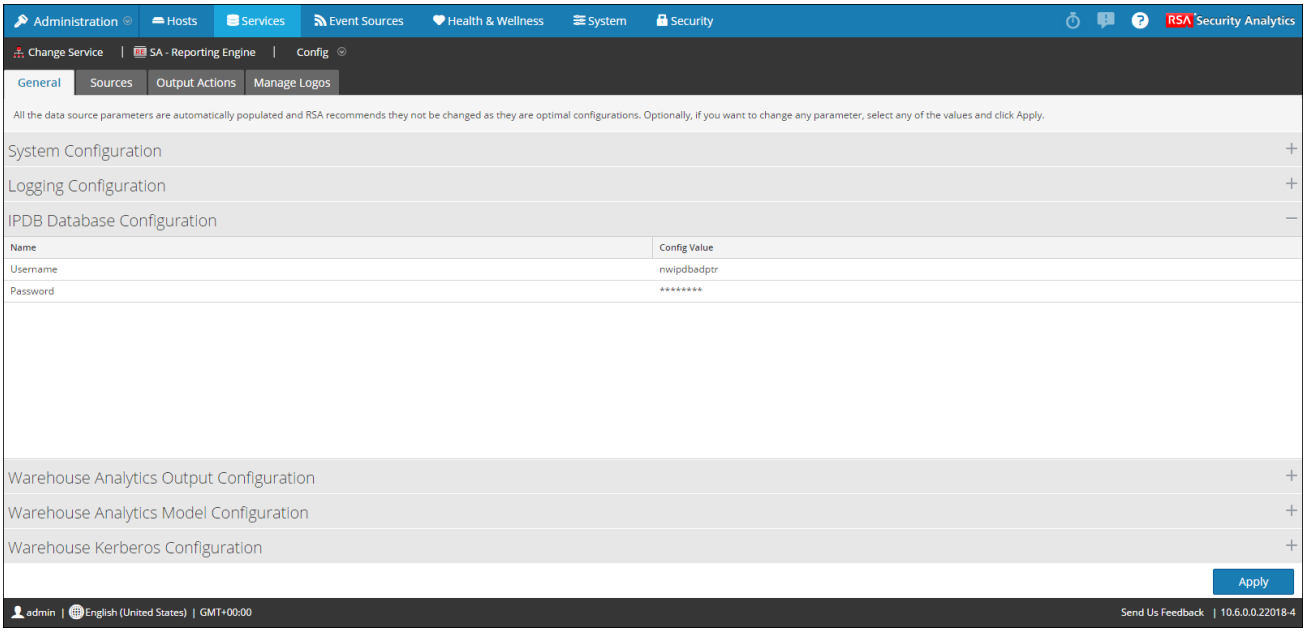
To reset a password for the nwipdbadptr user:

1. Log on to the Reporting Engine Appliance with super user credentials.
2. Execute the following commands.

```
su - postgres
 psql -d nwtmpdb
 ALTER ROLE nwipdbadptr  WITH PASSWORD  'password';
  \q
 Exit
 service postgresql restart
```

3. Replace the password under **IPDB Database Configuration** on the General Tab of the Reporting Engine topic in the *Reporting Engine Configuration Guide* with the password that

you reset in step 2.



Note: You use this password when you add a data source to a Reporting Engine topic in the *Reporting Engine Configuration Guide*

Step 5. Configure IPDB Extractor Data Sources in Reporting Engine

This topic describes how you can configure IPDB Extractor data sources for a Reporting Engine. This topic tells you how to:

- Add a Data Source to a Reporting Engine
- Set a Data Source as the Default Source

Add a Data Source to a Reporting Engine

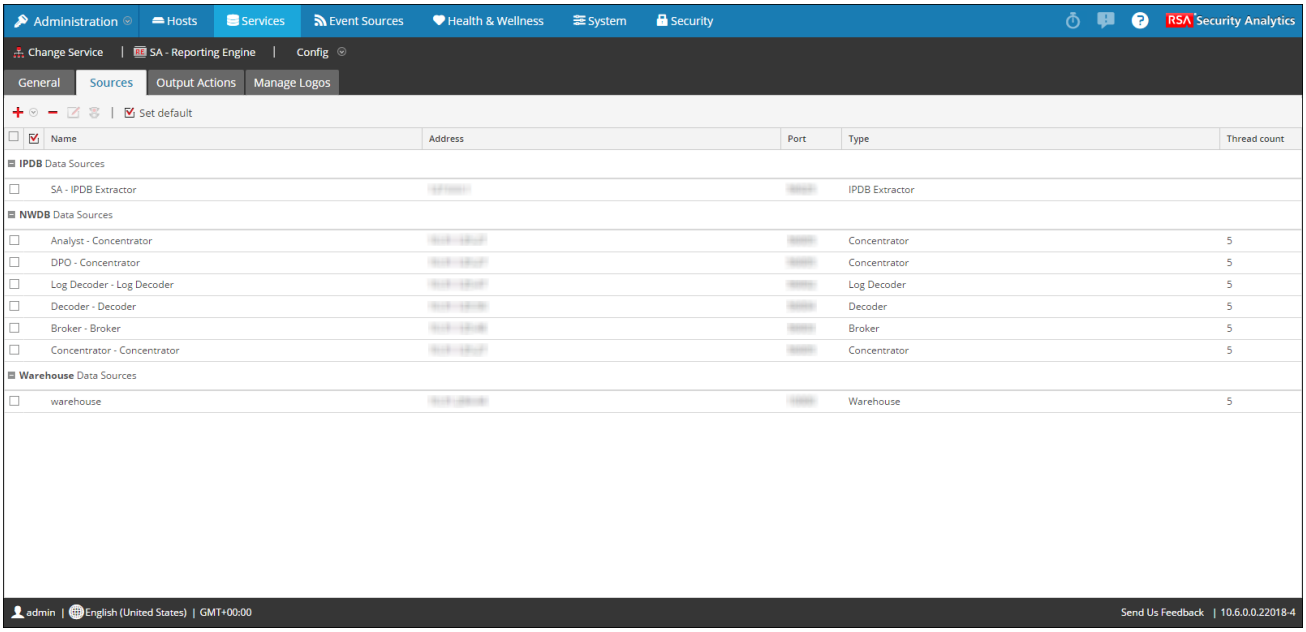
To associate a data source with a Reporting Engine:

1. In the **Security Analytics** menu, select **Dashboard > Administration > Services**.
2. In the **Services** grid, select an **IPDB Extractor** service.
3. Click  **> View > Config**.

   The Service Config view is displayed with the IPDB Extractor Service General tab open.
4. In the **Sources** tab, do the following
   a. Click **Available Services**.
   b. In the **Available Services** dialog box, select the service that you want to add as data source to the Reporting Engine and click **OK**.

      Security Analytics adds this as a data source available to alerts against this Reporting

Engine.



Set a Data Source as the Default Source

To set a data source to be the default source to create alerts:

1. In the **Security Analytics** menu, select **Dashboard > Administration > Services**.
2. In the **Services** grid, select a **Reporting Engine** service.
3. Click  **> View > Config**.

   The Services Config view of Reporting Engine is displayed.
4. Select the **Sources** tab.

   The Services Config view is displayed with the Reporting Engine Sources tab open.
5. Select the source that you want to be the default source (for example, IPDB Extractor).
6. Click the **Set Default** checkbox.

   Security Analytics defaults to this data source when you create alerts against this Reporting Engine.

Step 6. Create IPDB Datasource Event Source List for Reports

This topic describes how you can create an event source list from the IPDB data source and use that list in a report. As part of the configuration of the IPDB Extractor, you need to create event source lists for the IPDB data source. After you create an event source list, you use it in reports so that you can extract data from the IPDB for those event sources exclusively.

Create an IPDB Data Source Event Source Group

To create an IPDB data source event source group:

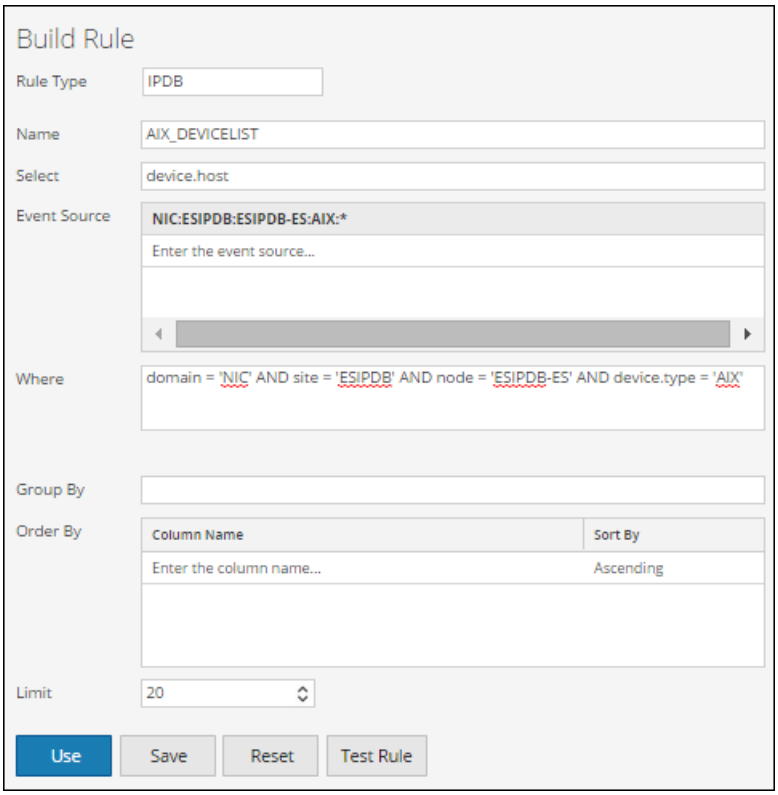
1. In the Security Analytics menu, click **Dashboard > Reports**.

   The **Manage** tab is displayed.

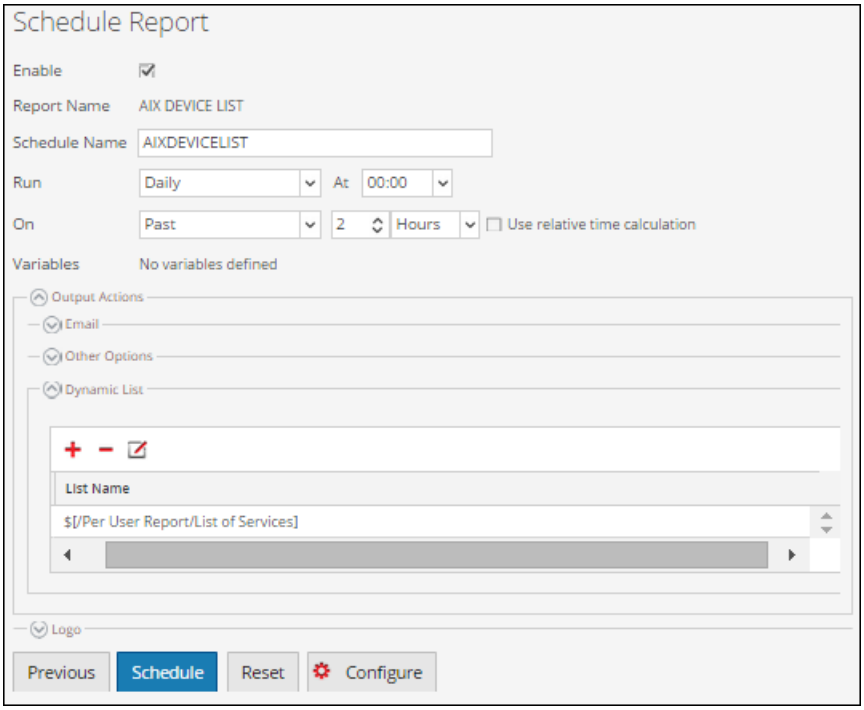
2. Create a rule group (refer to *Reporting Guide*) for event source lists (for example, **Aix_ Devicelst**).

3. **Create a rule** (for example, **AIX DEVICELIST**) to get a list of the event source address from which you want the IPDB data source to pull data. The following example is a rule that creates an event source list address from the NIC domain, ESIPDB site, ESIPDB-ES node and AIX service type.

   Note: You must use the format `domain:site:node:device-type` to specify the Event Source format topic in the *Reporting Guide*. For example, `NIC:ESIPDB:ESIPDB-ES:AIX`. The Event Source specification and WHERE clause must be same.

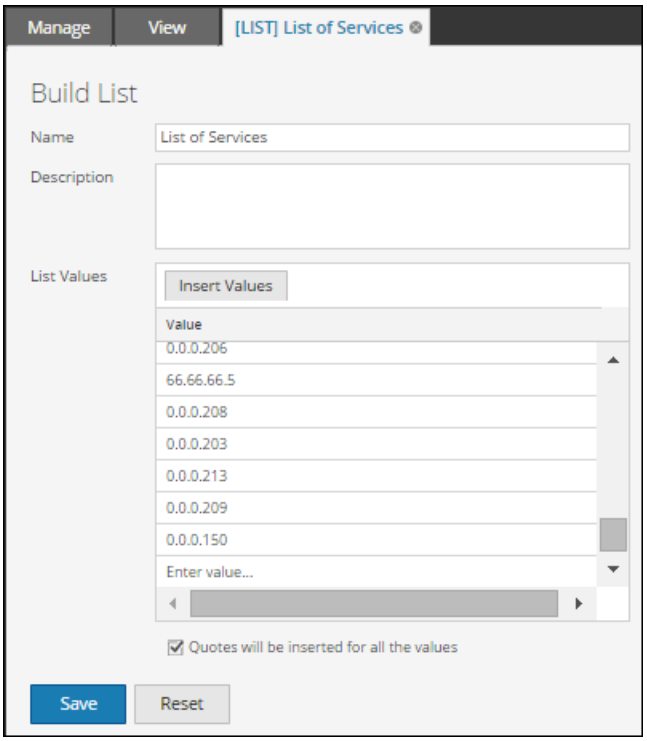


4. **Add a list**. You may not add any values to the list. For example: DEVICE LIST.
5. Create a report and add the rule with the rule **AIX DEVICELIST**.
6. Schedule a report with output to a list as shown below.



When you run the report (rule), Security Analytics populates the output into the list.

7. When the report is run, Security Analytics populates the list. For example:



Use an IPDB Data Source Event Source List in a Report

To use an IPDB event source list in a report:

1. Create a rule topic in the *Reporting Guide*. Specify the list *List of Services* as the Event Source.
2. Create a report topic in the *Reporting Guide* with this rule.
   When you run the report, all the services in the list are used to generate the report.

Step 7. Deploy Live Content to IPDB Extractor

This topic describes how you can download content from NetWitness Live to the IPDB Extractor. Use Security Analytics Live to deploy the latest content to the IPDB Extractor service. The download stores the IPDB Extractor service content in **/etc/netwitness/ng/envision/etc** directory. The content consists of:

- The service xml for all service types that RSA supports.
- The **ipaddr.tab** file.
- The **ecat.ini** file.
- The **table-map.xml** file - envision content to NetWitness meta map.

To download content to the IPDB Extractor service:

1. In the Security Analytics menu, click **Dashboard > Live > Search**.

   Security Analytics displays the Live Search View.
2. From the Resource Types drop-down list, select **RSA Log Device** and click **Search**.

   Security Analytics displays a **NWFL** (NetWitness for Logs) **Content** link in the **Matching Resources**. You can enter the keyword to search for this content.
3. Double-click Envision Content File (**NWFL Content**) link or select the file.
4. Click **Deploy**.
5. Select the resource (Envision Content File) and click **Next**.
6. Select the IPDB Extractor service in which you want to deploy the content and click **Next**.
7. Review the information and click **Deploy**.
8. Go to **/etc/netwitness/ng/envision/etc** directory on the Broker appliance running the IPDB Extractor service to make sure that Live downloaded the content successfully.
9. Restart the IPDB Extractor service to deploy the content.

Step 8. (Optional) Configure Multi-Site Deployment

This topic describes how you can update the Transport Vives URI parameter for the IPDB deployed in a multi-site environment. For a multi-site environment, you must update the Transport Vives URI parameter for the IPDB deployed.

For Multi-Site IPDB deployment only, to update the Transport Vives URI parameter:

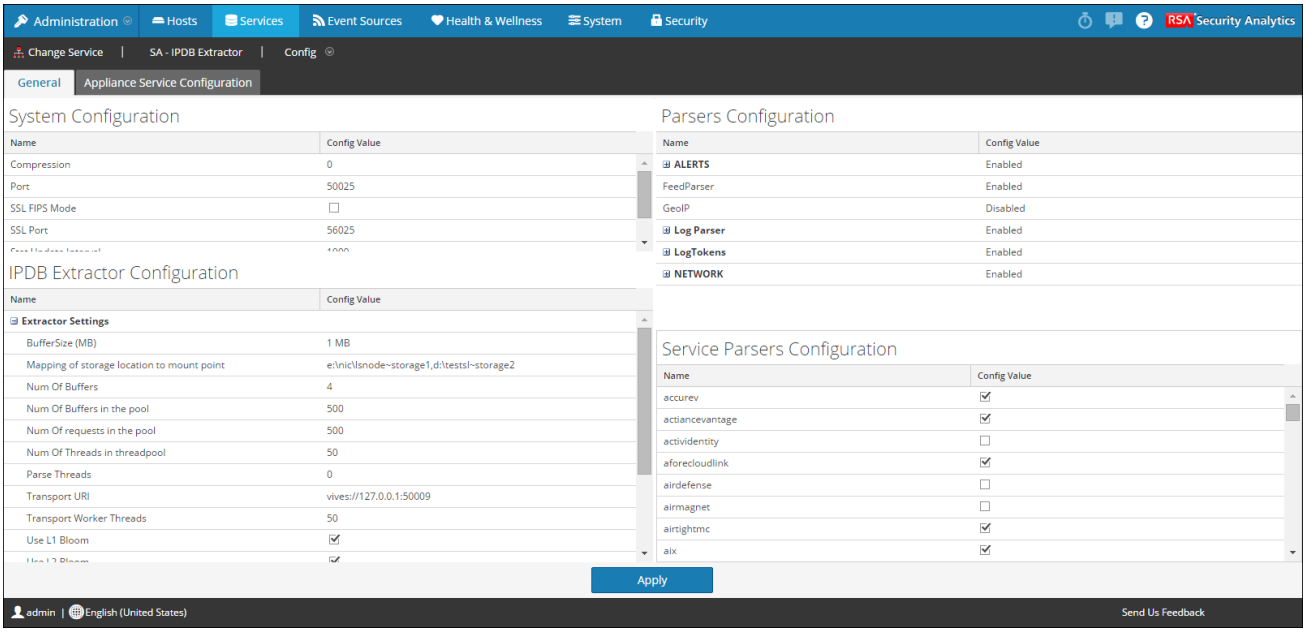
1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services grid**, select the **IPDB Extractor** service running on the remote site.
3. In the **Actions** column, click  **> View > Config**.
4. In the **IPDB Extractor General** tab under **Extractor Settings**, click the **Config Value** column of the **Transport URI** parameter.
5. Replace the **vives://127.0.0.1:50009** default value with the IP address of the IPDBExtractor service residing in the remote site (that is **vives://<remote-site-ip-address>:50009**) and click **Apply**, where <remote-site-ip-address> is the IP address.
6. Restart the IPDB Extractor service.

Services Config View - IPDB Extractor Configuration

This topic describes the General tab configuration parameters for IPDB Extractor service. The **General** tab for an IPDB Extractor in the Service Config view provides a way to manage service configuration, configure data retrieval, and select the parsers that are applied to the retrieved data.

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the Services View, select the **IPDB Extractor** service.
3. In the **Actions** column, click  **> View > Config**.

   The Service Config view is displayed with the IPDB Extractor Service General tab open.



System Configuration

The System Configuration section manages service configuration for a service. When a service is first added, default values are in effect. You can edit these values to tune performance.

The System Configuration section has these parameters.

Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.
Port	The port on which the service listens. The default ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services The default port for IPDB Extractor Service is 50025.
SSL	When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of 0 lets the system decide. The default value is **15.** A change takes effect on service restart.

IPDB Extractor Configuration

The **IPDB Extractor Configuration** panel parameters are used to manage service configuration for the IPDB Extractor. When you add an IPDB Extractor service, the default values are in effect. RSA designed the default values to accommodate most environments and recommends that you do not edit these values because it may adversely affect performance.

Parameters that set up and tune data retrieval include:

- Extractor Settings
- Query Settings

Extractor Settings

The following table describes the Extractor Settings.

Name	Config Value
Buffer Size (MB)	The size (in megabytes) of the data retrieval buffer. Default value is **1**. You must restart the IPDB Extractor service after modifications for this value to take effect.
Mapping of storage location to mount point	For an IPDB with multiple storage locations only. If you have multiple storage locations on an IPDB, you must map them to the corresponding mount points so that the IPDB Extractor can extract data from them. For example: \\1.1.1.1\-vol1\nic\lsnode\LSIPDB-LC1~storage1,\\1.1.1.1\vol2\nic\lsnode\LSIPDB-LC1~storage2 You must restart the IPDB Extractor service after modifications for this value to take effect.
Num Of Buffers	The number of data retrieval buffers. Valid values are 1 - 4. Default value is **4** buffers. You must restart the IPDB Extractor service after modifications for this value to take effect.
Num Of Buffers in the pool	The number of buffers in the pool of available buffers. Valid values are 500 - 700. Default value is **500** buffers. You must restart the IPDB Extractor service after modifications for this value to take effect.
Num Of requests in the pool	The number of requests in the pool. Valid values are 500 - 6000. Default value is **500** requests. You must restart the IPDB Extractor service after modifications for this value to take effect.
Num Of Threads in the thread-pool	The number of threads in the thread pool. Valid values are 50 - 200. Default value is **50** threads. You must restart the IPDB Extractor service after modifications for this value to take effect.

Name	Config Value
Parse Threads	The number of parse threads used for session parsing. Valid value is a number. Default is **0** parse threads. of parse threads. If you specify **0**, the server determines the number of threads based on the data volume. You must restart the IPDB Extractor service after modifications for this value to take effect.
Transport URI	Transport Uniform Resource Identifier (URI) is used to communicate between IPDB client and IPDB Extractor server. The default value is **vives://127.0.0.1:50009**. You must restart the IPDB Extractor service after modifications for this value to take effect.
Transport Worker Threads	The number of worker threads to process the transport client requests. You must restart the IPDB Extractor service after modifications for this value to take effect.
Use L1 Bloom	Use L1 Bloom for faster retrieval of data from IPDB. If the Bloom Filter index is enabled for a meta and the event logs contain the meta value that is being requested in the report query, then the corresponding data files are read, else they will be skipped. Default value is checked (use L1 Bloom). **Note:** You must have August 2013 or later content packet installed to specify the Use L1 Bloom and Use L2 Bloom options.
Use L2 Bloom	Use L2 Bloom for faster retrieval of data from the IPDB. If the Bloom Filter index is enabled for a meta and the event logs contain the meta value that is being requested in the report query, then the corresponding data files are read, else they will be skipped. Default value is checked (use L2 Bloom)
Use L2 Indexing	Use L2 indexing when retrieving data from the IPDB. Default value is checked (use L2 indexing).
Use Sqlite Filter	Apply sqlite filter to events. Default value is checked (apply sqlite filter).

Query Settings

The following table describes the IPDB Extractor Query Settings.

Name	Config Value
Query Idle Limit	The time in seconds Security Analytics waits between subsequent data retrieval before it closes a query. Default value is **3600**.
Query Status Interval	The time in seconds Security Analytics waits between updates to query statistics. Valid value is in the **1** - **200** range. Default value is **10**. Security Analytics sets this value to the **Stat Update Interval** value in the Profile View > Preferences panel > General Tab if the **Query Status Interval** is less than the **Stat Update Interval**.

Parsers Configuration

The Parsers Configuration panel provides a way to select parsers to use on the IPDB Extractor. The table describes the features of the Parsers Configuration section.

Feature	Description
Name	The names of parsers available to the IPDB Extractor. A plus sign indicates that the metadata generated by the parser is configurable. Clicking the plus sign displays the metadata that the parser can create.
Config Value	A checkbox toggles the setting for the parser or metadata on or off. When the box is checked, the IPDB Extractor is using the parser to filter traffic; when unchecked, the IPDB Extractor is not using the parser. If the generated metadata for the parser is configurable, a checkbox selects the metadata the parser will create.

Service Parsers Configuration

The Service Parsers Configuration panel is used to select the service parsers to use on the IPDB Extractor service.

Troubleshoot IPDB Extractor

This topic provides information about possible issues you may encounter while using the IPDB Extractor.

Possible Issues

Problem	Possible Causes	Solutions
In a Linux environment, when IPDB Extractor is installed on a Virtual Machine, it fails to load and you are not able to view the meta to define an IPDB rule. <dyou at="" can="" in="" log="" look="" the-="">/var-r/log/messages file where the following message is displayed: `Unable to allocate any memory in MemPages constructor.` </dyou>	The IPDB Extractor service may not be able to allocate sufficient memory to the parser.	To change the pool settings: 1. In the Security Analytics menu, select **Administration**> **Services**> IPDB Extractor > **View**> **Explore**. 2. Change the value of `/ipdbextractor/config/pool. packet. pages` to a value lower than the existing configuration. 3. Change the value of `/ipdbextractor/config/pool.session. pages` to a value lower than the existing configuration. 4. Restart the IPDBExtractor Service.

Recommended Values

Virtual Machine Memory Size	Packet pages	Session pages
>=24GB	50000	25000
>=17GB	30000	10000
>=9GB	20000	7000
>=4GB	10000	5000

Note: The above values are suggestions only. If the problem exists even after changing the configuration values, consider decreasing the values further.