**broadsoft**

**broadsoft**
**broadworks**®

BroadWorks Dashboards and Discovery

Installation and Configuration Guide

Release 1.0

Document Version 1

9737 Washingtonian Boulevard, Suite 350
Gaithersburg, MD 20878
Tel +1 301.977.9440

**WWW.BROADSOFT.COM**

# BroadSoft® Guide

## Copyright Notice

## Trademarks

## Document Revision History

**Example**

| Version | Reason for Change | Date | Author |
|---------|-------------------|------|--------|
| 1 | Created document. | *September 2016* | *DES* |
| | | | |

# Table of Contents

## Table of Figures

# 1  Overview

The BroadWorks Dashboards and Discovery toolset is a set of tools that collect BroadWorks logs and CDR data and allow analysis and visualization of data. They utilize ElasticSearch as the backend storage technology and Kibana as the Discovery/Visualization and Dashboarding frontend. Also included is custom Kibana plugins for providing BroadWorks specific visualization of SIP and XsiEvent flows.

The toolset includes (more detail in following sections):

- BroadWorks Log Collectors
- Broadworks XML/CSV CDR Collector
- BroadWorks Radius CDR Collector
- BroadWorks Subscriber Dump Processor
- Broadworks Message Archive Processor
- Sample Kibana Visualizations/Dashboards
- Script based samples of offboard data collection

## 2 Support

### 2.1 ElasticSearch and Kibana

ElasticSearch and Kibana are requirements of the BroadWorks Dashboards and Discovery but are not delivered or supported by BroadSoft. If maintenance and support is required, it is recommended to get that from the ElasticSearch organization. Additionally, BroadSoft will provide guidance on configuration and installation but is beyond the scope of the what is being delivered.

### 2.2 BroadWorks Dashboards and Discovery

The BroadWorks Dashboards and Discovery toolset is being delivered as an open source project available from GitHub. Support will be provided through issue reporting on GitHub where BroadSoft will respond to questions/issues and product requests on a best effort basis. Issues can be opened from the same location on GitHub as this document was received and the toolset downloaded from. For reference the download location is:

https://github.com/BroadSoft-Xtended/BroadWorks-Dashboards-and-Discovery

To open an issue – navigate to the above page and go to the Issues tab then click "New Issue"

BroadSoft has a team that is supporting the toolset and will review the Issues reported and provide comments on resolution.

### 2.3 License

The BroadWorks Dashboards and Discovery toolset is being delivered under the Apache License, Version 2.0 – License is below:

Licensed under the Apache License, Version 2.0 (the "License");

you may not use this file except in compliance with the License.

You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software

distributed under the License is distributed on an "AS IS" BASIS,

WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and

limitations under the License.

# 3    ElasticSearch & Kibana

ElasticSearch is the backend storage for the data collected and is used for the searching and filtering of the data for analysis by the frontend applications. The requirements for this release of the toolset are:

- ElasticSearch version 2.3.3

- Kibana version 4.5.2

ElasticSearch and Kibana can be downloaded at https://www.elastic.co

It is strong recommended to review the documentation on the site for performance and configuration details and recommendations.

## 3.1    ElasticSearch Installation

### 3.1.1    Requirements

The pre-requisite requirement for installation is a dedicated server – with the desired memory and disk space (see section on Hard Guidance)

The simplest installation guidance of ElasticSearch on a server is provided below

- Download ElasticSearch version 3.1.1 (elasticsearch-2.3.3.zip)

- Create a new user on the server named elastic

   o   useradd -m elastic

   o   password elastic

   o   <input desired password>

- Login as elastic

- unzip elasticsearch-2.3.3.zip

ElasticSearch is effectively installed. It is self-contained in its own directory.

### 3.1.2    Configuration Guidance

This section provides guidance on configuration of ElasticSearch. Please visit https://www.elastic.co for full configuration documentation that may be pertinent to your deployment.

- File elasticsearch.3.2.2/config/elasticsearch.yml

   This file holds the static configuration for ElasticSearch.

   The initial content of the file will be with no elements enabled (all at application default)

   o   cluster.name – This parameter defines the name of the ElasticSearch cluster. If you have multiple nodes with the same cluster name – they will auto-discover and join in the cluster automatically. Should be unique within your network if you have more than one cluster. Example:

   cluster.name: broadworksdd

   o   network.host – This defines the network interfaces that the ElasticSearch cluster will listen to for connections. If you intend to have a single ES node with all applications on the node then this does not need to be

configured. But if you intend to connect from other nodes in your network – you need to define the interface for it to listen on.

- o  bootstrap.mlockall – Set to true for performance. It prevents ES memory from being swapped out.

- o  index.refresh_interval – This is the time interval between document indexing and the document being available for searching/available for analysis. The default is 1 second (1s) – the higher the index rate the more CPU cycles will be utilized merging the documents. This deployment is extremely heavy in indexing (100s of thousands a minute) – by extending the refresh interval – overall performance of the server will increase. Example:

  index.refresh_interval: 30s

- o  path.data – This is the list of disks that the ES will store the documents and the indexes. Example:

  path.data: /data/disk1, /data/disk2, /data/disk3, /data/disk4

- o  path.logs – Directory ES will store it's application logs. Example:

  path.logs: /home/elastic/elasticlogs

See more specific configurations, see:

https://www.elastic.co/guide/en/elasticsearch/reference/2.3/setup-configuration.html

- ■  Example startup script

  Below is a sample startup script. The operator will need to create/configure the server startup to reference this in the rc.d scripts (based upon your deployment OS):

  #!/bin/sh

  export ES_HEAP_SIZE=16G

  export JAVA_HOME=<path to java installation>


  /home/elastic/elasticsearch-2.3.3/bin/elasticsearch -d

  Note: The recommended ES configuration on a server is to give the ES heap no more than 50% of the RAM in the server. This allows the OS to manage the file cache which improves performance for the underlying indexing algorithms underlying ElasticSearch (see https://lucene.apache.org/ for more information on that technology)

## 3.2   Kibana

### 3.2.1   Requirements

Section assumes section 2.1 has been executed.

- ■  Download Kibana version 4.5.2 (kibana-4.5.2-linux-x64.tar.gz)
- ■  Login as elastic
- ■  tar -zxvf kibana-4.5.2-linux-x64.tar.gz

Kibana is effectively installed. It is self-contained in its own directory.

### 3.2.2 Configuration Guidance

This section provides guidance on configuration of Kibana. Please visit https://www.elastic.co for full configuration documentation that may be pertinent to your deployment.

- File kibana-4.5.2-linux-x64/config/kiban.yml

  This file holds the static configuration for ElasticSearch.

- File kibana-4.5.2-linux-x64/config/kibana.yml

  File contents will initially be commented out. Below is guidance on items of interest

  - elasticsearch.url – Defines the access to ES. If Kibana is running on a different server than the Kibana instance. Example:

    elasticsearch.url: "https://10.10.10.10:9200"

  - elasticsearch.requestTimeout – Defines the time before Kibana will timeout a request. It can sometimes take a bit for Kibana to heat up the cache on the first queries if the info being requested has been flushed to disk. Example:

    elasticsearch.requestTimeout: 120000

- Example startup

  - Kibana-4.5.2-linux.x64 serve -Q &

  - It is recommended to use the same startup strategy for kibana as ElasticSearch.

- More information on Kibana configuration/setup at:

  https://www.elastic.co/guide/en/kibana/4.0/setup.html

# 4    BroadWorks Log Collector

The BroadWorks Log Collector is a set of two applications. First the bwlogsender – is an application that runs on BroadWorks nodes that via a configuration file collects logs as they are generated, formats them for transport and sends them across a compressed stream to the bwlogreceiver. The receiver then parses the logs for specific information and indexes the log into ElasticSearch.

This section provides guidance on the installation and configuration of the applications

## 4.1    bwlogsender

This application runs on the BroadWorks nodes. The package is provided as a self-extracting archive and is required to be installed as root. It is installed in /usr/local/bwlogsender/. Inside the bwlogsender directory – there will be a symlink called bwlogsender which is symlinked to bwlogsender_<version> to facilitate upgrades. When ran, the java application runs as bwadmin. Additionally a startup script is installed in the rc.d system so the application will start automatically after a server restart.

The package file name is structured as bwlogsender_<version>.run.

### 4.1.1    Installation & Configuration

The following are the commands and configuration to install bwlogsender

- Login to the BroadWorks server as root

- cd to the directory of the bwlogsender_<version>.run file

- chmod 755 bwlogsender_<version>.run

- ./bwlogsender_<version>.run

- The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| Do you want to enable this application: | Whether you want the initial state of the application to be able to run | 2 – Yes |
| What is the Server Type: [AS] | What the BroadWorks Server Type is. Application should auto detect the server type | BroadWorks Server Type |
| What is the Receiver Server host: | The hostname or IP address where bwlogreceiver is/will be running. | No default |
| What is the Receiver Server port to use: | The port the bwlogreceiver is listening to | 9072 |
| What is the desired size of the Sender Log Queue Size: | The Log Queue size between the log readers and the transmitter queues. This size should be optimal for normal networks | 1000 |
| What is the desired number of Sender Write Threads: | The number of sender/transmitter threads. The default of 1 should be sufficient for normal networks | 1 |
| What is the desired Zip Block Size: | The Zip Block Size is the size of the block (of logs) will be used for compression. 128000 has proven to be an optimal size. | 128000 |

| | | |
|---|---|---|
| What is the desired JVM Heap Size: | JVM Heapsize for the application. 512M is the default and sufficient for the rest of the settings | 512M |

- To start the application – shouldn't be done until the receiver is installed and running – do one of the following

    o As root – "service bwlogsender start"

    o As bwadmin – "/usr/local/bwlogsender/bwlogsender/bwlogsender.pl –start

    o To verify application status – "/usr/local/bwlogsender/bwlogsender/bwlogsender.pl  –showrun

- To stop the application

    o As root – "service bwlogsender stop"

    o As bwadmin – "/usr/local/bwlogsender/bwlogsender/bwlogsender.pl --stop

## 4.2    bwlogreceiver

This application runs on another server. The package is provided as a self-extracting archive and is required to be installed as a normal user (in the example "elastic"). It is installed in the current working directory into a new directory bwlogreceiver. Inside the bwlogreceiver directory – there will be a symlink called bwlogreceiver which is symlinked to bwlogreceiver_<version> to facilitate upgrades.

The package file name is structured as bwlogreceiver_<version>.run.

### 4.2.1    Installation & Configuration

The following are the commands and configuration to install bwlogreceiver.

The following detail of the commands assumes running in the same server as ES was installed into (I.E. has user elastic)

- Login to the server as elastic

- cd to /home/elastic

- chmod 755 bwlogreceiver_<version>.run

- ./bwlogreceiver_<version>.run

- The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| What is the Elastic Server host: | IP or hostname of the ES server. Assuming local – you can enter 127.0.0.1 | No default |
| What is the Elastic Server port to use: | Normally 9300 – if there have been customizations to ES – then the listening port of the native connections. | 9300 |
| What is the Elastic Server Cluster name: | The ES cluster name as configured cluster.name | No default |
| What is the desired number of Elastic Concurrent Requests: | This is the number of concurrent Bulk requests to send to Elastic. | 4 |

| | Default is 4 and is sufficient in normal configurations | |
|---|---|---|
| What is the desired size of the Log Processor Queue Size | This is log queue size between the receiver threads and the indexer. 200 is optimal but care should be taken as it affect he JVM heap size. | 200 |
| What is the desired number of Log Processor Threads: | This is number of threads processing incoming logs – parses and indexes. The default is 8. This should be half the number CPU's in the system. | 8 |
| What is the desired JVM Heap Size: | Default JVM heap size. Optimal sizing based on other configuration. This should be increased as the other parameters are increased. | 1024m |
| What is the path to the Java installation: | Path to Java. Should be auto-detected and will only be prompted for if it is found in the "normal" locations. | No default unless found by installation script. |

- Once installed – the Index Template (like a schema) needs to be installed in the ElasticSearch instance
  - As the elastic user – cd /home/elastic/bwlogreceiver/bwlogreceiver
  - ./log_template.pl <hostname of the ElasticSearch instance>
  - See the following link for more information on index templates: https://www.elastic.co/guide/en/elasticsearch/reference/2.1/indices-templates.html
- To start the application, do the following:
  - As the elastic user – "/home/elastic/bwlogreceiver/bwlogreceiver/bwlogreceiver.pl –start"
  - To verify application status – "/home/elastic/bwlogreceiver/bwlogreceive/bwlogreceiver.pl –showrun"
- To stop the application, do the following:
  - As the elasticuser – "/home/elastic/bwlogreceiver/bwlogreceiver/bwlogreceiver.pl –stop"

# 5 CDR Collectors

## 5.1 bwcdrprocessor

This application runs on another server. The package is provided as a self-extracting archive and is required to be installed as a normal user – in our example "elastic". It is installed in the current working directory. Into a new directory bwcdrprocessor. Inside the bwcdrprocessor directory – there will be a symlink called bwcdrprocessor which is symlinked to bwcdrprocessor_<version> to facilitate upgrades.

The package file name is structured as bwcdrprocessor_<version>.run.

The way this collector works is that the BroadWorks Application Server is configured to ftp the accounting records (either XML or CSV) to the server that is acting as the collector. Once there, this application is executed through cron to audit the receiving directory for new files which then are parsed and processed into ElasticSearch. The directory structure needed for this is a main directory location with a directory with a new and archive directory within it. In our example we have used – we'll use the following

- /home/elastic/cdrfiles
- /home/elastic/cdrfiles/new
- /home/elastic/cdrfiles/archive

What happens is the "new" directory is where the Application Servers push the files to – then the application will process then move the file(s) to the archive directory.

Please review the Broadworks Application Server CLI Guide for information to configure accounting for this application.

### 5.1.1 Installation & Configuration

The following are the commands and configuration to install bwcdrprocessor.

The following detail of the commands assumes running in the same server as ES was installed into (I.E. has user elastic)

- Login to the server as elastic
- cd to /home/elastic
- chmod 755 bwcdrprocessor_<version>.run
- ./bwcdrprocessor_<version>.run
- The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| What is the Elastic Server host: | IP or hostname of the ES server. Assuming local – you can enter 127.0.0.1 | No default |
| What is the Elastic Server port to use: | Normally 9300 – if there have been customizations to ES – then the listening port of the native connections. | 9300 |
| What is the Elastic Server Cluster name: | The ES cluster name as configured cluster.name | No default |
| What is the prefix to use for ElasticSearch CDR Indexes: | This is the prefix to use for the applications creation of CDR Indexes. BroadSoft suggests bwcdr | No default |

| | as this the index patterns used by the Visualizations and Dashboards provided. | |
|---|---|---|
| What interval is desired for unique Elastic Search Indexes: | This is the interval that a new index will be created. The options are Never, Monthly or Daily | Never |
| What is the path to process CDR files: | This is the path that is discussed in section 4.1 | No default |

- Once installed – the Index Template (like a schema) needs to be installed in the ElasticSearch instance
  - o As the elastic user – cd /home/elastic/bwcdrprocessor/bwcdrprocessor
  - o ./cdr_template.pl <hostname of the ElasticSearch instance>
  - o See the following link for more information on index templates: https://www.elastic.co/guide/en/elasticsearch/reference/2.1/indices-templates.html
- An example cron is the following (this follows that the Application Server is configured to send files 288 times (Every 5 minutes).
  - o 0,5,10,15,20,25,30,35,40,45,50,55   * * * * /home/elastic/bwcdrprocessor/bwcdrprocessor/cdrProcessor.pl > /home/elastic/bwcdrprocessor/bwcdrprocessor/cdrProcessor`date +\%d`.log 2>&1

## 5.2   bwradiusprocessor

This application runs on another server. The package is provided as a self-extracting archive and is required to be installed as a normal user – in our example "elastic". It is installed in the current working directory. Into a new directory bwradiusprocessor. Inside the bwradiusprocessor directory – there will be a symlink called bwradiusprocessor which is symlinked to bwradiusprocessor _<version> to facilitate upgrades.

The package file name is structured as bwradiusprocessor _<version>.run.

The way this collector works is that the BroadWorks Application Server is configured to push the radius accounting records to the server hosting this application. This is a running application that parses and indexes the radius records real time.

Please review the Broadworks Application Server CLI Guide for information to configure accounting for this application.

### 5.2.1   Installation & Configuration

The following are the commands and configuration to install the bwradiusprocessor.

The following detail of the commands assumes running in the same server as ES was installed into (I.E. has user elastic)

- Login to the server as elastic
- cd to /home/elastic
- chmod 755 bwradiusprocessor_<version>.run
- ./ bwradiusprocessor _<version>.run

- The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| What is the Elastic Server host: | IP or hostname of the ES server. Assuming local – you can enter 127.0.0.1 | No default |
| What is the Elastic Server port to use: | Normally 9300 – if there have been customizations to ES – then the listening port of the native connections. | 9300 |
| What is the Elastic Server Cluster name: | The ES cluster name as configured cluster.name | No default |
| What is the prefix to use for ElasticSearch CDR Indexes: | This is the prefix to use for the applications creation of CDR Indexes. BroadSoft suggests bwcdr as this the index patterns used by the Visualizations and Dashboards provided. | No default |
| What interval is desired for unique Elastic Search Indexes: | This is the interval that a new index will be created. The options are Never, Monthly or Daily | Never |
| What is the Radius Accounting Shared Secret: | This should be configured as the same value as provisioned in the application server. | No default |

- Once installed – the Index Template (like a schema) needs to be installed in the ElasticSearch instance
    o As the elastic user – cd /home/elastic/bwradiusreceiver/bwradiusreceiver
    o ./radius_cdr_template.pl <hostname of the ElasticSearch instance>
    o See the following link for more information on index templates: https://www.elastic.co/guide/en/elasticsearch/reference/2.1/indices-templates.htm

- To start the application, do the following:
    o As the elastic user – "/home/elastic/bwradiusprocessor/ bwradiusprocessor/bwradiusreceiver.pl –start"
    o To verify application status – "/home/elastic/bwradiusprocessor/ bwradiusprocessor/bwradiusreceiver.pl –showrun"

- To stop the application, do the following:
    o As the elasticuser – "/home/elastic/bwradiusprocessor/ bwradiusprocessor/bwradiusreceiver.pl –stop"

# 6    Message Archive Processor

## 6.1    messagearchiveprocessor

This application runs on another server. The package is provided as a self-extracting archive and is required to be installed as a normal user – in our example "elastic". It is installed in the current working directory. Into a new directory messagearchiveprocessor. Inside the messagearchiveprocessor directory – there will be a symlink called messagearchiveprocessor which is symlinked to messagearchiveprocessor _<version> to facilitate upgrades.

The package file name is structured as messagearchiveprocessor _<version>.run.

This processor is an application that is executed from cron and fetches the Message Archive file from the Profile Servers that generated by the Messaging Server. It indexes the instant messages that have been archived (the application ignores the content of the instant messages) and indexes them into ElasticSearch. The purpose of this application is for analysis and patterns of usage across the Enterprises and Service Providers.

Please review the Message Archive documentation on Xchange for configuring the access lists for this application to connect and fetch the archived logs.

### 6.1.1    Installation & Configuration

The following are the commands and configuration to install messagearchiveprocessor.

The following detail of the commands assumes running in the same server as ES was installed into (I.E. has user elastic)

■    Login to the server as elastic

■    cd to /home/elastic

■    chmod 755 messagearchiveprocessor _<version>.run

■    ./messagearchiveprocessor _<version>.run

■    The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| What is the ProfileServer URL: | This is the URL to the Profile Server URL configured for the Message Archive application. | No default |
| What is the ProfileServer UserName: | This is the username to pass to the Profile Server to fetch the Message Archive logs. | No default |
| What is the ProfileServer Password: | | |
| What is the Elastic Server host: | IP or hostname of the ES server. Assuming local – you can enter 127.0.0.1 | No default |
| What is the Elastic Server port to use: | Normally 9300 – if there have been customizations to ES – then the listening port of the native connections. | 9300 |
| What is the Elastic Server Cluster name: | The ES cluster name as configured cluster.name | No default |

- Once installed – the Index Template (like a schema) needs to be installed in the ElasticSearch instance
    - As the elastic user – cd /home/elastic/messagearchiveprocessor/messagearchiveprocessor
    - ./messagearchive_template.pl <hostname of the ElasticSearch instance>
    - See the following link for more information on index templates: https://www.elastic.co/guide/en/elasticsearch/reference/2.1/indices-templates.htm
- An example cron is the following (this follows the default value that Message Archives are generated once an hour).
    - 45 * * * * /home/elastic/messagearchiveprocessor/messagearchiveprocessor/processMessageArchive > /home/elastic/messagearchiveprocessor/messagearchiveprocessor/messagearchiveprocessor`date +\%d`.log 2>&1

# 7 Subscriber Dump

## 7.1 subscriberdumpprocessor

This application runs on another server. The package is provided as a self-extracting archive and is required to be installed as a normal user – in our example "elastic". It is installed in the current working directory. Into a new directory subscriberdumpprocessor. Inside the subscriberdumpprocessor directory – there will be a symlink called subscriberdumpprocessor which is symlinked to subscriberdumpprocessor_<version> to facilitate upgrades.

The package file name is structured as subscriberdumpprocessor_<version>.run.

This processor is an application that is executed from cron and does the following:

- Logs in through OCI to the Secondary Application Server

- Executes the SystemExportSubscriberRequest OCI Transaction. This transaction dumps specific Enterprise/Group/User information into XML files

- Logs out of OCI

- scp's the files from the Application Server

- Processes the XML files and indexes the content into ElasticSearch

Note: If there is apprehension to storing Admin credential on this server – it is possible to simply process the files without doing the OCI command or the SSH. This way a back office could do the processing and simply ship the files to location the application can process the files.

Please review the Message Archive documentation on Xchange for configuring the access lists for this application to connect and fetch the archived logs.

### 7.1.1 Installation & Configuration

The following are the commands and configuration to install subscriberdumpprocessor.

The following detail of the commands assumes running in the same server as ES was installed into (I.E. has user elastic)

- Login to the server as elastic

- cd to /home/elastic

- chmod 755 subscriberdumpprocessor_<version>.run

- ./subscriberdumpprocessor_<version>.run

- The following table represents the prompts and a description that will be required for installation.

| Prompt | Description | Default |
|---|---|---|
| What is the Elastic Server host: | IP or hostname of the ES server. Assuming local – you can enter 127.0.0.1 | No default |
| What is the Elastic Server port to use: | Normally 9300 – if there have been customizations to ES – then the listening port of the native connections. | 9300 |

| | | |
|---|---|---|
| What is the Elastic Server Cluster name: | The ES cluster name as configured cluster.name | No default |
| What is the Elastic Search Index Name to index Subscriber Export data into: | The name of the Index to store the message archive content. | No default |
| What is the Secondary AS host/IP: | The IP address or hostname of the Secondary AS. | No default |
| What is the OCI Admin Username: | An Admin user name for the Application Server | No default |
| What is the OCI Admin Password: | The password for the Admin user above. | No Default |

An example cron is the following (only recommending to do once a day – can be modified to do once a week or month if desired):

35 01 * * *
/home/elastic/subscriberdumpprocessor/subscriberdumpprocessor/SubscriberExport Driver.pl >> /home/elastic/subscriberdumpprocessor/subscriberdumpprocessor/processor.log 2>&1

- To start the application – shouldn't be done until the receiver is installed and running – do one of the following
    - As root – "service bwlogsender start"
    - As bwadmin – "/usr/local/bwlogsender/bwlogsender –start
    - To verify application status – "/usr/local/bwlogsender/bwlogsender --showrun