ESP-VAERS: Technical Guide for ESP-VAERS system managers.

By Bob Zambarano, 31 May 2019.

Contents

[Overview 2](#_Toc10210032)

[ESP-VAERS Installation and configuration 2](#_Toc10210033)

[Determine the server hardware requirements for ESP 2](#_Toc10210034)

[Install ESP 2](#_Toc10210035)

[Install PHINMS 3](#_Toc10210036)

[Set up the data feed from the ETL process, configure daily data load and VAE detection process 3](#_Toc10210037)

[ESP-VAERS ongoing operations 5](#_Toc10210038)

## Overview

This document provides a “How-To” for obtaining, installing, configuring, implementing and maintaining ESP-VAERS. This document is intended for a technical audience. Before using this document, you should read the accompanying document “Optimal Installation of ESP-VAERS”. The Optimal installation document is intended for both a technical and less-technical audience; it provides a narrative context for the steps outlined below. Many parts of this document are maintained elsewhere, and are simply provided as web links in the text below. Web resources for ESP can be found here: <https://www.esphealth.org/>

Resources specific to ESP-VAERS can be found here: <https://espnet.atlassian.net/wiki/x/AYCXM>

## ESP-VAERS Installation and configuration

### Determine the server hardware requirements for ESP

Storage capacity requirements heuristic:

Count of active patients \* number of years \* 0.00025 = Gigabytes of storage required

For example, a system with 300,000 patients and 3 years of data would require:

300,000\*3\*0.00025=225Gb storage

Memory (RAM) requirements heuristic:

2 \* ((Storage capacity requirements / 2) / 50) = Gigabytes of memory required

For example, a system that requires 225GB of storage would require:

2 \* ((225 / 2) /50) = 4.5Gb memory

You would want to round up as necessary.

CPU requirements heuristic:

2 + CEILING(number of new encounter records per day / 40,000) - 1 + CEILING(number of new lab records per day / 40,000) -1 = Number of CPUs

For example, a system that processes 20,000 encounters and 50,000 labs a day would require:

2 + CEILING(20000/40000) -1 + CEILING(50000/40000)-1 = 3 CPUs

These are rough estimates. If you are able to dynamically allocate resources to your ESP server (this is straight-forward for many virtual hosting environments), it is of course acceptable to start with fewer resources and allocated additional resources as required.

### Install ESP

To complete an ESP installation, follow the accompanying instructions “HowTo - Install and Configure ESP on Ubuntu 18.04”. (This link will always provide the most up-to-date version of these instructions: <https://espnet.atlassian.net/wiki/spaces/EP/pages/42958879/ESP+Implementation+Kit+Materials>).

Step 14: Setting Up Basic Disease Detection can be ignored, unless you will be using ESP for disease detection as well as VAERS reporting.

There are some ESP-VAERS specific configuration requirements when editing application.ini under the reporting section. Instructions for setting these values are provided in the default INI:

phinms\_server = 'your\_phinms\_server'

phinms\_username = 'your\_phinms\_sftp\_username'

phinms\_path = 'your\_phinms\_path'

# Path to vaers line listing reports (PHI and no-PHI)

# Must exist and must have esp read-write access

# Default value is ESP home directory, fine for test and dev

# Alternative below is suggestion for production implementation

vaers\_linelist\_path = '/home/esp/'

# Is sending AE reports via PHIN-MS enabled?

# set to True to use this feature

vaers\_send\_report = 'False'

# Is the EMR updated via the transcription interface when a VAERS report is transmitted to CDC?

vaers\_update\_emr = 'True'

# Login details for SFTP server where transcription interface messages will be sent

update\_emr\_server = 'your\_update\_sftp\_server'

update\_emr\_username = 'your\_update\_sftp\_username'

update\_emr\_path = 'your\_update\_sftp\_path'

# If set, send “suspected vaccine AE” message to the specified provider instead of the normal reviewer

# This must be a valid "Natural\_Key" value from the EMR\_PROVIDER table, with corresponding data to identify the override clinician reviewer

vaers\_override\_clinician\_reviewer = ''

# The VAERS autosender is the clinician identified by the site as the point of contact for auto-sent vaers reports.

vaers\_autosender = ''

### Install PHINMS

PHINMS is the VAERS message transfer software that provides secure authenticated and authorized transfer of VAERS messages to the CDC VAERS reporting system. This is installed on a MS Windows system and does not require anything more than a single CPU and sufficient storage for the OS and a relatively small number of VAERS message files: An additional 5Gb of storage beyond the needs of the OS will be more than sufficient.

PHINMS installation and operation is documented extensively elsewhere: <https://www.cdc.gov/phin/tools/phinms/installation.html>.

PHINMS installation is likely to require Network support to ensure that routes through the firewall are opened for PHINMS traffic.

### Set up the data feed from the ETL process, configure daily data load and VAE detection process

The data feed is mentioned briefly in the Installation how-to. The document “Optimal Installation of ESP” provides guidance on how to set up the ETL system for the data feed. With the ETL developed and testing, implementation is as follows.

1. Determine the amount of historical data required for the system. This is typically a minimum of two years. Run the ETL process to generate the historical data files in the ESP incoming data folder, as specified during the ESP system installation and configuration.
2. Execute the following ESP command from the Linux shell:

* $> [$ESPHOME]/bin/esp load\_epic

The command should be run from a detachable process, such a tmux or nohup, as it can take considerable time to complete. This can be several days to several weeks depending on the amount of historic data being loaded. The command name “load\_epic” is vestigial – ESP was originally developed to work with an Epic system. The command will load ETL data from any EHR system.

1. Monitor the historic load. When it is complete, configure the lab test and vaccine mapping data. From the Linux command line, run the command:

[$ESPHOME]/bin/esp concordance

Login to the ESP administrative interface you set up during the ESP installation. Navigate to Admin>Unmapped Lab Tests Report. Use the lab mapping interface to map local lab codes to the required ESP lab concepts. When done, navigate to VAERS>Vaccine Mapping. Map the local immunization names to the CDC standard names. This is described in some detail in the accompanyin “Optimal Installation of ESP” document.

1. Prepare a shell script that will run the ETL process on a regular basis and then run the VAE detection and messaging processes. Here is an example:

#!/bin/bash

ESP\_DIR=/srv/esp

LOGFILE=$ESP\_DIR/log/daily\_cron.log.$$

VAERS\_ESP=$ESP\_DIR/vaers/test/bin/esp

exec 5>&1 6>&2 >>$LOGFILE 2>&1

. $ESP\_DIR/vaers/test/bin/activate

export PIP\_RESPECT\_VIRTUALENV=true

export PIP\_REQUIRE\_VIRTUALENV=true

python $ESP\_DIR/scripts/esp\_etl.py -i $ESP\_DIR/scripts/esp\_vaers.ini

#The esp\_etl.py script runs the ELR process. Default mode is to

# generate data collected from the prior day and save to the ESP

# data incoming folder.

deactivate

($VAERS\_ESP load\_epic -l --reload && \

$VAERS\_ESP immunization\_checker && \

$VAERS\_ESP vaers -a && \

$VAERS\_ESP vaers\_hl7 && \

$VAERS\_ESP status\_report --send-mail)

exec 1>&5 2>&6

Besides load\_epic, the ESP commands include above are:

* immunization\_checker updates immunization records to exclude non-immunization data (tb tine test, gamma globulin, etc.)
* vaers run the VAE detection process
* vaers\_hl7 generates the various hl7 message files and transfers them as appropriate
* status\_report generates an email describing the outcome of the various commands.

Add this shell script to the ESP users crontab. It should be run daily at off-hours.

## ESP-VAERS ongoing operations

Daily operations include: review the daily status report email.

Weekly operations include: (all these activities can be monitored via automated alerting systems.)

* review the ESP and PHINMS system and auth logs for any suspicious events
* check and confirm that ESP backups have been running
* run the ESP concordance command, and check for unmapped labs and vaccines
* check the unused storage capacity of the ESP and PHINMS systems and ensure there is sufficient available storage for ongoing operations
* check the PHINMS administrative interface and confirm that any new messages have be routed and received.

On an as needed basis: when unmapped labs or vaccines are encountered, use the administrative mapping interfaces to map as appropriate.

There should be a schedule for performing system updates to apply security patches, and for testing backups.

The PHINMS system relies on a certificate pack with an expiration setting. New certificates must be requested and installed, typically on a once-yearly basis.