



All Categories



Search



ATAC > EDR > Getting started

Getting started



[EDRM] EDRM Installation Guide

Follow



이우람(Liam)

Created : 04/10/2024 · Edited : 04/18/2024

1. Overview

- This guide provides the overall procedure for installing EDRM (Endpoint Detection & Response) on the prepared Linux server.
- The content of this article is based on the following versions.
OS: Rocky 8.6
EDRM: 2.0.4.15 (Build 2276)
- Please refer to the following link for OS installation guide.
[\[OS\] EPPM/EDRM Deployment Operating System \(Linux\) Installation Guide](#)

2. Table of Contents

- Install Required Packages for EDRM
- Install EDRM RPM
- Set Up EDR CLI

3. Install Required Packages for EDRM

※ This is the required step which sets up the required packages before installing EDRM.

※ The code blocks below are the same as the messages displayed on the terminal.

3-1) Prepare OS Installation File

- Require the same version files (Use the FULL version containing all packages) as the prepared OS (CD or ISO).
- For version 7.x, the name of the file containing all packages contains 'Everything'.
- For version 8.x, the name of the file containing all packages contains 'dvd'.

3-2) Mount Image

- Create /cdrom path.

```
[root@localhost ~]# mkdir /cdrom
```

- Mount ISO file. (Provided that the ISO file to be used is located in the /tmp/ISO path)

```
[root@localhost ~]# mount -o loop /tmp/ISO/Rocky-8.6-x86_64-dvd1.iso /cdrom
mount: /cdrom: WARNING: device write-protected, mounted read-only.
```

- If the mount is completed successfully, confirm the files in the /cdrom path as shown below.

```
[root@localhost ~]# ll /cdrom
Total 14
dr-xr-xr-x. 4 root root 2048 May 16 2022 AppStream
dr-xr-xr-x. 4 root root 2048 May 16 2022 BaseOS
dr-xr-xr-x. 3 root root 2048 May 16 2022 EFI
-r--r--r--. 1 root root 2204 May 30 2022 LICENSE
-r--r--r--. 1 root root 883 May 16 2022 TRANS.TBL
dr-xr-xr-x. 3 root root 2048 May 16 2022 images
dr-xr-xr-x. 2 root root 2048 May 16 2022 isolinux
-r--r--r--. 1 root root 86 May 16 2022 media.repo
```

3-3) Upload the EDRM Installation File, 'edr_installer.tar', to the Server and Unzip

- Upload the installation file (edr_installer.tar) to the /root path
- Use the tar command to unzip the installation file.

```
[root@localhost ~]# tar xvf /root/edr_installer.tar
edr_installer-2.0.4.15-2276.x86_64.rpm
edrinstall_r5.sh
install_os_package.sh
local.repo
```

3-4) Install OS Packages

- Run 'install_os_package.sh' from the extracted files.

```
[root@localhost ~]# ./install_os_package.sh
Local_BaseOS 113 MB/s | 2.6 MB 00:00
Local_AppStream 140 MB/s | 7.8 MB 00:00
```

```
Last metadata expiration check: 0:00:01 ago on Sun 25 Feb 2024 04:03:19 PM KST.  
Package rsyslog-8.2102.0-7.el8.x86_64 is already installed.  
Package libevent-2.1.8-5.el8.x86_64 is already installed.  
Package psmisc-23.1-5.el8.x86_64 is already installed.  
...  
Install 98 Packages  
  
Total size: 58 M  
Installed size: 171 M  
Is this ok [y/N]:
```

- Enter 'y'.

```
Is this ok [y/N]: y  
Downloading Packages:  
Running transaction check  
Transaction check succeeded.  
Running transaction test  
Transaction test succeeded.  
Running transaction  
...  
telnet-1:0.17-76.el8.x86_64 timedatex-0.5-3.el8.x86_64  
tree-1.7.0-15.el8.x86_64 unixODBC-2.3.7-1.el8.x86_64  
unzip-6.0-46.el8.x86_64 vim-common-2:8.0.1763-16.el8_5.13.x86_64  
vim-enhanced-2:8.0.1763-16.el8_5.13.x86_64 vim-filesystem-2:8.0.1763-  
16.el8_5.13.noarch  
vsftpd-3.0.3-35.el8.x86_64 wget-1.19.5-10.el8.x86_64  
zip-3.0-23.el8.x86_64  
  
Complete!
```

4. Install EDRM RPM

- Run EDRM installation script.

```
[root@localhost edr]# ./edrinstall_r5.sh  
-----  
Tool provides the following three action for EDR Server  
[ INSTALL | UPDATE | REMOVE | PERFECT_REMOVE | RETRY_UPDATE ]  
-----  
Enter the action :
```

- After entering 'INSTALL', enter the settings values. (Enter 'no' for cli setting and then edit it in 4-2.)

```
Enter the action : INSTALL
```

```
< Input the value >
```

```
-----
[ip] [buildnum] [cli autoset yes:no] [reinstall yes:no]
192.168.56.256 2276 no no
```

- Confirm the entered settings values and then enter 'y'. (Make sure to check the Time zone.)

```
< Input the value >
```

```
-----
[ip] [buildnum] [cli autoset yes:no] [reinstall yes:no]
192.168.56.256 2276 no no
```

```
-----
> IP : [ 192.168.56.256 ]
```

```
> Buildnum : [ 2276 ]
```

```
> Cli autoset : [ no ]
```

```
> Reinstall : [ no ]
```

```
-----
----- Continue to install?(y/n) y
```

```
...
```

- The installation is successfully completed if the messages as shown below appears.

```
Installed:
```

```
edr_amazon_corretto-11.0.12.7.1-1.x86_64 edr_common-2.0.4.15-2276.x86_64
```

```
edr_edrcmd-2.0.4.15-2276.x86_64
```

```
edr_edrup-2.0.4.15-2276.x86_64 edr_kafka-3.5.1-1.x86_64 edr_ml-2.6.1.1-1.x86_64
```

```
edr_service-2.0.4.15-2276.x86_64 edr_tool-2.0.4.15-2276.x86_64 edr_web-2.0.4.15-2276.x86_64
```

```
edr_zookeeper-3.9.1-1.x86_64 iftop-1.0-0.21.pre4.el8.x86_64 libssh2-1.9.0-5.el8.x86_64
```

```
...
```

```
Complete!
```

5. Set Up EDR CLI

※ The code blocks below are the same as the messages displayed on the terminal.

- Executable File: /opt/ahnlab/epp/bin/eppcli

```
[root@localhost ~]# /opt/ahnlab/edr/bin/edrcli
```

- Create eppcli account. (e.g. Create an account with User ID 'edrcli256')

```
create cli account
enter user id :edrcli256
Do you want to add new account (edrcli256) ? [Yes|No] : yes
Changing password for user edrcli256.
New password:<Input Required>
Retype new password:<Input Required>
passwd: all authentication tokens updated successfully.
You must reconnect with the new admin
It will disconnect after 3 seconds
```

- Re-run edrcli and then set the site auth key.

```
[root@localhost ~]# /opt/ahnlab/edr/bin/edrcli
[SITE_KEY] change site key : [(A)uto/(M)anual] M
[SITE_KEY] enter new sitekey : <Input Required>
[SITE_KEY] retype new sitekey : <Input Required>
[2024-02-21T08:38:54.866Z][e5001033] :
[2024-02-21T08:38:54.866Z][e5001033] :
```

- Set up a site auth key and a server key.

```
[SITE_AUTH_KEY] change site auth key : [(A)uto/(M)anual] M
[SITE_AUTH_KEY] enter site auth key : <Input Required>
[SITE_AUTH_KEY] retype site auth key : <Input Required>
input master ip :192.168.56.256
[SERVER_KEY] enter server key : <Input Required>
[SERVER_KEY] retype server key : <Input Required>
```

- Set up the edrrdb (PostgreSQL) account.

```
[EDRRDB] Do you want to auto create edrrdb user? [Yes|No] :no
[EDRRDB] enter edrrdb user :edrrdb256
[EDRRDB] Do you want to change edrrdb user : (edrrdb256) ? [Yes|No] : yes
[EDRRDB] enter edrrdb password :<Input Required>
[EDRRDB] retype edrrdb password :<Input Required>
Success change
```

- Set up the nosql admin (MongoDB) account.

```
[NOSQL] Do you want to auto create nosql admin user? [Yes|No] :no
[NOSQL] enter nosql admin user :nosqladmin256
[NOSQL] Do you want to change nosql admin user : (nosqladmin256) ? [Yes|No] : yes
[NOSQL] enter nosql admin password :<Input Required>
[NOSQL] retype nosql admin password :<Input Required>
Success change
```

- Set up the nosql user (MongoDB) account.

```
[NOSQL] Do you want to auto create nosql user? [Yes|No] :no
[NOSQL] enter nosql user :nosqluser256
[NOSQL] Do you want to change nosql user : (nosqluser256) ? [Yes|No] : yes
[NOSQL] enter nosql password :<Input Required>
[NOSQL] retype nosql password :<Input Required>
Success change
```

- Set up the cached (Redis) password.

```
[CACHED] Do you want to auto create cached password? [Yes|No] :no
[CACHED] enter cached password :<Input Required>
[CACHED] retype cached password :<Input Required>
Success change
```

- Complete the settings and then connect to the web.

```
[Connect Web URL] https://192.168.56.256:8903
```

- You need to deliver the set username and password to the client for safekeeping.

Was this article helpful?

Yes

No

0 out of 0 found this helpful

Have more questions? [Submit a request](#)

[Return to top](#) ^

Recently viewed articles

[EDRM] Preparing for Installation

[EDRM] Specification (Requirements)

[EPPM] EPPM Installation Guide

[EPPM] Installing Agent

[EPPM] Master Resgistration

[OS] EPPM/EDRM Deployment Operating System (Linux) Installation Guide

0 comments

© AhnLab, Inc. All rights reserved.

Privacy & Security

English (US)