



All Categories



Search



ATAC > EDR > Technical Guide

Technical Guide



[EDR2] EDRM P5 Installation Guide

Follow



이우람(Liam)

Created : 05/20/2024 · Edited : 07/22/2024

1. Overview

- EDRM P5 installation guide
- EDRM P5 version operates with [EPPM 1.0.16.24](#) version

2. Table of Contents

- EDRM Installation Guide
- Create OpenSearch Template
- OpenSearch Node configuration
- Add Domain and Apply Role

3. EDRM Installation Guide

- [\[EDR2\] EDR 2.0 Installation Guide](#)
- Basic EDRM installation method remains the same as before (CLI Auto Setting: NO), but additional steps are required before adding domains and applying roles

4. Create OpenSearch Template

4-1) Default OpenSearch Account After Initial Setup

Note : During the initial installation of OpenSearch, the default account name and password are `edropensearch<4th octet of the server IP>`

ex) server IP 10.10.70.156 -> username & PW: edropensearch156

4-2) Create Template - OpenSearch status check

```
curl -X GET "https://<EDRM IP>:8961/_cluster/health" -u "edropensearch<서버 IP의 4 번째 옥텟>:edropensearch<서버 IP의 4 번째 옥텟>" --insecure
```

Check for "status": "green" then move on

```
[epvm-202][root][epptool4]# curl -X GET "https://10.2.101.202:8961/_cluster/health" -u "edropensearch202:edropensearch202" --insecure
{"cluster_name":"edr-opensearch-cluster","status":"green","timed_out":false,"number_of_nodes":3,"number_of_data_nodes":3,"discovered_master":true,"discovered_cluster_manager":true,"active_primary_shards":158,"active_shards":165,"relocating_shards":0,"initializing_shards":0,"unassigned_shards":0,"delayed_unassigned_shards":0,"number_of_pending_tasks":0,"number_of_in_flight_fetch":0,"task_max_waiting_in_queue_millis":0,"active_shards_percent_as_number":100.0}[epvm-202][root][epptool4]#
```

4-3) Create Template

```
sudo /opt/ahnlab/edr/bin/search-engine/edr_opensearch_cli.sh
create_index_templates
```

execute command

```
Creating OpenSearch index templates.....
```

wait until message ends

5. OpenSearch Node Configuration

5-1) Check Index before setting

• Check Index Template

```
curl -X GET "https://<EDRM IP>:8961/_cat/templates" -u "edropensearch<서버 ip의 4 번째 옥텟>:edropensearch<서버 ip의 4 번째 옥텟>" --insecure
```

25 counts of Index

```

root@localhost:~# curl -X GET "https://10.10.70.156:8961/_cat/templates" -u "edropsearch156:edropsearch156" --insecure
template_tb_edr_diagram_relation      [tb_edr_diagram_relation]      0 [common_settings_and_analyzer]
template_tb_log_server_resource        [tb_log_server_resource]       0 [common_settings_and_analyzer]
template_tb_log_audit_transaction      [tb_log_audit_transaction]     0 [common_settings_and_analyzer]
template_tb_log_edr_network_info      [tb_log_edr_network_info_*)    0 [common_settings_and_analyzer]
template_tb_log_service                [tb_log_service]               0 [common_settings_and_analyzer]
template_tb_master_edr_inoutflow       [tb_master_edr_inoutflow]      0 [common_settings_and_analyzer]
template_tb_log_audit_exception        [tb_log_audit_exception]       0 [common_settings_and_analyzer]
template_tb_edr_incident               [tb_edr_incident]              0 [common_settings_and_analyzer]
template_tb_edr_diagram_analysis       [tb_edr_diagram_analysis]      0 [common_settings_and_analyzer]
template_tb_log_immediate_task         [tb_log_immediate_task]        0 [common_settings_and_analyzer]
template_tb_log_edr_evidence           [tb_log_edr_evidence_*)       0 [common_settings_and_analyzer]
template_tb_history_system              [tb_history_system]            0 [common_settings_and_analyzer]
template_tb_log_edr_behavior           [tb_log_edr_behavior_*)       0 [common_settings_and_analyzer]
template_tb_log_process_block          [tb_log_process_block]         0 [common_settings_and_analyzer]
template_tb_log_audit                  [tb_log_audit]                 0 [common_settings_and_analyzer]
template_tb_log_os_event               [tb_log_os_event_*)           0 [common_settings_and_analyzer]
template_tb_log_edr_powershell         [tb_log_edr_powershell_*)     0 [common_settings_and_analyzer]
template_tb_edr_diagram                [tb_edr_diagram]              0 [common_settings_and_analyzer]
template_tb_log_timeline               [tb_log_timeline_*)           0 [common_settings_and_analyzer]
template_tb_log_engine_update          [tb_log_engine_update]         0 [common_settings_and_analyzer]
template_tb_v3_alert_log               [tb_v3_alert_log]              0 [common_settings_and_analyzer]
template_tb_log_backup                 [tb_log_backup]                0 [common_settings_and_analyzer]
template_tb_log_edr_inoutflow          [tb_log_edr_inoutflow_*)      0 [common_settings_and_analyzer]
template_tb_edr_diagram_item           [tb_edr_diagram_item]         0 [common_settings_and_analyzer]
template_tb_edr_incident_confirm_state_history [tb_edr_incident_confirm_state_history] 0 [common_settings_and_analyzer]
root@localhost:~#

```

<IP 10.10.70.156 in the example image>

- Check Index Shard

```
curl -X GET "https://<EDRM IP>:8961/_cat/indices?v" -u
"edropensearch156:edropensearch156" --insecure | grep -v -e ".opensearch" -e
".opendistro" -e ".plugin"
```

25 count of index, all rep 0

```

[root@localhost ~]# curl -X GET "https://10.10.70.156:8961/_cat/indexes?v=&u=edrsearch156:edrsearch156" --insecure | grep -v -e ".opensearch" -e ".opendistro" -e ".plugin"
% Total    % Received % Xferd  Average Speed   Time    Time     Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 5719 100 5719    0    0 81700      0 --:--:-- --:--:-- --:--:-- 81700

health status index                                uuid                                pri rep docs.count docs.deleted store.size pri.store.size
green open      tb_log_immediate_task                          YFFmZASAQSGSVeMBbi-fA      2    0    0            0            416b
green open      tb_log_edr_evidence_20240519                  kmqde3WzSp2T0ZSG6gpBVa    1    0    0            0            208b
green open      tb_log_edr_evidence_20240518                  B1NwupibTCemY4WNgpt3NQ    1    0    0            0            208b
green open      tb_edr_diagram_item                          btBHFJB2SOMW1x6ApE-zyA    5    0    0            0            1kb
green open      tb_log_edr_evidence_20240517                  lJpFSK2QRz26nyqW6ra55Q    2    0    0            0            416b
green open      tb_log_edr_powershell_20240518                cFQ_QCKPSN24F6GwYOGug    1    0    0            0            208b
green open      tb_log_edr_powershell_20240519                SY6N3nJMSf18LwUvAj3Q     1    0    0            0            208b
green open      tb_log_process_block                         fHmUeS2JbR3y3w-o0UtiTw    1    0    0            0            208b
green open      tb_log_os_event_20240518                      f1imeKCQ02TMHvN5G4dw     1    0    0            0            208b
green open      tb_log_edr_powershell_20240517                xS0dW8y1a5e2M1h3o1K     1    0    0            0            1kb
green open      tb_log_os_event_20240519                      CJe-BdQPT4Sd0Lrmbz7WpQ   1    0    0            0            208b
green open      tb_log_audit_exception                       JPlqc0IUSC6D8wAyhb8zTg   1    0    0            0            208b
green open      tb_log_engine_update                         cX9VqvKzQOSVApFgIP3CQ    1    0    0            0            208b
green open      tb_edr_diagram_relation                      uoqct8MGOpC0UM-t0x1lgg    5    0    0            0            1kb
green open      tb_log_audit                                2d-NkVnNSKa_B5cCu0CYFw   2    0    0            0            416b
green open      tb_edr_incident_confirm_state_history          msYDeD06QeeK2L3qRfgw1g   1    0    0            0            208b
green open      tb_edr_diagram                              10CR7T4u5UrZMYBMfjpnA    2    0    0            0            416b
green open      tb_log_backup                               aWl-pezdOpQz1lQjx_1lPg   2    0    0            0            416b
green open      tb_log_server_resource                       RdXsgxpXQN-Pr39KfLW4AQ    1    0    0            0            208b
green open      tb_history_system                           Ewqj3JhyURLG6g0h7001NTg  1    0    0            0            208b
green open      tb_edr_incident                             3T2AU0Z8R9u0pvoXKPGICA   2    0    0            0            416b
green open      tb_log_edr_behavior_20240519                  v_QMTJg-RV6D9y35P0metug   1    0    0            0            208b
green open      tb_log_edr_inoutflow_20240517                 kRnVQjTfLy5n-7Tz577Q    2    0    0            0            416b
green open      tb_log_edr_behavior_20240518                  iucuaH5aFm6Z1Kf52Y0A     1    0    0            0            208b
green open      tb_log_edr_network_info_20240517              IuIwxeGn1MQT2wihH7z1A    2    0    0            0            416b
green open      tb_log_service                              jwBGEHLRTjutm7Jf3k3rJ4g  1    0    0            0            208b
green open      tb_log_edr_behavior_20240517                  wH45nYit0heK0NhuQ99s1Pg  5    0    0            0            1kb
green open      tb_edr_diagram_analysis                      75p1PuQUTS2u52Myu8JHzRA  2    0    0            0            416b
green open      tb_log_edr_network_info_20240519              5Umb_qr1TBey8JKAQJ3T9A   1    0    0            0            208b
green open      tb_log_edr_network_info_20240518              Y8G6R8gSYRO09p_ReyK10IA  1    0    0            0            208b
green open      tb_log_edr_inoutflow_20240518                 UAan7x-ZTN0Kxw0CesP4bw   1    0    0            0            208b
green open      tb_log_edr_inoutflow_20240519                 WfJ3-eS5TFqH0518XGemmQ   1    0    0            0            208b
green open      tb_v3_alert_log                             5vGMXzyG1x0h7QYrZaYTua   2    0    0            0            416b
green open      tb_log_os_event_20240517                      x31fElvDQJ-YUBEyP12I6A   5    0    0            0            1kb
green open      tb_log_audit_transaction                     h91F71xSRUMEURXSlyKw5A    1    0    0            0            208b
green open      tb_master_edr_inoutflow                       BG01Th9x1kyM57z5T5bHg    2    0    0            0            416b
green open      tb_log_timeline_20240517                      v9vci215e2uq-f4F3pYb4   5    0    0            0            1kb
green open      tb_log_timeline_20240519                      uXZLWRR4Q30kqfLFCV0BA    1    0    0            0            208b
green open      tb_log_timeline_20240518                      TTfQ3c4GSRelpkqy6ucZQ    1    0    0            0            208b

```

<IP 10.10.70.156 in the example image>

5-2) Node Configuration

- execute setting script

```
/opt/ahnlab/edr/bin/search-engine/edr_opensearch_cli.sh
```

Please select mode에서 [2.Manual OpenSearch nodes setting] mode 선택

→ mode > 2

→ How many OpenSearch servers are in total? : 1

→ Please enter the IP address of Server 1. : <EDRM IP>

```
[root@localhost ~]# /opt/ahnlab/edr/bin/search-engine/edr_opensearch_cli.sh
EDR OpenSearch manual mode started.
# Please select mode
* 1.OpenSearch Upgrade
* 2.Manual OpenSearch nodes setting
* 3.Manual OpenSearch index shard setting
* 4.Print OpenSearch Cluster info
-> mode > 2
-> How many OpenSearch servers are in total?(OpenSearch 서버는 총 몇대 인가요?) : 1
-> Please enter the IP address of Server 1.(서버 1의 ip를 입력하세요) : 10.10.70.156
```

- Memory configured automatically if choose [Auto] (auto cannot be used for EPP/EDR server on one server)

```
[root@localhost ~]# /opt/ahnlab/edr/bin/search-engine/edr_opensearch_cli.sh
EDR OpenSearch manual mode started.
# Please select mode
* 1.OpenSearch Upgrade
* 2.Manual OpenSearch nodes setting
* 3.Manual OpenSearch index shard setting
* 4.Print OpenSearch Cluster info
-> mode > 2
-> How many OpenSearch servers are in total?(OpenSearch 서버는 총 몇대 인가요?) : 1
-> Please enter the IP address of Server 1.(서버 1의 ip를 입력하세요) : 10.10.70.156
* Memory(GB) : 31
-> Choose opensearch node configuration type (Manual | Auto): auto
Total nodes info
Server 1 (ip: 10.10.70.156) heap memory per Nodes :
* master,data : 5GB
* master,data : 5GB
* master,data : 5GB
```

Check server Memory spec for auto

- If [Manual] master, data recommended memory

Memory	OpenSearch allocated memory	setting guide	EPP + EDR server
32GB	9~15GB	3 master, data - 5GB each	3 master, data - 2GB each
64GB	32GB	3 master - 4GB each 2 data - 10GB each	3 master, data - 5GB each
128GB	64GB	3 master - 8GB each 2 data - 20GB each	

256GB	128GB	3 master - 16GB each 4 data - 20GB each	
-------	-------	---	--

set OpenSearch master and data referring to the table above

- enter done' after finished entering

[example 1. memory 32GB]

```
# Configuring OpenSearch nodes for Server 1 started.(서버 1의 노드구성을 시작합니다)
[Node type]
1. master
2. coordinating
3. data
4. search
5. master,data

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 5
-> Please enter heap memory size(GB) for master,data node : 5

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 5
-> Please enter heap memory size(GB) for master,data node : 5

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 5
-> Please enter heap memory size(GB) for master,data node : 5

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : done
[Server 1 node]
master,data
master,data
master,data

-----Total nodes info-----
Server 1 (ip: 10.10.70.156) heap memory per Nodes :
* master,data : 5GB
* master,data : 5GB
* master,data : 5GB
```

[example 2. memory 64GB]

```

# Configuring OpenSearch nodes for Server 1 started.(서버 1 의 노드구성을 시작합니다)
[Node type]
1. master
2. coordinating
3. data
4. search
5. master,data

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 1
-> Please enter heap memory size(GB) for master node : 4

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 1
-> Please enter heap memory size(GB) for master node : 4

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 1
-> Please enter heap memory size(GB) for master node : 4

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 3
-> Please enter heap memory size(GB) for data node : 10

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : 3
-> Please enter heap memory size(GB) for data node : 10

-> Please enter number of node type , or 'done'(노드 타입 숫자 혹은 done 을 입력하세요) : done
[Server 1 node]
data
data
master
master
master

-----Total nodes info-----
Server 1 (ip: 10.10.70.156) heap memory per Nodes :
* data : 10GB
* data : 10GB
* master : 4GB
* master : 4GB
* master : 4GB

```

- Create OpenSearch User(ID) & PW (recommend to set user account instead of using default account)

Caution: ! / \$ / ` / " is not supported for password. (@#%^&*()) is ok

```

-> Please input OpenSearch user(id) : AhnlabEDR
-> Please input OpenSearch password :
-> Please input OpenSearch password again :

edr-manager service stopped.
OpenSearch services stopped.
OpenSearch storage dir removed.
edr-opensearch dir removed.
OpenSearch service file removed.
Making nodes dir done.
Making storage dir done.
edropensearch.properties has been initialized.
OpenSearch service file has been made.
cert subject in opensearch.yml has been modified.
opensearch.yml has been initialized.
opensearch.yml has been modified.
chown done. []
chown done. []
OpenSearch services restarted.
Creating index templates...
edr-manager started. []
[root@localhost ~]#

```


5-3) Check manually configured node

- 25 Templates (Enter OpenSearch User account set from above)

```
[root@localhost ~]# curl -X GET "https://10.10.70.156:8961/_cat/templates" -u "AhnlabEDR:" --insecure
```

template tbedr_diagram_relation	[tbedr_diagram_relation]	0	[common_settings_and_analyzer]
template tb_log_server_resource	[tb_log_server_resource]	0	[common_settings_and_analyzer]
template tb_log_audit_transaction	[tb_log_audit_transaction]	0	[common_settings_and_analyzer]
template tb_log_edr_network_info	[tb_log_edr_network_info*]	0	[common_settings_and_analyzer]
template tb_log_service	[tb_log_service]	0	[common_settings_and_analyzer]
template tb_master_edr_inoutflow	[tb_master_edr_inoutflow]	0	[common_settings_and_analyzer]
template tb_log_audit_exception	[tb_log_audit_exception]	0	[common_settings_and_analyzer]
template tbedr_incident	[tbedr_incident]	0	[common_settings_and_analyzer]
template tbedr_diagram_analysis	[tbedr_diagram_analysis]	0	[common_settings_and_analyzer]
template tb_log_immediate_task	[tb_log_immediate_task]	0	[common_settings_and_analyzer]
template tb_log_edr_evidence	[tb_log_edr_evidence*]	0	[common_settings_and_analyzer]
template tb_history_system	[tb_history_system]	0	[common_settings_and_analyzer]
template tb_log_edr_behavior	[tb_log_edr_behavior*]	0	[common_settings_and_analyzer]
template tb_log_process_block	[tb_log_process_block]	0	[common_settings_and_analyzer]
template tb_log_audit	[tb_log_audit]	0	[common_settings_and_analyzer]
template tb_log_os_event	[tb_log_os_event*]	0	[common_settings_and_analyzer]
template tb_log_edr_powershell	[tb_log_edr_powershell*]	0	[common_settings_and_analyzer]
template tbedr_diagram	[tbedr_diagram]	0	[common_settings_and_analyzer]
template tb_log_timeline	[tb_log_timeline*]	0	[common_settings_and_analyzer]
template tb_log_engine_update	[tb_log_engine_update]	0	[common_settings_and_analyzer]
template tb_v3.alert_log	[tb_v3.alert_log]	0	[common_settings_and_analyzer]
template tb_log_backup	[tb_log_backup]	0	[common_settings_and_analyzer]
template tb_log_edr_inoutflow	[tb_log_edr_inoutflow*]	0	[common_settings_and_analyzer]
template tbedr_diagram_item	[tbedr_diagram_item]	0	[common_settings_and_analyzer]
template tbedr_incident_confirm_state_history	[tbedr_incident_confirm_state_history]	0	[common_settings_and_analyzer]

```
[root@localhost ~]#
```

- check Node(Memory 32GB example)

```
[root@localhost ~]# curl -X GET "https://10.10.70.156:8961/_cat/nodes?v" -u "AhnlabEDR:" --insecure
```

ip	heap.percent	ram.percent	cpu	load_1m	load_5m	load_15m	node.role	node.roles	cluster_manager	name
10.10.70.156	13	66	36	2.38	4.04	3.52	dm	data,master *		master-data-1
10.10.70.156	19	66	36	2.38	4.04	3.52	dm	data,master -		master-data-2
10.10.70.156	12	66	36	2.38	4.04	3.52	dm	data,master -		master-data-3

```
[root@localhost ~]#
```

- reset integrity

```
[root@localhost ~]# /opt/ahnlab/edr/bin/edr_integrity.sh INIT
Setting environments
/opt/ahnlab/edr/lib/edr-tools.jar:/opt/ahnlab/edr/lib
SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder".
SLF4J: Defaulting to no-operation (NOP) logger implementation
SLF4J: See http://www.slf4j.org/codes.html#StaticLoggerBinder for further details.
```

'N`ä[[[![[[[_M_]"Z^x_"81[~p%t_î_&ψ_m#_b

L+t""-8s?`-

N_.Elv3V(h--yg_#H5^®3r_0_n_0\$ _°q_Q_l>mCAZ(<3=x_q_3>:_!b

'N`ä[<+_I"3_"81[~p%t_î_&ψ

```
-bash: PuTTYPuTTYPuTTYPuTTYPuTTY: command not found
[root@localhost ~]#
```

SLF4J : Failed is a normal process

6. Add Domain and Apply Role

- [EDRM] Registering Domain

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

[EDRA] Guide to Install/Delete EDR Agent for Linux

[EDRM] EDRM Installation Guide

[EDRM] Preparing for Installation

[EDRM] Specification (Requirements)

[EPPM] EPPM Installation Guide

Related articles

[EPPM] [EPPM] OS Package Installation Guide (version 1.0.12.30 or later)

Comments

0 comments



Be the first to write a comment.

English (US)
