viettel
security

Viettel Endpoint Detection & Response (VCS-aJiant)

Phiên bản 3.3.0 EPP – Năm 2021

Ngày cập nhật: 31/12/2021

Tài liệu Hướng dẫn Triển khai Cài đặt (Installation Guide)

Mục lục

Thuật ngữ

Viết tắt	Diễn giải	Ghi chú
VCS	Viettel Cyber Security	Công ty An ninh mạng Viettel
VCS-aJiant	Tên giải pháp Endpoint Detection & Response do Công ty An ninh mạng viettel phát triển	
EDR	Endpoint Detection & Response	Tên 1 dòng sản phẩm giám sát phát hiện và phản ứng với các bất thường phía Endpoint
HA	High Availability	Tính sẵn sàng cao

1. GIỚI THIỆU

1.1. Thực trạng hiện nay

Ngày nay, các tổ chức, doanh nghiệp tiếp tục gặp rất nhiều khó khăn với việc phát hiện, xác định, điều tra và giảm thiểu các dạng phần mềm độc hại tiên tiến trong hệ thống. Các công nghệ phòng chống mã độc truyền thống như Anti Virus dựa trên chữ ký đang bị vượt qua một cách cố ý bởi những kẻ tấn công chuyên nghiệp có trình độ cao với các bộ công cụ tấn công, phần mềm độc hại được tùy chỉnh và hướng mục tiêu cụ thể. Nhiều tổ chức đã thừa nhận rằng các phương pháp phòng thủ chống phần mềm độc hại truyền thống của họ đã thất bại và một chiến lược mới phải được tạo ra để xác định những vi phạm này tại endpoint. Một số lượng đáng kể các vi phạm dữ liệu gần đây từ các dạng phần mềm độc hại nâng cao đã làm tăng sự quan tâm của khách hàng đối với các Giải pháp phát hiện và phản ứng cho lớp endpoint (EDR) mà VCS-aJiant là một trong số đó.

1.2. Sự phát triển của công nghệ

Công nghệ của Giải pháp VCS-aJiant giúp bù đắp các thiếu sót của các công nghệ dựa trên chữ ký mà các tổ chức đang sử dụng như Anti Virus hay IPS/IDS để cung cấp khả năng phát hiện bất thường dựa trên hành vi và cho cái nhìn sâu hơn về các thông tin cụ thể có liên quan trên endpoint để phát hiện và giảm thiểu các mối đe dọa nâng cao.

1.3. VCS-aJiant

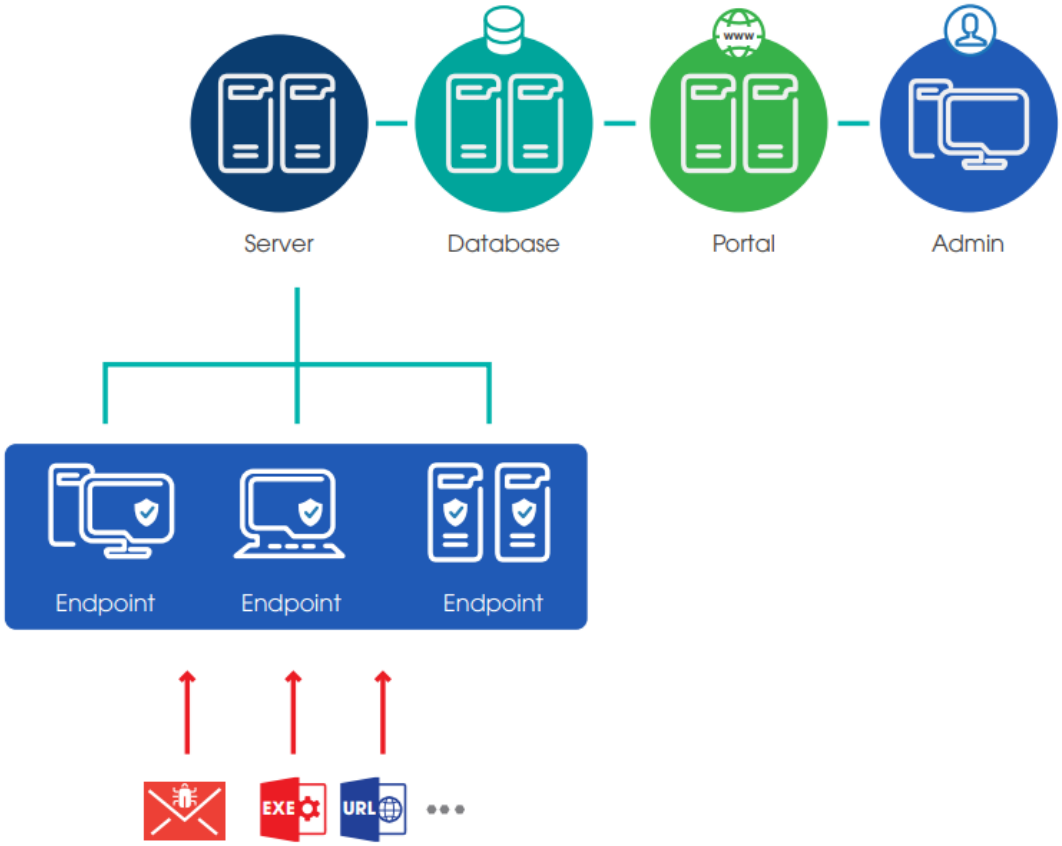
VCS-aJiant có khả năng cung cấp thông tin chi tiết về việc lây nhiễm phần mềm độc hại và các hành vi mở rộng phạm vi tấn công (lateral movement) của những kẻ tấn công khi chúng thực hiện việc dò quét hoặc sử dụng thông tin bị đánh cắp trong mạng nội bộ đối với các hệ thống và ứng dụng.

Ngoài ra, VCS-aJiant cũng bổ sung cho các công nghệ bảo mật hiện có như giải pháp quản lý sự kiện và thông tin bảo mật (SIEM), các công cụ giám định mạng (Network Forensics) và các thiết bị phòng chống mối đe dọa tiên tiến (Advanced Threat Detection), đồng nghĩa là bổ sung vào danh mục các giải pháp phản ứng sự cố an toàn thông tin của tổ chức.

2. TỔNG QUAN

2.1. Kiến trúc hạ tầng

Mô hình triển khai VCS-aJiant như sau:



Các thành phần của hệ thống bao gồm:

- **Endpoint**: Là thành phần được cài đặt trên từng máy tính, có nhiệm vụ giám sát các dấu hiệu bất thường trên máy tính, gửi log về server tập trung. Các thông tin giám sát bao gồm các hành vi liên quan đến File, Process, Memory, Registry, Network trên máy tính người dùng và server.
- **Cụm server xử lý tập trung và lưu trữ**: Là thành phần xử lý dữ liệu do Endpoint gửi về, đóng vai trò chính trong việc phân tích và xử lý dữ liệu theo thời gian thực.
- **Thành phần Web Portal**: Là thành phần mà người quản trị sẽ sử dụng để điều tra, giám sát và phân tích các thông tin của hệ thống, phản ứng khi có cảnh báo bất thường tại các agents

2.2. Công nghệ được sử dụng

VCS-aJiant sử dụng cộng nghệ Filter Driver (cho phép chạy và theo dõi ở mức Kernel-based) thu thập các thông tin bao gồm File, Process, Registry, Network trên máy tính người dùng và server. Các dấu hiệu về file bao gồm (modified, delete, changed attribute), về registry (delete key/value, set value, rename key/value, create key với access nghi ngờ. Các dấu hiệu nghi ngờ về Memory được định kì quét rà soát liên tục. Các hành vi được xác định là nghi ngờ được đẩy về hệ thống Back-end phân tích tập trung.

Luồng nghiệp vụ điều tra tấn công được thiết kế khép kín theo kịch bản incident response (IR Flow), hỗ trợ phát hiện và phân tích các dấu hiện bất thường ngay trên một giao diện duy nhất. Cung cấp các chức năng điều tra (Forensic) sâu trên Endpoint. Hỗ trợ lấy file nghi ngờ (Get Artifact), đẩy công cụ rà quét (Tool Deployment), cho phép thực hiện điều tra, cung cấp bằng chứng theo thời gian thực (Process Analysis, Live Response), cho phép thực hiện phản ứng khi phát hiện mối đe dọa.

Ngay khi xác minh được bất thường, Endpoint cung cấp các công cụ gỡ bỏ mã độc trên diện rộng (Response Scenario) bao gồm: cô lập mạng máy bị nhiễm (network containment), kill process, delete file/registry.

3. HƯỚNG DẪN CÀI ĐẶT BACKEND

3.1. Điều kiện đảm bảo cài đặt

- Cấu hình IP:
  - cấu hình 1 IP tĩnh cho node server.
- Mở kết nối đến server qua các port sau:

Mục đích	Port	Protocol
Agent kết nối server	4443, 5672, 8443, 8888	TCP
Truy cập Portal	80, 443	TCP

- Mở kết nối từ server tới các địa chỉ sau ngoài Internet:

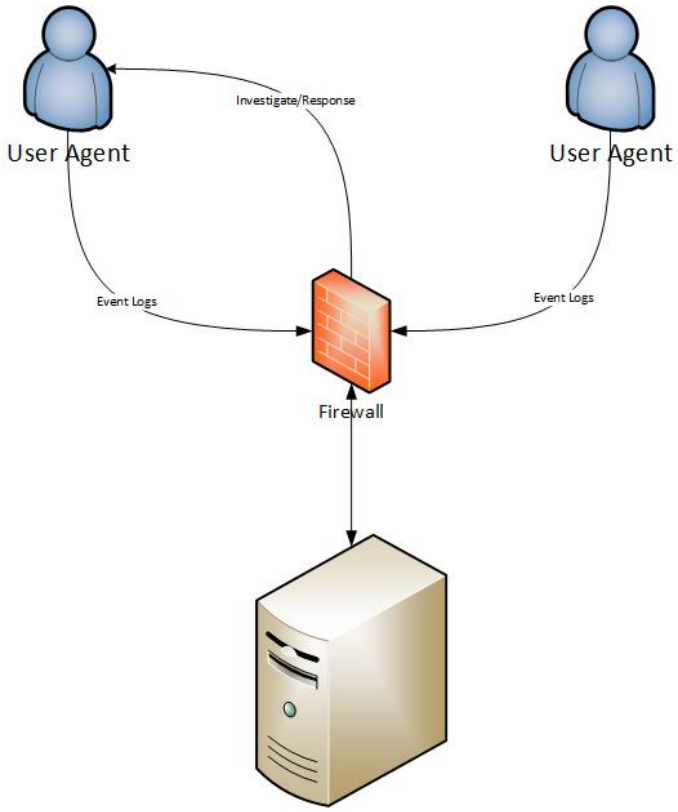
Mục đích	Address & Port	Protocol
Server định kỳ update AV database	hub.viettelcybersecurity.com:443 notary.viettelcybersecurity.com:443	TCP

- Server cần bật tính năng ảo hoá Intel VT-x/AMD-V để chạy máy ảo build bộ cài agent Windows.

3.2. Topo của khách hàng

3.2.1. AllInOne Topo

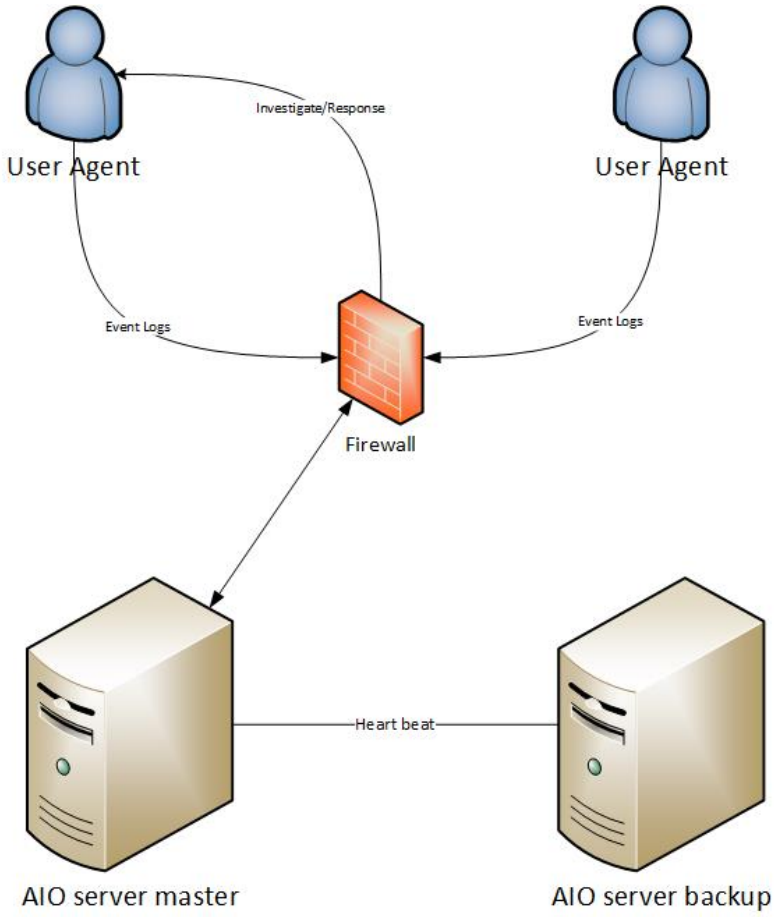
Với mô hình triển khai AllInOne, tất cả các dịch vụ backend VCS-aJiant được triển khai trên 1 node server duy nhất.



Hình 1. Mô hình triển khai backend VCS-aJiant AllInOne

3.2.2. HA Topo

Với các khách hàng yêu cầu có HA, thì sử dụng mô hình gồm 2 node AllInOne, trong đó có 1 node chạy chính và 1 node dự phòng. Database của 2 node được đồng bộ với nhau.



Hình 2. Mô hình triển khai VCS-aJiant AllInOne có HA

3.3. Định cỡ tài nguyên (Sizing)

Tùy theo số lượng agents cần triển khai, lượng tài nguyên cần thiết như sau:

3.3.1. Cấu hình server tiêu chuẩn

Cấu hình mỗi server vật lý thông thường chia thành các loại sau:

- Loại 1:
  - CPU: 24 core vật lý
  - RAM: 128 GB
- Loại 2:
  - CPU: 12 core vật lý
  - RAM: 64 GB
- Loại 3:
  - CPU: 8 core vật lý
  - RAM: 32 GB
- Loại 4:

- CPU: 4 core vật lý
- RAM: 16 GB

3.3.2. Sizing tài nguyên CPU và RAM theo số agents

Số agents	Không có HA		Có HA	
	Số server vật lý	Loại server	Số server vật lý	Loại server
0 → 200	1	4	2	4
200 → 5k	1	3	2	3
5k → 20k	1	2	2	2
20k → 50k	1	1	2	1

3.3.3. Sizing dung lượng ổ cứng theo số agents

Yêu cầu hiệu năng ổ cứng tối thiểu như sau:

Thông số	Giá trị yêu cầu	Cách kiểm tra
Tốc độ đọc	>= 200 MB/s	Chạy lệnh sau trên node cần kiểm tra (xem *buffered disk reads*): $ sudo hdparm -Tt /dev/sda
Tốc độ ghi	>= 100 MB/s	Chạy lệnh sau trên node cần kiểm tra: $ sudo dd if=/dev/sda of=largefile bs=1M count=200
Độ trễ ổ cứng	< 1 ms	Cài thêm gói ioping để kiểm tra độ trễ ổ cứng: $ apt update && apt install -y ioping Chạy lệnh sau trên node cần kiểm tra: $ ioping -c 10 .
IOPS	read: iops >= 500 write: iops >= 200	Cài thêm gói fio để kiểm tra IOPS ổ cứng: $ apt update && apt install -y fio Chạy lệnh sau trên node cần kiểm tra: $ fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1 --name=tempfile --filename=tempfile --bs=4k --iodepth=64 --size=4G --readwrite=randrw --rwmixread=75

Dung lượng ổ cứng theo số agents triển khai

Số lượng agents	Tổng dung lượng HDD chia đều các server vật lý (cài VM và lưu log 1 năm)	
	Không có HA dữ liệu	Có HA dữ liệu (1 bản sao dữ liệu)

0 → 50	160 GB	
50 → 200	250 GB	
200 → 500	300 GB	600 GB
500 → 2k	500 GB	1 TB
2k → 5k	700 GB	1.4 TB
5k → 10k	1 TB	2 TB
10k → 20k	1.5 TB	3 TB
20k → 25k	2 TB	4 TB
25k → 30k	3 TB	6 TB
30k → 40k	4 TB	8 TB

3.4. Bảng thông tin phiên bản hỗ trợ nâng cấp

Thông tin về phiên bản hỗ trợ nâng cấp được mô tả trong bảng sau đây:

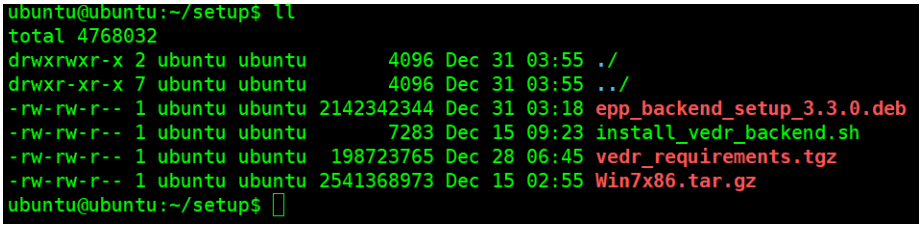
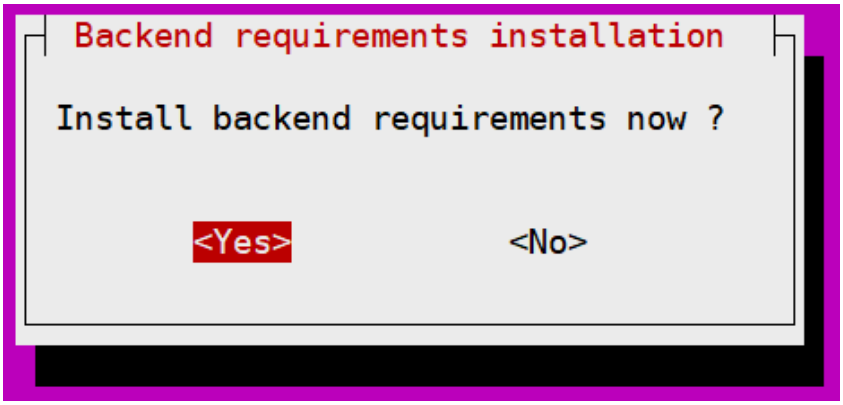
		Version muốn nâng cấp		
		3.3.0 EDP	**3.3.0 EDR**	**3.3.0 EPP**
Version hiện tại	**3.1.0 EDR**	✓	✓	X
	3.3.0 EPP	✓	✓	
	3.3.0 EDR	✓		X
	3.3.0 EDP		X	X

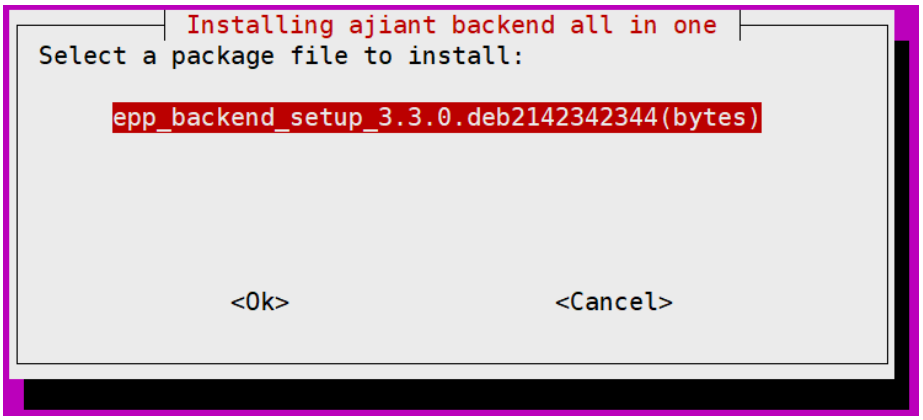
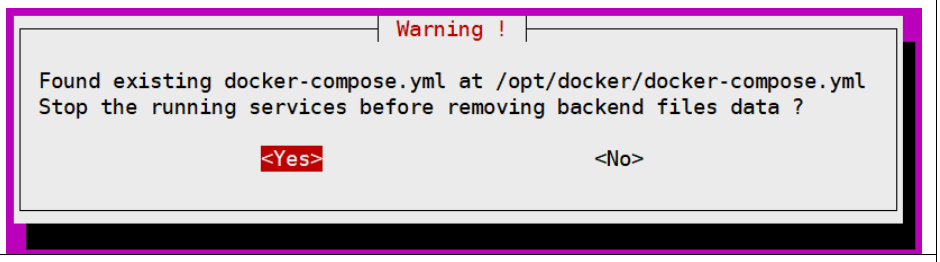
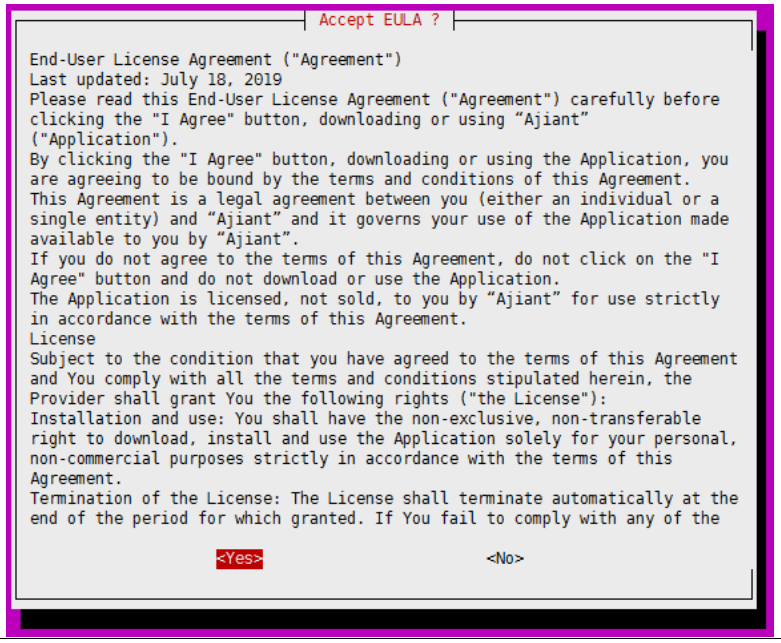
3.5. Các bước cài đặt backend

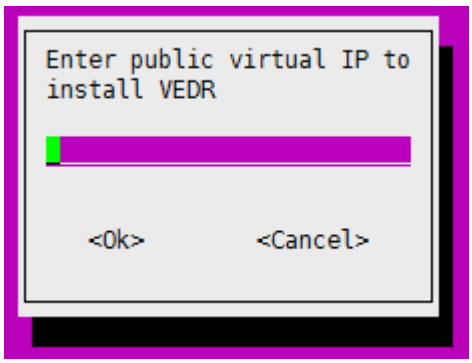
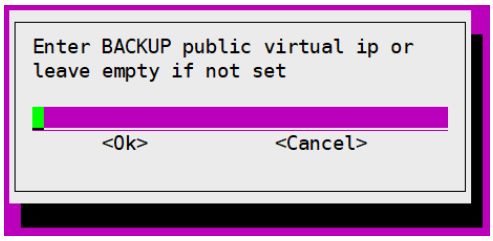
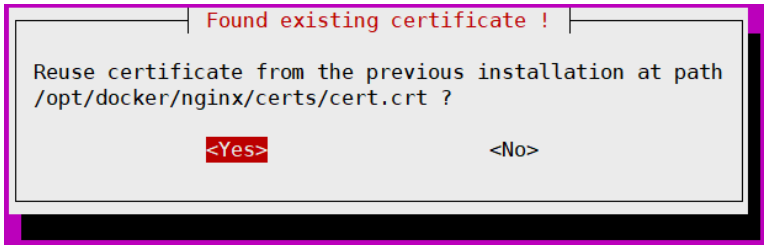
Chú ý: Trước khi cài đặt backend nên quy hoạch sử dụng tên miền cho hệ thống tập trung thay vì sử dụng IP để đơn giản cho quá trình đổi server có thể phát sinh sau giai đoạn triển khai.

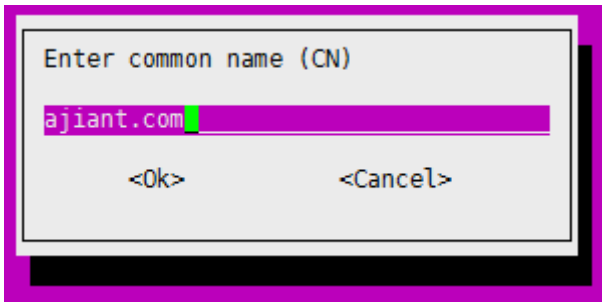
3.5.1. Cài đặt backend AllInOne version 3.3.0

Bước	Tên	Thực hiện
1	Cài hệ điều hành server	Cài đặt 1 node server Ubuntu Server 20.04.3 x64
2	Đồng bộ thời gian cho server	Chỉnh đúng thời gian và múi giờ cho server, khuyến nghị cấu hình NTP để đồng bộ thời gian cho server.

		Chú ý: thời gian server không đúng có thể gây ra lỗi license, timestamp event log, timestamp alert…
3	Chạy script cài đặt	Copy các file sau lên server và đặt cùng 1 thư mục: - install_vedr_backend.sh - vedr_requirement.tgz - Win7x86.tar.gz - epp_backend_setup_3.3.0.deb  Vào thư mục chứa 4 file ở trên, chạy script: $ sudo bash install_vedr_backend.sh
4	Cài đặt các gói cần thiết	Cài các gói cần thiết cho server (chọn Yes) hoặc skip (chọn No). Việc cài đặt các gói cần thiết sẽ diễn ra tự động sau đó. **Chú ý:** cài gói offline chỉ thành công với phiên bản Ubuntu Server x64 20.04.3 trở lên. Các phiên bản Ubuntu thấp hơn đều có thể gây lỗi.  Sau khi cài đặt các gói cần thiết, nếu trong thư mục đã có sẵn file cài đặt vedr_backend_setup_3.3.0.deb thì sẽ được hiện ra trong danh sách file muốn cài đặt.

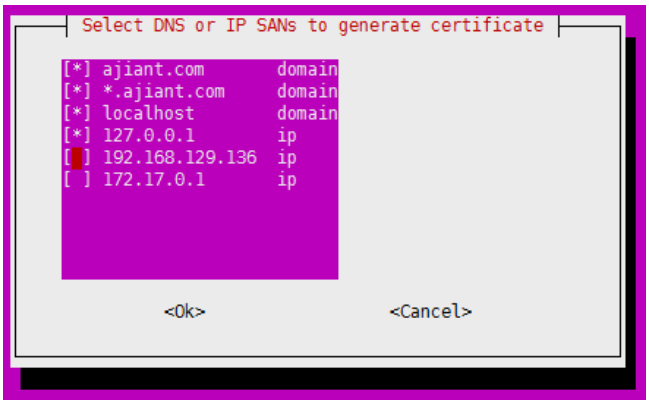
		 Lựa chọn đúng file muốn cài và chọn OK hoặc ấn Enter để tiếp tục. Nếu phát hiện có phiên bản VEDR được cài trước đó, cần xác nhận có dừng tất cả dịch vụ lại trước khi cài bản mới không (chọn Yes) 
5	Đồng ý với điều khoản sử dụng (EULA)	Khi được hỏi chấp nhận điều khoản sử dụng (**EULA**), chọn **Yes** để tiếp tục cài đặt, chọn **No** nếu không chấp nhận và thoát cài đặt. 

6	Nhập địa chỉ của server	Sau khi bộ cài DEB được unpack ra **/opt/docker**, sẽ đến phần cấu hình cài đặt VEDR Backend.   Nhập địa chỉ theo dạng tên miền hoặc public ip đã được quy hoạch để các agent kết nối đến server, nếu không sử dụng địa chỉ backup thì bỏ trống. Chú ý: nên quy hoạch sử dụng tên miền thay cho IP để đơn giản cho quá trình đổi server có thể phát sinh sau giai đoạn triển khai.
7	Khởi tạo chứng thư (certificate) cho hệ thống	Nếu quá trình cài đặt phát hiện chứng thư cũ đã tồn tại khi nâng cấp backend - Chọn Yes nếu muốn dùng chứng thư cũ - Chọn No nếu muốn thiết lập lại chứng thư mới  Nếu cài mới thì đến luôn màn tạo mới chứng thư. Trong màn hình tiếp theo (trường hợp tạo mới chứng thư) Nhập CommonName (nhập tên miền hoặc public ip của server). Mặc định là **ajiant.com**. Có thể nhập tên miền mà agent kết nối lên server vào CommonName.

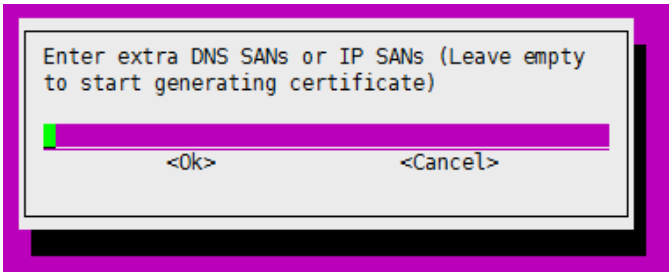


Nhập DNS SANs và IP SANs từ danh sách tùy chọn.

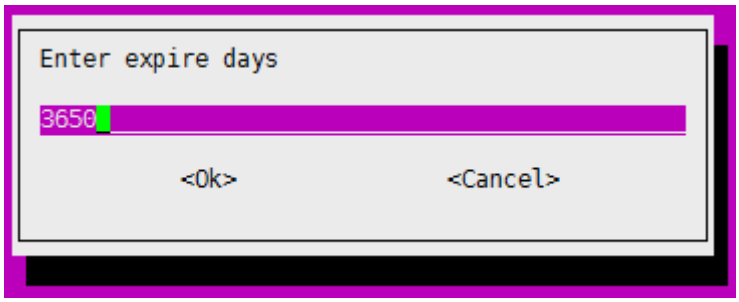
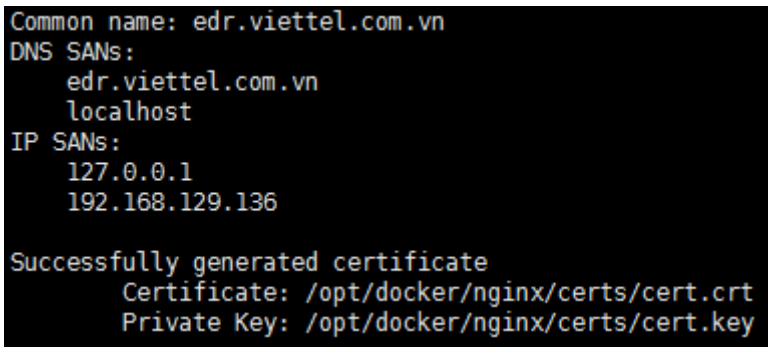
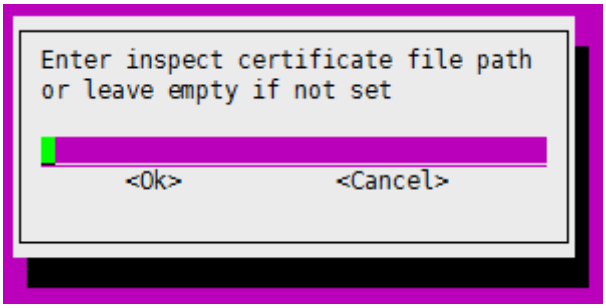
Chú ý: trong danh sách IP SANs phải có tên miền hoặc public ip để agent có thể kết nối đến server.

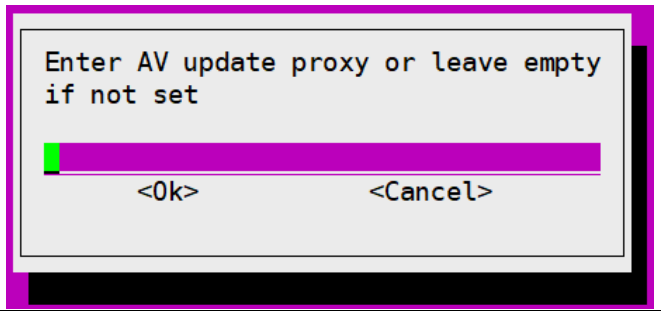
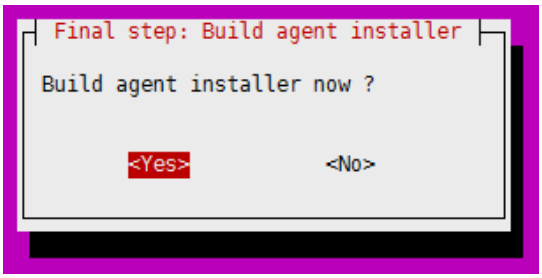
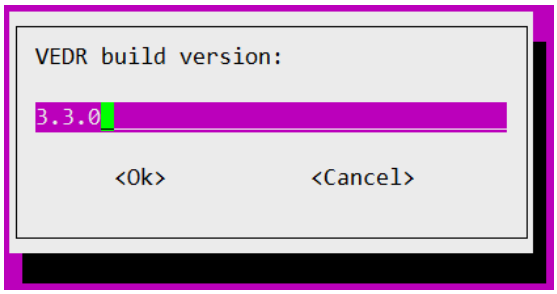


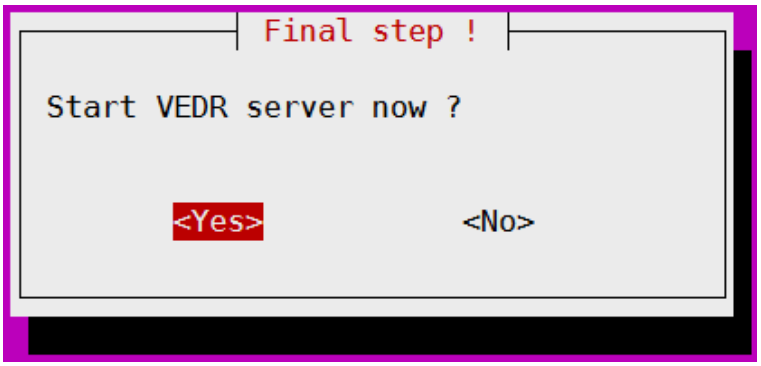
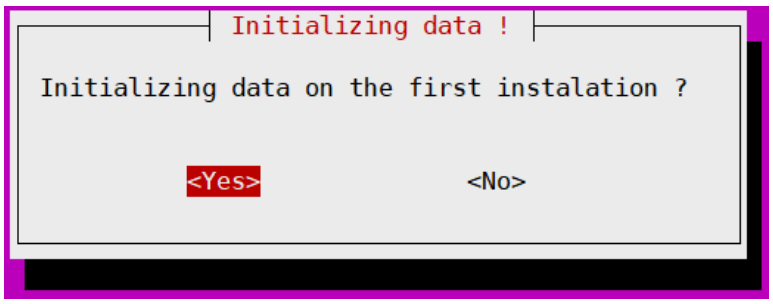
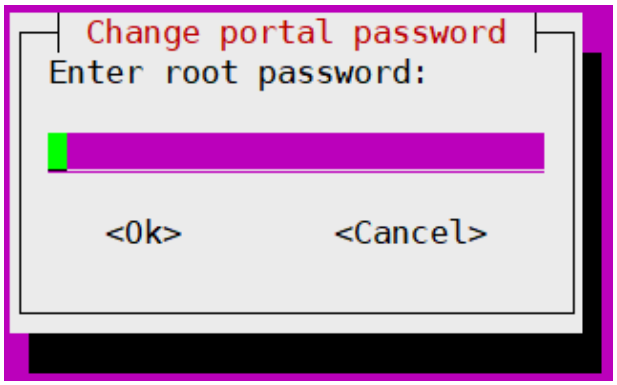
Nếu agent kết nối qua tên miền thì nhập tên miền vào ô DNS SANs.

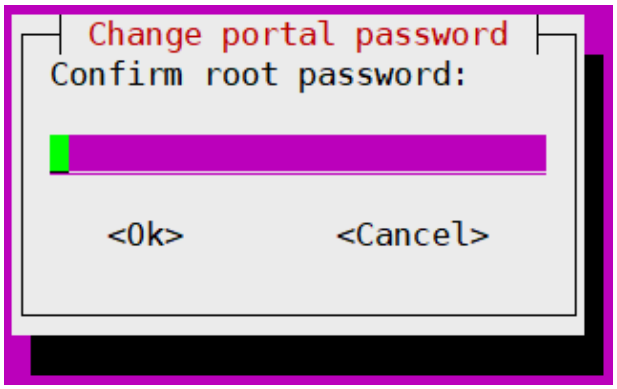
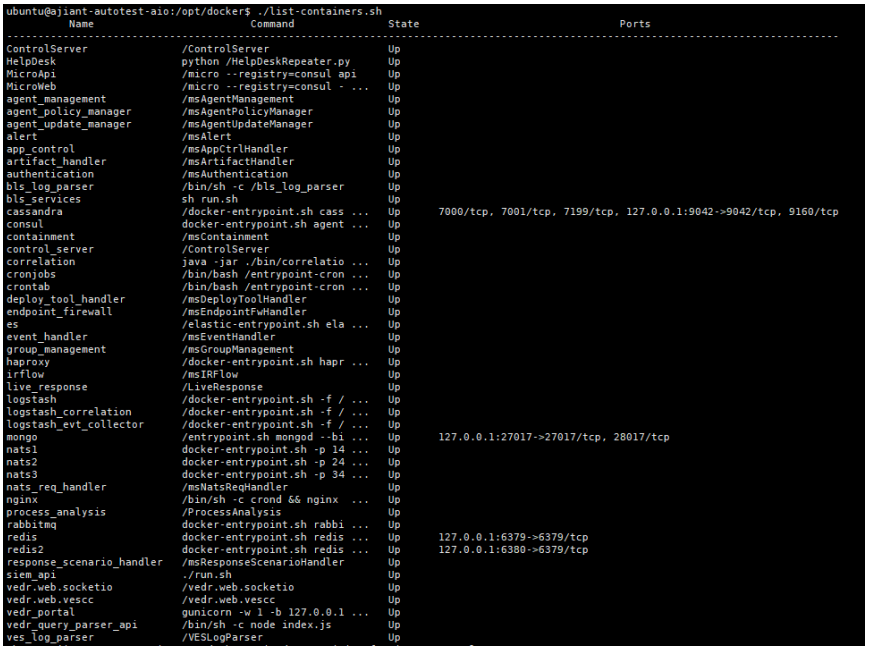


Nhập thời gian hết hạn chứng thư theo ngày (mặc định là 3650):

		 Kết quả sẽ sinh 2 file trong thư mục: /opt/docker/nginx/certs/ - cert.crt - cert.key 
8	Nhập đường dẫn cert inspect	 Nếu không dùng cert inspect để rỗng và enter bỏ qua bước này. Nếu có dùng cert inspect thì nhập đường dẫn cert inspect. Chọn OK. Script sẽ copy file cert_insp vào: /opt/docker/config/cert_insp.crt
9	Nhập địa chỉ proxy nội bộ để server update AV database	Nhập địa chỉ proxy nội bộ để server định kỳ update AV database từ hệ thống AV repo. Nếu server có thể kết nối trực tiếp tới hệ thống AV repo của VCS thì bỏ trống.

		
10	Tạo bộ cài đặt agent	Khi được xác nhận tạo bộ cài agent không, chọn Yes để tiếp tục.  Nhập phiên bản bộ cài agent hoặc ấn Enter để lấy phiên bản mặc định tự sinh  Chờ khoảng 10 phút để server build bộ cài agent (***build agent windows có thể đến 5 phút 1 lần build do phải khởi động máy ảo vbox***) Nếu quá trình cài đặt thành công, server sẽ sinh ra 2 file MSI cho windows trong thư mục: **/opt/docker/repo/public/** - ajiant_windows_3.3.0_x64_full.msi - ajiant_windows_3.3.0_x86_full.msi

11	Khởi động server vedr backend	 Chọn ‘y’ hoặc ‘enter’ để khởi động ngay vedr backend hoặc chọn ‘n’ để khởi động sau. Nếu chọn “n”, để khởi động VEDR backend sau đó thì chạy lệnh sau: $ sudo bash /opt/docker/start_vedr.sh
12	Khởi tạo dữ liệu database	 Khi được hỏi có khởi tạo dữ liệu không thì chọn Yes để thực hiện khởi tạo (kể cả cài mới và nâng cấp). Bước tiếp theo là đặt password cho user root, có thể ấn Enter để bỏ qua nếu muốn user root giữ mật khẩu cũ.  Xác nhận password đã nhập

		 Nếu thành công thì password mới sẽ được thiết lập cho user root.
13	Kiểm tra lại các dịch vụ đang chạy, các port kết nối	Khi khởi động thành công, chạy script sau để kiểm tra các dịch vụ: $ cd /opt/docker $ sudo docker-compose ps Hoặc $ cd /opt/docker $ ./list-containers.sh Nếu tất cả các service ở trạng thái “UP” là OK.  Kiểm tra các port dịch vụ: $ telnet <PUBLIC_IP> 8888

```
ubuntu@ajiant-autotest-aio:/opt/docker$ ./list-containers.sh
          Name                        Command               State                                                  Ports
-------------------------------------------------------------------------------------------------------------------------------------------
ControlServer              /ControlServer                   Up
HelpDesk                   python /HelpDeskRepeater.py      Up
MicroApi                   /micro --registry=consul api     Up
MicroWeb                   /micro --registry=consul - ...   Up
agent_management           /msAgentManagement               Up
agent_policy_manager       /msAgentPolicyManager            Up
agent_update_manager       /msAgentUpdateManager            Up
alert                      /msAlert                         Up
app_control                /msAppCtrlHandler                Up
artifact_handler           /msArtifactHandler               Up
authentication             /msAuthentication                Up
bls_log_parser             /bin/sh -c /bls_log_parser       Up
bls_services               sh run.sh                        Up
cassandra                  /docker-entrypoint.sh cass ...   Up      7000/tcp, 7001/tcp, 7199/tcp, 127.0.0.1:9042->9042/tcp, 9160/tcp
consul                     docker-entrypoint.sh agent ...   Up
containment                /msContainment                   Up
control_server             /ControlServer                   Up
correlation                java -jar ./bin/correlatio ...   Up
cronjobs                   /bin/bash /entrypoint-cron ...   Up
crontab                    /bin/bash /entrypoint-cron ...   Up
deploy_tool_handler        /msDeployToolHandler             Up
endpoint_firewall          /msEndpointFwHandler             Up
es                         /elastic-entrypoint.sh ela ...   Up
event_handler              /msEventHandler                  Up
group_management           /msGroupManagement               Up
haproxy                    /docker-entrypoint.sh hapr ...   Up
irflow                     /msIRFlow                        Up
live_response              /LiveResponse                    Up
logstash                   /docker-entrypoint.sh -f / ...   Up
logstash_correlation       /docker-entrypoint.sh -f / ...   Up
logstash_evt_collector     /docker-entrypoint.sh -f / ...   Up
mongo                      /entrypoint.sh mongod --bi ...   Up      127.0.0.1:27017->27017/tcp, 28017/tcp
nats1                      docker-entrypoint.sh -p 14 ...   Up
nats2                      docker-entrypoint.sh -p 24 ...   Up
nats3                      docker-entrypoint.sh -p 34 ...   Up
nats_req_handler           /msNatsReqHandler                Up
nginx                      /bin/sh -c crond && nginx  ...   Up
process_analysis           /ProcessAnalysis                 Up
rabbitmq                   docker-entrypoint.sh rabbi ...   Up
redis                      docker-entrypoint.sh redis ...   Up      127.0.0.1:6379->6379/tcp
redis2                     docker-entrypoint.sh redis ...   Up      127.0.0.1:6380->6379/tcp
response_scenario_handler  /msResponseScenarioHandler       Up
siem_api                   ./run.sh                         Up
vedr.web.socketio          /vedr.web.socketio               Up
vedr.web.vescc             /vedr.web.vescc                  Up
vedr_portal                gunicorn -w 1 -b 127.0.0.1 ...   Up
vedr_query_parser_api      /bin/sh -c node index.js         Up
ves_log_parser             /VESLogParser                    Up
```

		$ telnet <PUBLIC_IP> 5672 $ telnet <PUBLIC_IP> 80 $ telnet <PUBLIC_IP> 443 $ telnet <PUBLIC_IP> 4443 $ telnet <PUBLIC_IP> 8443

3.5.2. Cấu hình HA cho backend AllInOne

Với khách hàng cài đặt backend AllInOne và có yêu cầu HA thì trước hết cần cài đặt 2 node backend AllInOne. Sau đó thực hiện cấu hình HA theo các bước sau:

STT	Công việc	Thực hiện
1	Cài đặt các gói haproxy & keepalived	Copy file haproxy-keepalived.tgz vào 2 node Giải nén bộ file cài đặt: $ tar -zxf haproxy-keepalived.tgz Kết quả giải nén ra thư mục **haproxy-keepalived** Cài đặt các gói DEB: $ sudo dpkg -i haproxy-keepalived/$(lsb_release -s -c)/*.deb Có thể chạy gộp 2 lệnh trên thành 1 lệnh duy nhất: $ tar -zxf haproxy-keepalived.tgz && sudo dpkg -i haproxy-keepalived/$(lsb_release -s -c)/*.deb
2	Cấu hình keepalived	Quy hoạch 01 địa chỉ virtual ip (VIP) cùng dải với ip 2 node AllInOne Cấu hình keepalived trên 2 node, tạo file **/etc/keepalived/keepalived.conf** với nội dung trên 2 node như sau: Node 1: global_defs { router_id lb1 } vrrp_script chk_haproxy { script "killall -0 haproxy" interval 2 weight 2 } vrrp_instance VI_1 {

```
        virtual_router_id 51
        advert_int 1
        priority 100
        state MASTER
        interface <net interface, vd: ens160/eth0>
        virtual_ipaddress {
            <VIP> dev <net interface, vd: ens160/eth0>
        }
        authentication {
            auth_type PASS
            auth_pass 123456
        }
        track_script {
            chk_haproxy
        }
}
```

Node 2:

```
global_defs {
        router_id lb2
}
vrrp_script chk_haproxy {
        script "killall -0 haproxy"
        interval 2
        weight 2
}
vrrp_instance VI_1 {
        virtual_router_id 51
        advert_int 1
        priority 99
        state MASTER
        interface <net interface, vd: ens160/eth0>
```

		virtual_ipaddress { <VIP> dev <net interface, vd: ens160/eth0> } authentication { auth_type PASS auth_pass 123456 } track_script { chk_haproxy } } Khởi động dịch vụ keepalived: $ sudo service keepalived start Kiểm tra lại virtual ip đã được gắn vào node 1 chưa: $ ip a Kiểm tra VIP xuất hiện cùng ip chính không. Kiểm tra dịch vụ qua VIP: $ ping <VIP> $ telnet <VIP> 443
3	Cấu hình cluster cho cassandra	Mở file /opt/docker/docker-compose.yml Sửa cấu hình service Cassandra trên 2 node: + Network_mode: host + CASSANDRA_BROADCAST_ADDRESS=<ip node hiện tại> + CASSANDRA_RACK=<2 node nhập giá trị khác nhau, vd: rack1,rack2> + CASSANDRA_SEEDS=<danh sách ip của clusters, gồm cả ip 2 node>

		`` cassandra: image: cassandra restart: always container_name: cassandra network_mode: host # user: 1000:1000 ports: - 9042:9042 - 8778:8778 environment: - CASSANDRA_CLUSTER_NAME=EDR - MAX_HEAP_SIZE=500M - HEAP_NEWSIZE=500M - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_ENDPOINT_SNITCH=GossipingPropertyFileSnitch - CASSANDRA_DC=dc1 - CASSANDRA_RACK=rack1 - CASSANDRA_SEEDS=10.0.0.131,10.0.0.132 - CASSANDRA_AUTO_BOOTSTRAP=false volumes: - ./data:/var/lib/cassandra - ./log:/var/log/cassandra - ./java:/usr/share/java ``` Khởi động lại Cassandra trên 2 node: $ cd /opt/docker/ $ docker-compose up -d cassandra Kiểm tra lại trạng thái cluster Cassandra: $ /opt/docker/cacssandra/nodetool.sh status Nếu hiện 2 node ở trạng thái UP (**UN**) là OK ``` edr@EDR-Cassandra1:/opt/docker$ /opt/docker/cassandra/nodetool.sh status Datacenter: dc1 ========== Status=Up/Down |/ State=Normal/Leaving/Joining/Moving -- Address Load Tokens Owns Host ID Rack UN 10.0.0.131 5.5 MiB 256 ? 86725091-29f7-4392-ade1-764014bc36b7 rack1 UN 10.0.0.132 7.19 MiB 256 ? 2f9527ee-1cb9-4e06-87fd-12fb89bc97a9 rack2 ```
4	Cấu hình cluster cho elasticsearch	Mở file /opt/docker/elasticsearch/elasticsearch.yml Sửa các cấu hình như sau: + network.host: 0.0.0.0 + discovery.zen.ping.unicast.hosts: ["<ip node 1>", “<ip node 2>”]

		<pre>cluster.name: "ES-EDR" node.name: ES network.host: 0.0.0.0 http.cors.enabled: true http.cors.allow-origin: "*" discovery.zen.ping.unicast.hosts: ["10.0.0.121", "10.0.0.122"] discovery.zen.minimum_master_nodes: 1</pre> Restart lại elasticsearch trên 2 node: $ cd /opt/docker/ $ ./restart-containers.sh elasticsearch Chờ để elasticsearch khởi động xong, kiểm tra lại trạng thái cluster: $ curl http://127.0.0.1:9200/_cluster/health?pretty Nếu thấy status=yellow hoặc green và number_of_data_nodes=2 là OK
5	Cấu hình đồng bộ repo từ node chính sang node dự phòng	Tại node 1, chạy 3 lệnh cấu hình để cho phép ssh từ node 1 sang node 2 mà không cần mật khẩu (chạy quyền user thường, không phải root): Sinh cặp key ssh: $ ssh-keygen Copy public key sang node 2: $ ssh-copy-id <user>@<ip-node-2> Thử ssh sang node 2. Nếu không cần nhập mật khẩu là OK: $ ssh <user>@<ip-node-2> Chạy thử lệnh sau để đồng bộ thư mục từ node 1 sang node 2: $ rsync -avr --delete /opt/docker/repo/ <user>@<ip-node-2>:/opt/docker/repo/ Tại node 1, chạy lệnh “crontab -e” và thêm dòng cấu hình sau: 0 */10 * * * rsync -avr --delete /opt/docker/repo/ <user>@<ip-node-2>:/opt/docker/repo/
6	Kiểm tra hoạt động của các dịch vụ	Bật trình duyệt vào portal qua VIP: https://<VIP>/login Thử kiểm tra agents đã cài đặt có online không.

3.6. Hướng dẫn kích hoạt license tập trung

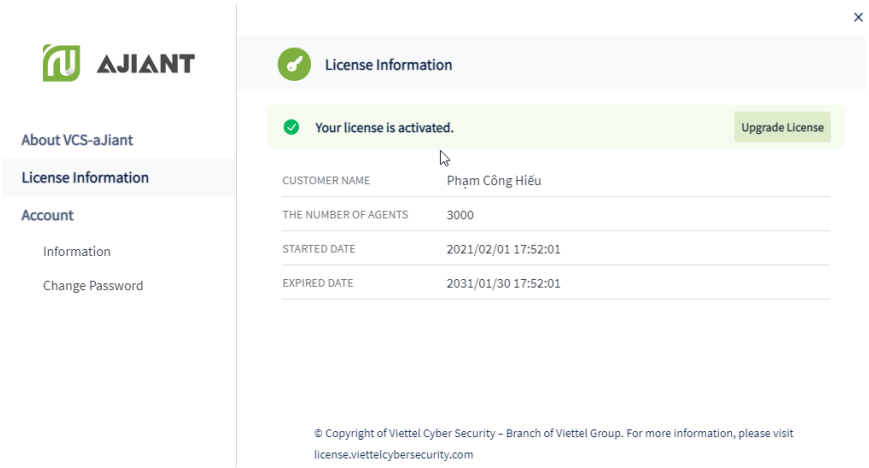
Tính năng license tập trung phục vụ bài toán kinh doanh, cho phép cung cấp sản phẩm theo hợp đồng đã ký kết với đơn vị, quy định về thời hạn sử dụng sản phẩm và số lượng agents tối đa cho phép cài đặt tại đơn vị.

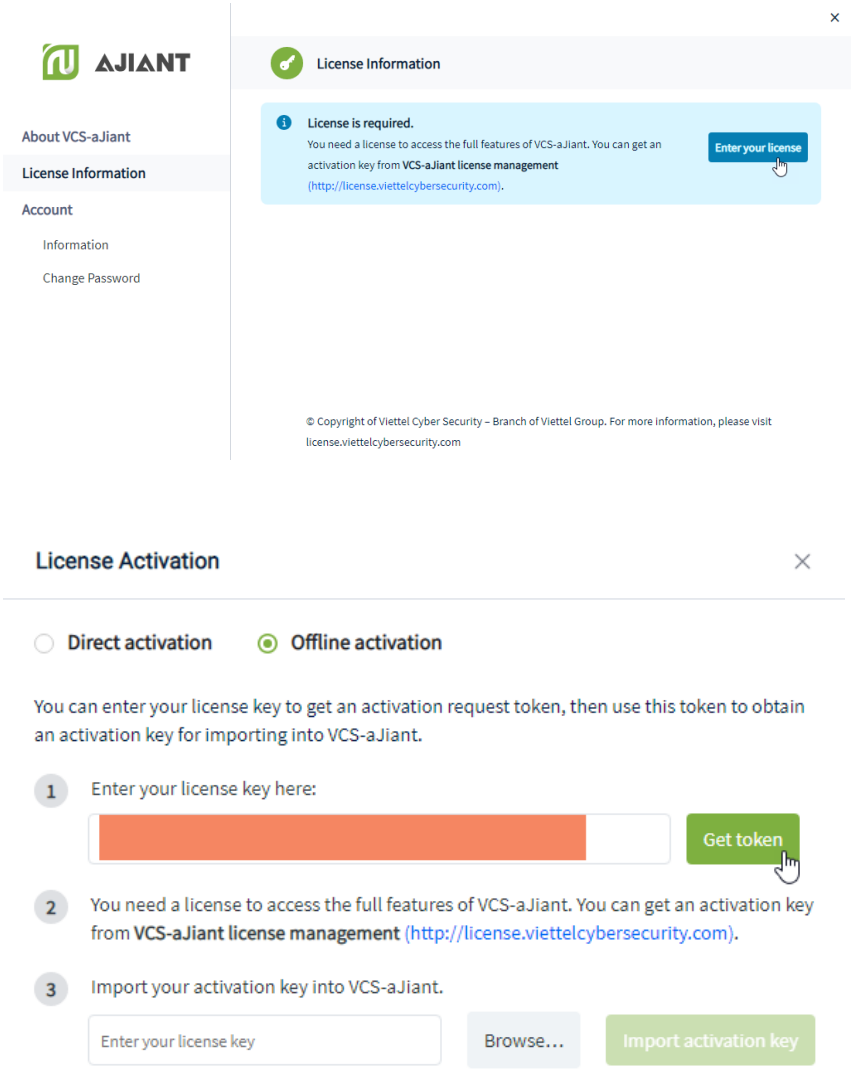
Về luồng quản lý license, sản phẩm gửi thông tin lên hệ thống quản lý license tập trung của VCS để kích hoạt, gia hạn, hủy hoặc định kỳ kiểm tra thời gian còn lại của license để quyết định cho phép agent hoạt động (trường hợp hết license, đơn vị vẫn có thể truy cập giao diện tuy nhiên không còn nhận được log từ agent nữa).

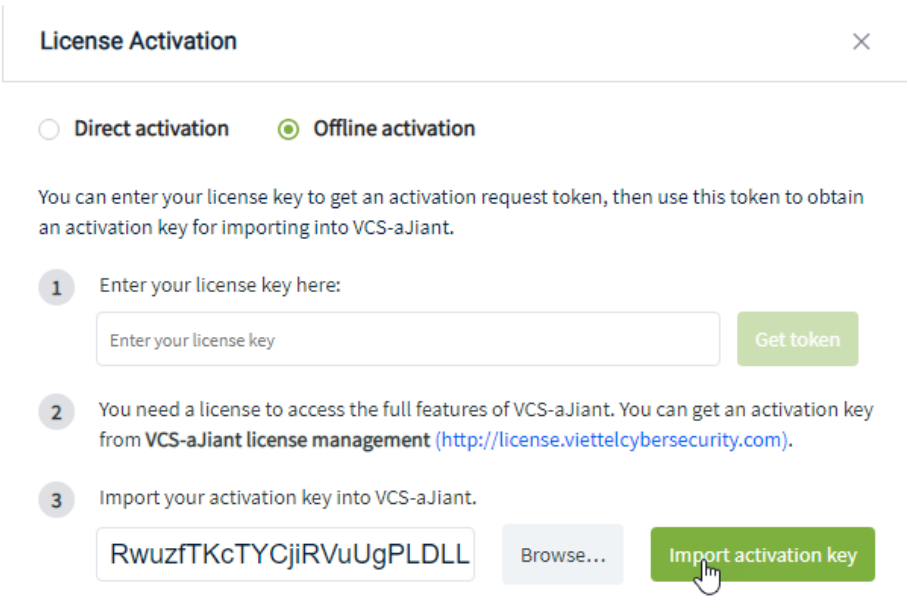
Lưu ý về cách thức kích hoạt license theo khách hàng:

- Kích hoạt online: áp dụng với khách hàng cho phép truy cập ngoại mạng từ hệ thống nội bộ.
- Kích hoạt offline: áp dụng với khách hàng **không** cho phép truy cập ngoại mạng từ hệ thống nội bộ (hệ thống bị cô lập).

Để tránh việc tính năng của phần mềm phụ thuộc vào đường Internet, khuyến nghị sử dụng cách kích hoạt license offline theo các bước sau:

Bước	Tên	Thực hiện
1	Tạo license key cho từng khách hàng	Gửi các thông tin qua email cho PM của dự án: • Họ tên, số điện thoại và địa chỉ email của đầu mối bên khách hàng. • Số lượng agent tối đa và thời hạn license của khách hàng theo Hợp đồng. PM dự án sẽ tạo license key cho từng khách hàng dựa vào các thông tin trên. Lưu ý: họ tên của đầu mối bên khách hàng sẽ hiển thị trên trang thông tin license 

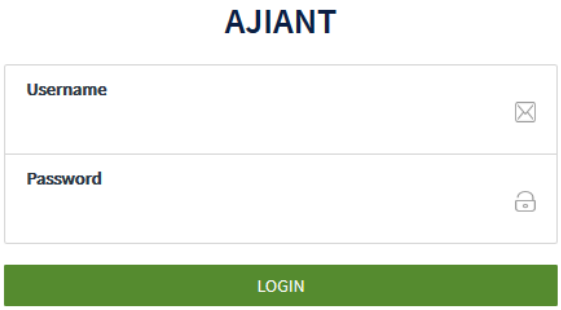
2	Lấy token	Đăng nhập portal VCS-aJiant, click vào icon thông tin **User > License Information > Enter your license > Offline activation**  Nhập license key vào **Enter your license key here**, click nút Get token, hệ thống sẽ cho tải về file **offline_request.txt**
3	Kích hoạt license	Gửi file offline_request.txt cho PO để PO tạo tiếp activation key dưới dạng 1 file text. Sau khi PO gửi lại activation key, import file text chứa activation key vào mục **Import your activation key into VCS-aJiant**



3.7. Đăng nhập Portal

Sau khi cài đặt thành công, vào trình duyệt, truy cập portal tại địa chỉ sau:

https://<ajiant-ip>



Đăng nhập bằng tài khoản quản trị đã được cung cấp

3.8. Tải bộ cài agent từ repo

Tải về bộ cài agent về tại địa chỉ URL:

https://<AJIANT_IP>/repo/

Hoặc

https://<AJIANT_IP>:8443/repo/

Index of /repo/

../		
release/	15-Dec-2021 10:46	-
ajiant_windows_3.3.0_x64_full.msi	31-Dec-2021 03:46	67051520
ajiant_windows_3.3.0_x86_full.msi	31-Dec-2021 03:46	62750720

4. HƯỚNG DẪN CÀI ĐẶT AGENT

4.1. Yêu cầu đảm bảo cài đặt

Hệ điều hành:

Tương thích cài đặt với các máy Windows 7 SP1, Windows Server 2008 R2 và các phiên bản mới hơn.

Cấu hình phần cứng:

Yêu cầu tối thiểu:

- RAM 2GB
- CPU 1 core
- Dung lượng cài đặt 128MB

Kết nối mạng:

Đảm bảo thông kết nối tới hệ thống quản lý tập trung theo các port (4443, 5672, 8443, 8888)

4.2. Hướng dẫn cài đặt

Cài đặt thông qua hệ thống tập trung:

B1. Tải bộ cài agent (x86 và x64) thông qua địa chỉ https://<server-ip>/repo/ theo version mới nhất.

Index of /repo/

../		
release/	28-Dec-2021 10:33	-
ajiant_centos6_3.3.0_x64_full.rpm	28-Dec-2021 11:04	52827752
ajiant_centos7_3.3.0_x64_full.rpm	28-Dec-2021 11:05	54602684
ajiant_macos_3.3.0_x64_full.dmg	28-Dec-2021 09:37	34210789
ajiant_ubuntu_3.3.0_x64_full.deb	28-Dec-2021 11:03	54155360
ajiant_windows_3.3.0_x64_full.msi	28-Dec-2021 11:03	67727360
ajiant_windows_3.3.0_x86_full.msi	28-Dec-2021 11:03	63311872

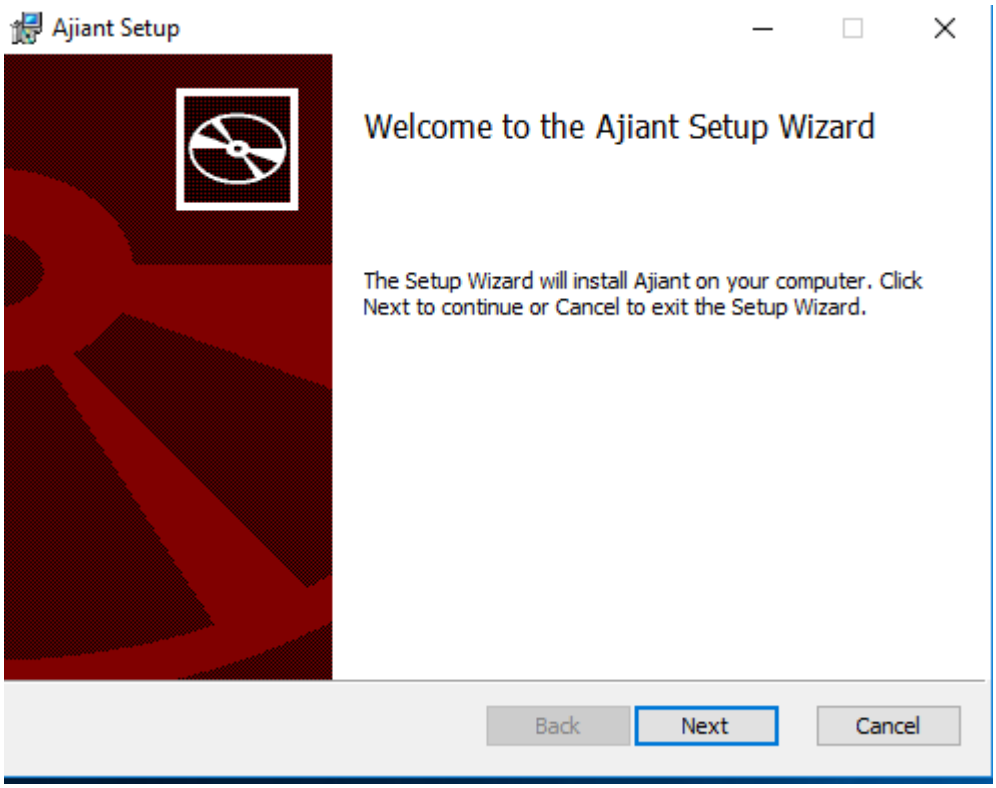
B2. Với các hệ thống quản trị tập trung AD thực hiện tạo package cài đặt từ xa cho bộ cài VCS-aJiant. Đẩy package xuống các máy cần cài đặt. Cấu hình tham số cài đặt cho bộ cài VCS-aJiant như sau:

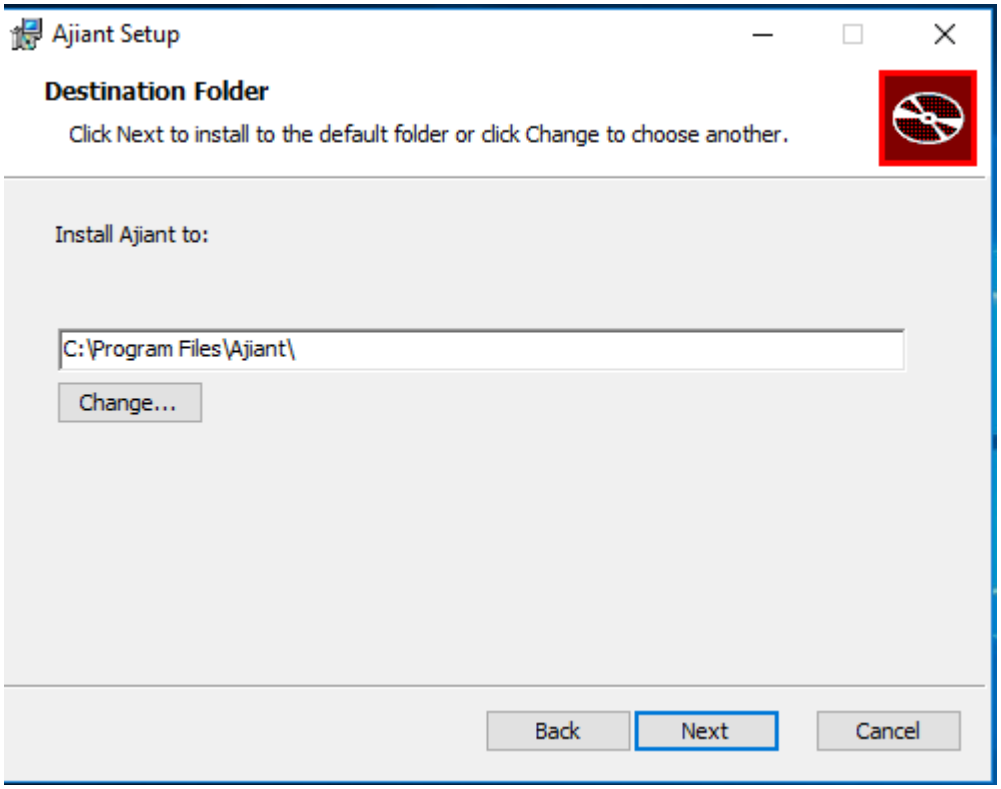
Msiexec.exe /i <setup_file>.msi /qn

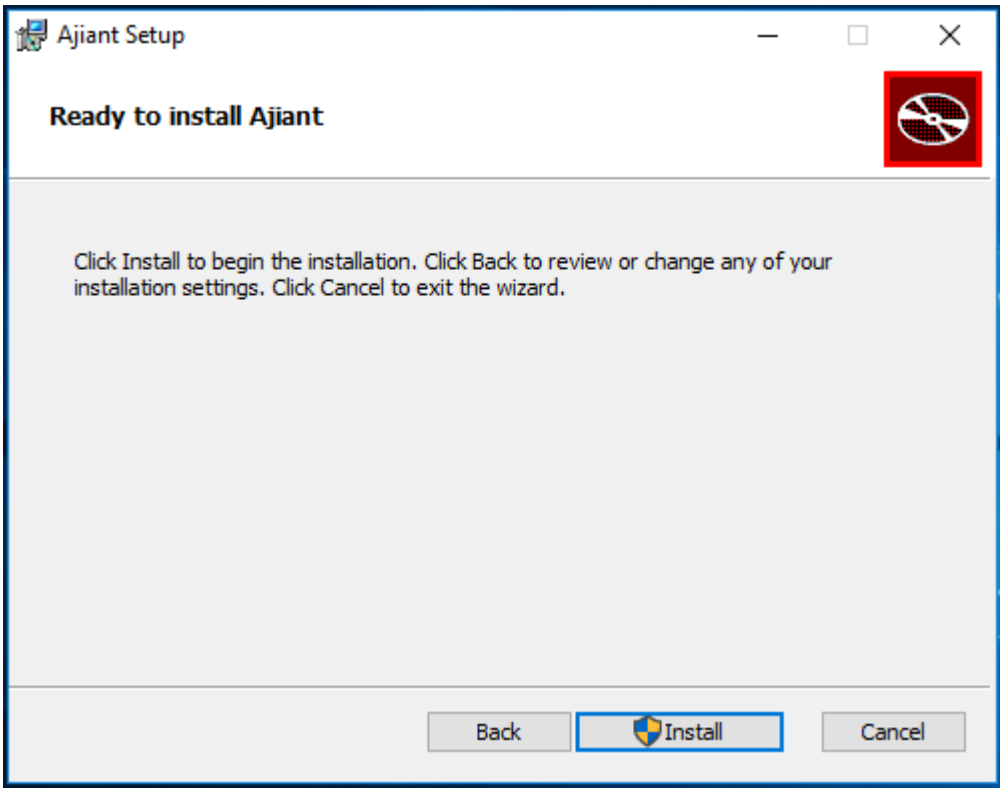
Cài đặt trực tiếp:

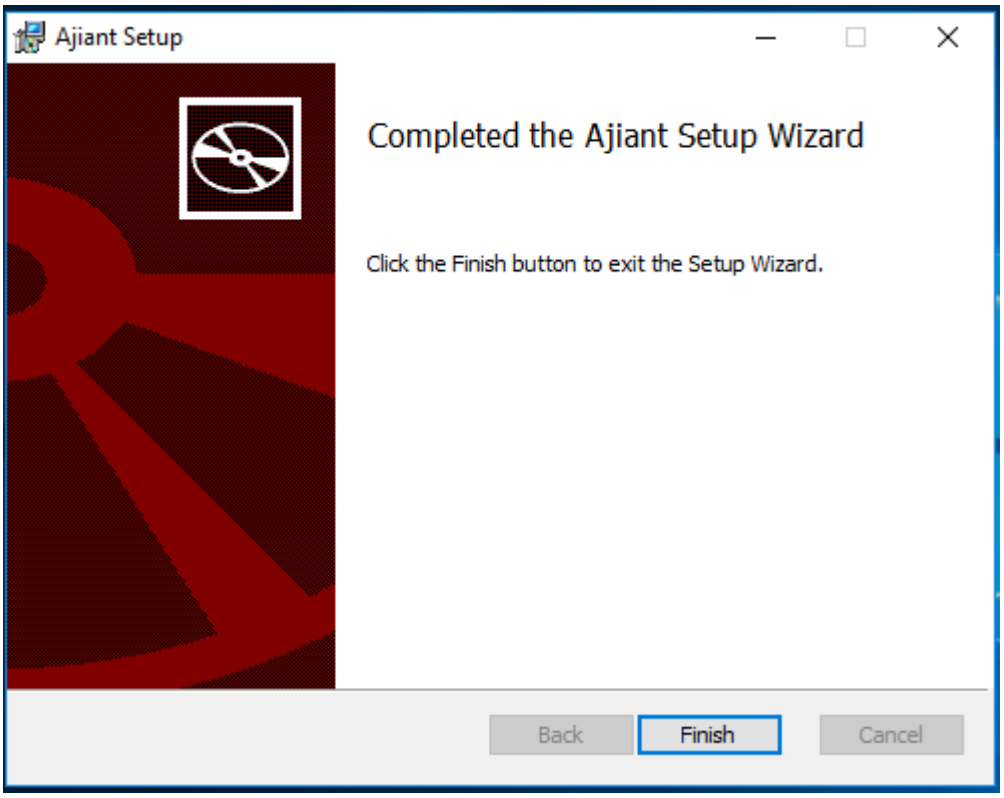
B1. Tải bộ cài (x86 và x64) thông qua địa chỉ https://<server-ip>/repo/ theo version mới nhất.

B2. Click đúp bộ cài, tiến hành cài đặt theo các bước (cần quyền administrator để thực hiện cài đặt)



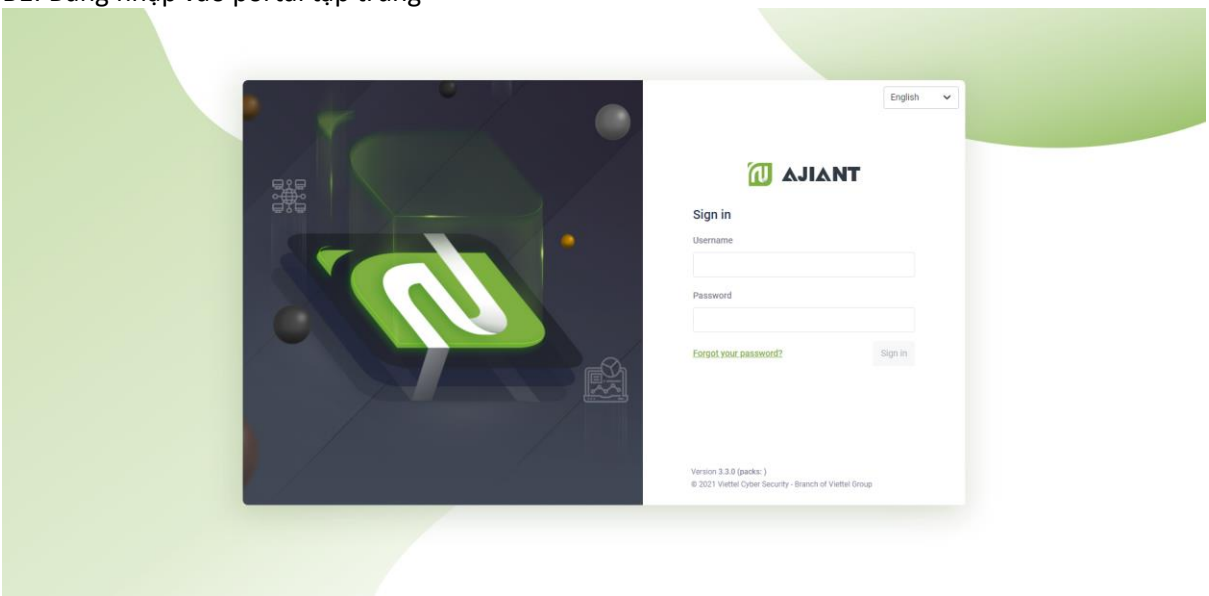

Ajiant Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install Ajiant to:
C:\Program Files\Ajiant\
Change...
Back
Next
Cancel


Ajiant Setup
Ready to install Ajiant
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

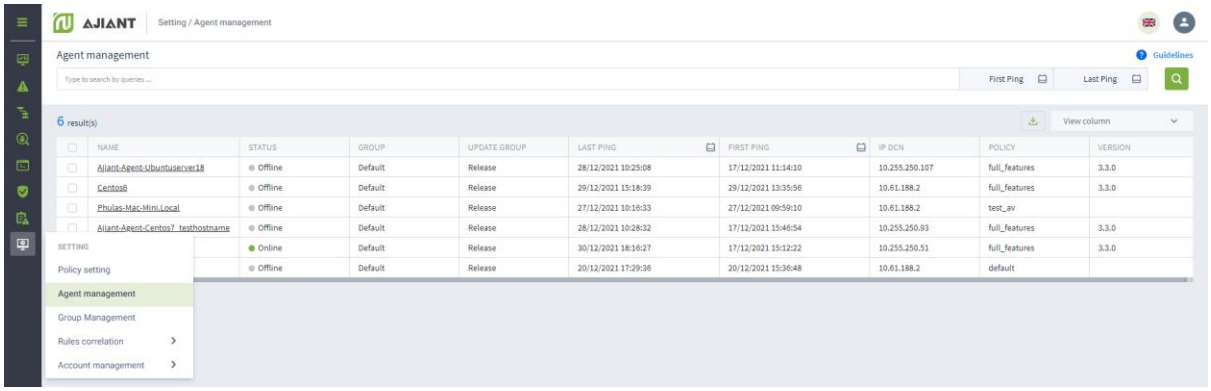


Kiểm tra sau cài đặt

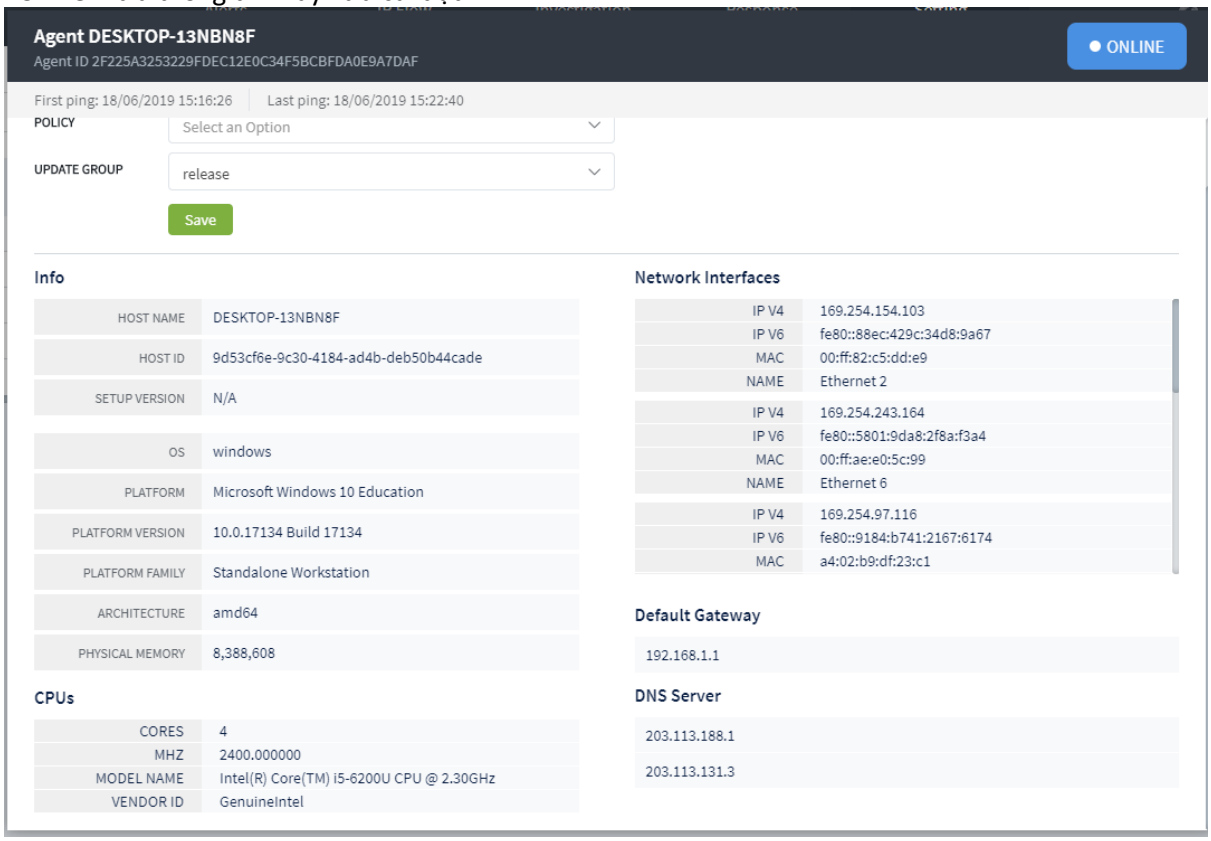
B1. Đăng nhập vào portal tập trung



B2. Vào mục quản lý agent (Agent Management)



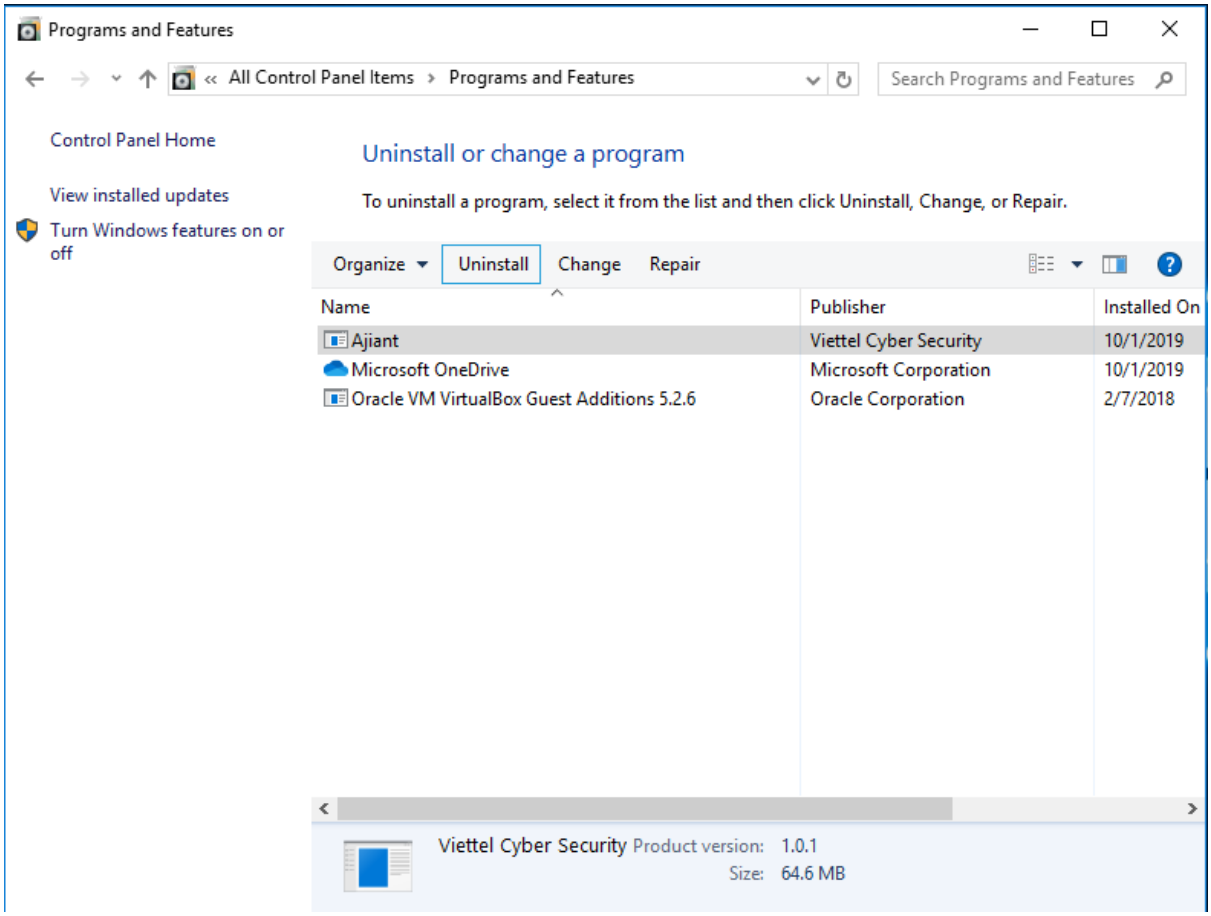
B3. Kiểm tra thông tin máy vừa cài đặt



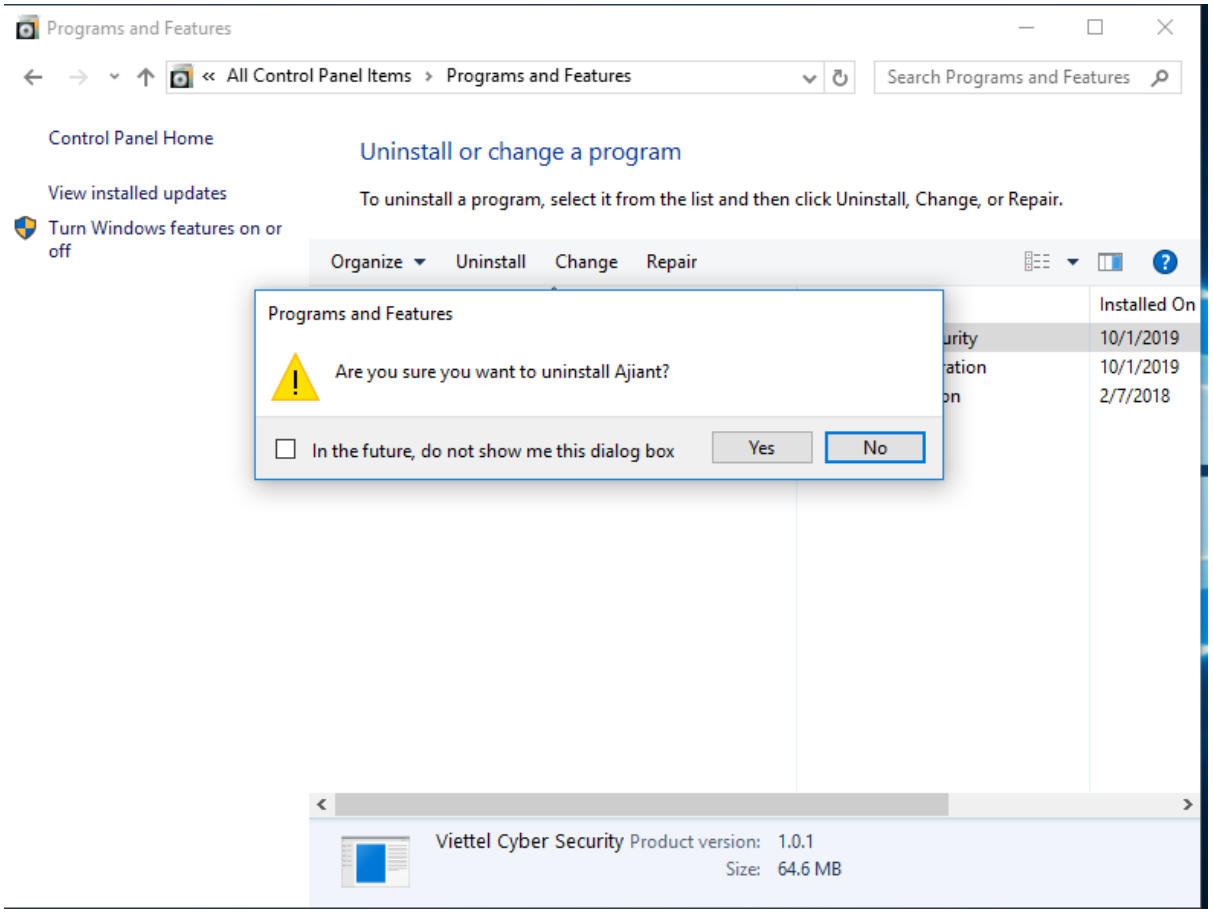
4.3. Hướng dẫn gỡ cài đặt

Gỡ cài đặt thông qua hệ thống tập trung:
Với các hệ thống quản trị tập trung AD thực hiện đẩy lệnh gỡ bỏ agent xuống các máy như sau:
wmic product where name="Ajiant" call uninstall

Gỡ cài đặt trực tiếp:
Trong trình quản lý **Programs and Features** của Windows thực hiện chọn gỡ bỏ agent



Thực hiện theo hướng dẫn để hoàn tất quá trình gỡ bỏ



5. KHẮC PHỤC SỰ CỐ

5.1. Các lỗi thường gặp khi cài đặt và nâng cấp backend

5.1.1. Lỗi build bộ cài agents

Quá trình sinh bộ cài MSI có thể xem log như sau:

```
$ tailf /opt/docker/agentbuild/Win7x86/Logs/VBox.log
```

Lỗi build bộ cài agent có thể do các nguyên nhân sau:

- Cài virtual box lỗi: cần cài đặt lại gói virtual box và gói mở rộng (extension pack)
- Giải nén file máy ảo bị lỗi: kiểm tra lại file máy ảo copy vào vào server (**Win7x86.tar.gz có kích thước 2.4GB**) và file sau khi giải nén (**Win7x86.vdi có kích thước khoảng 5GB**)
- Server chưa được bật tính năng ảo hoá Intel VT-x/AMD-V.

5.1.2. Không đăng nhập được portal

Tham khảo tài liệu Admin Guide mục 5.2.4

5.2. Khôi phục hệ thống

5.2.1. Khôi phục hệ thống sau khi nâng cấp gặp lỗi

Thay lại file *docker-compose.yml* vào ***/opt/docker/docker-compose.yml***

Chạy lệnh:

```
$ docker-compose up –d
```

Kiểm tra lại:

```
$ ./list-containers.sh
```

Xem các service có ở trạng thái "**Up**" không

5.2.2. Khôi phục toàn bộ (rollback)

Nếu hệ thống backend gặp lỗi không thể phục hồi lại (lỗi phần cứng server, lỗi ổ cứng) thì cần phải cài đặt lại hệ thống backend với các file cert và licence đã lưu lại ở bước cài đặt:

```
/opt/docker/nginx/certs/cert.crt
/opt/docker/nginx/certs/cert.crt
```

Các bước thực hiện tương tự mục 3.4 và 3.5 với file cert đã có sẵn

5.3. Thông tin đầu mối hỗ trợ

- Trung tâm giám sát và phản ứng trên không gian mạng, Công ty An ninh mạng Viettel

  Email: soc247@viettel.com.vn

- Bộ phận chăm sóc khách hàng, Công ty An ninh mạng Viettel

  Email: cskh_anm@viettel.com.vn