

Viettel Endpoint Detection & Response (VCS-aJiant)

Phiên bản 3.3.0 EDR – Năm 2021 Ngày cập nhật: 31/12/2021

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





Mục lục

Thuật ngữ.		5
1. GIỚI 1	THIỆU	6
1.1. Thự	rc trạng hiện nay	6
1.2. Sự p	phát triển của công nghệ	6
1.3. VCS	S-aJiant	6
2. TỔNG	G QUAN	7
2.1. Kiếr	n trúc hạ tầng	7
2.2. Côn	ng nghệ được sử dụng	8
3. HƯỚI	NG DẪN CÀI ĐẶT BACKEND	
3.1. Điều	u kiện đảm bảo cài đặt	8
3.2. Тор	oo của khách hàng	8
3.2.1.	AllInOne Topo	9
3.2.2.	MultiNode Topo	10
3.2.3.	MSSP Торо	11
3.3. Địn	h cỡ tài nguyên (Sizing)	12
3.3.1.	Cấu hình server tiêu chuẩn	12
3.3.2.	Sizing tài nguyên CPU và RAM theo số agents	13
3.3.3.	Sizing dung lượng ổ cứng theo số agents	13
3.4. Bản	ng thông tin phiên bản hỗ trợ nâng cấp	14
3.5. Các	: bước cài đặt backend AllInOne	15
3.5.1.	Cài đặt backend AllInOne version 3.3.0	15
3.5.2.	Cấu hình HA cho backend AllInOne	23
3.6. Các	: bước cài đặt backend MultiNode	
3.6.1.	Cấu hình các node máy ảo	28



3	3.6.2.	Cấu hình network interfaces	30
3	3.6.3.	Cài đặt backend MultiNode	30
3	3.6.4.	Cài đặt AJiantRegistry	36
3.7.	Ηướι	ng dẫn nâng cấp hệ thống	41
3	3.7.1.	Mô hình AllInOne	41
3	3.7.2.	Mô hình MultiNode	48
3.8.	Ηướι	ng dẫn kích hoạt license tập trung	
3.9.	Đăng	g nhập Portal	51
3.10	. Tải	bộ cài agent từ repo	51
3.11	. Hư	ớng dẫn cài đặt các thành phần của mô hình MSSP	
3	3.11.1.	Cài đặt server forwarder	52
3	3.11.2.	Cài đặt agent	52
3.12	. Hư	ờng dẫn thay certificate cho Portal	
4. I	HƯỚN	G DẪN CÀI ĐẶT AGENT	
4.1.	Ηướι	ng dẫn cài đặt trên Windows	53
2	4.1.1.	Yêu cầu đảm bảo cài đặt	53
2	4.1.2.	Hướng dẫn cài đặt	53
2	4.1.3.	Kiểm tra cài đặt	60
2	4.1.4.	Hướng dẫn gỡ cài đặt	61
4.2.	Ηướι	ng dẫn cài đặt trên Ubuntu và CyOS	
2	4.2.1.	Yêu cầu đảm bảo cài đặt	63
2	4.2.2.	Hướng dẫn cài đặt	64
2	4.2.3.	Kiểm tra cài đặt	64
2	4.2.4.	Hướng dẫn gỡ cài đặt	64
4.3.	Ηướι	ng dẫn cài đặt trên CentOS6 và CentOS7	65
2	4.3.1.	Yêu cầu đảm bảo cài đặt	65
2	4.3.2.	Hướng dẫn cài đặt	66



4.3.3.	Kiểm tra cài đặt	66
4.3.4.	Hướng dẫn gỡ cài đặt	66
4.4. Hư	ớng dẫn cài đặt trên MacOS	67
4.4.1.	Yêu cầu đảm bảo cài đặt	67
4.4.2.	Hướng dẫn cài đặt	67
4.4.3.	Kiểm tra cài đặt	70
4.4.4.	Hướng dẫn gỡ cài đặt	70
5. KHẮo	C PHỤC SỰ CỐ	71
5.1. Cá	c lỗi thường gặp khi cài đặt và nâng cấp backend	71
5.1.1.	Lỗi build bộ cài agents	71
5.1.2.	Không đăng nhập được portal	71
5.2. Kh	ôi phục hệ thống	71
5.2.1.	Khôi phục hệ thống sau khi nâng cấp gặp lỗi	71
5.2.2.	Khôi phục toàn bộ (rollback)	71
5.3. Thé	ông tin đầu mối hỗ trợ	72



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
НА	High Availability	Tính sẵn sàng cao

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

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:
 - Mô hình AllInOne: cấu hình 1 IP tĩnh cho node server.
 - Mô hình MultiNode: cần 3 IP tĩnh (1 public virtual ip cho kết nối từ agents đến server, 2 ip cho loadbalancer)
- Mở kết nối đến server qua các port sau:

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

 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

Tùy theo quy mô khách hàng triển khai, có thể lựa chọn triển khai hệ thống backend của VCS-aJiant theo 2 mô hình AllInOne hoặc MultiNode.



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. Mô hình này phù hợp khi triển khai với số lượng khách hàng nhỏ (<3000 agent).



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

Với các khách hàng có số agent nhỏ (<3000) nhưng vẫn yêu cầu có HA, thì có thể triển khai mô hình AllInOne có HA. Mô hình này 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.





3.2.2. MultiNode Topo

Với mô hình backend MultiNode, các dịch vụ được chạy trên nhiều node máy ảo khác nhau giữa các server vật lý. Mô hình Multinode hỗ trợ cân bằng tải, HA cho các dịch vụ và HA cho dữ liệu.





Hình 3. Mô hình triển khai backend MultiNode

3.2.3. MSSP Topo

Trong mô hình MSSP (Managed Security Service Provider) bao gồm 3 thành phần chính:

- Server tập trung: chứa các dịch vụ backend, được cài đặt theo cách thông thường theo mô hình AllInOne hoặc MultiNode
- Forwarder: forward các gói tin từ agent đến server tập trung và ngược lại. Forwarder đóng vai trò trung gian giữa agent và server đích.
- Agents: chỉ giao tiếp với forwarder





Hình 4. Mô hình triển khai MSSP qua forwarder

3.3. Định cỡ tài nguyên (Sizing)

Mô hình AllInOne không hỗ trợ được số lượng agents trên 3000. Với số lượng agents trên 3000,

cần cài đặt mô hình backend MultiNode.

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
 - o RAM: 16 GB

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 12



3.3.2. Sizing tài nguyên CPU và RAM theo số agents

Chú ý: với mô hình có multinode cần 3 (hoặc 5) server vật lý (số lẻ) để tính năng HA chạy hiệu quả

Số agents	Mô hình cài đặt	Không có HA		Có HA	
		Số server vật lý	Loại server	Số server vật lý	Loại server
0 → 200	All In One	1	4	2	4
$200 \rightarrow 2k$	All In One	1	3	2	4
2k → 5k	All In One	1	2	2	2
	Multi Node	N/A	N/A	3	2
5k → 10k	Multi Node	N/A	N/A	3	2
10k → 25k	Multi Node	N/A	N/A	3	1
25k → 50k	Multi Node	N/A	N/A	5	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 <i>buffered disk reads</i>):
		\$ 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	< 1 ms	Cài thêm gói ioping để kiểm tra độ trễ ổ cứng:
cứng		\$ apt update && apt install -y ioping
		Chạy lệnh sau trên node cần kiểm tra:
		\$ ioping -c 10 .
IOPS	read: iops >= 500	Cài thêm gói fio để kiểm tra IOPS ổ cứng:
		\$ apt update && apt install -y fio

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com \square



,	write: iops >= 200	Chạy lệnh sau trên node cần kiểm tra:
		\$ fiorandrepeat=1ioengine=libaiodirect=1gtod_reduce=1 name=tempfilefilename=tempfilebs=4kiodepth=64
		size=4Greadwrite=randrwrwmixread=75

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	500 GB	1 TB
500 → 2k	1 TB	2 ТВ
$2k \rightarrow 5k$	2 TB	4 TB
$5k \rightarrow 7k$	3 TB	6 ТВ
$7k \rightarrow 10k$	4 TB	8 TB
10k → 15k	6 TB	12 TB
15k → 20k	8 TB	16 TB
20k → 25k	10 TB	20 ТВ
25k → 30k	12 TB	25 TB
30k → 40k	15 TB	30 ТВ

Dung lượng ổ cứng theo số agents triển khai

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 cấ	р
		3.3.0 EDP	3.3.0 EDR	3.3.0 EPP
ai	3.1.0 EDR	\checkmark	\checkmark	Х
ersion hiện t	3.3.0 EPP	\checkmark	\checkmark	
	3.3.0 EDR	\checkmark		х
>	3.3.0 EDP		Х	Х

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com \square



3.5. Các bước cài đặt backend AllInOne

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 back	cend 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	Chỉnh đúng thời gian và múi giờ cho server, khuyến nghị cấu hình NTP để đồng bộ thời gian cho server.	
	cho server	Chú ý: thời gian server không đúng có thể gây ra lỗi license, timestamp event log, timestamp alert	
3	Chạy script	Copy các file sau lên server và đặt cùng 1 thư mục:	
	cài đặt	 install_vedr_backend.sh vedr_requirement.tgz Win7x86.tar.gz vedr_backend_setup_3.3.0.deb 	
		<pre>ubuntu@ubuntu:~/setup\$ ll total 4921616 drwxrwxr-x 2 ubuntu ubuntu</pre>	
		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.	
		<mark>Chú ý:</mark> 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.	

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com \square



		Backend requirements installation
		Install backend requirements now ?
		<yes> <no></no></yes>
		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.
		Installing ajiant backend all in one Select a package file to install:
		<pre>vedr_backend_setup_3.3.0.deb2185408896(bytes)</pre>
		<0k> <cancel></cancel>
		Lựa chọn đúng file muôn cài và chọn OK hoặc ân Enter để tiếp tục.
		tất cả dịch vụ lại trước khi cài bản mới không (chọn Yes)
		Warning !
		Found existing docker-compose.yml at /opt/docker/docker-compose.yml Stop the running services before removing backend files data ?
		<yes> <no></no></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.

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | **16**



		Accept EULA ?
		End-User License Agreement ("Agreement") Last updated: July 18, 2019 Please read this End-User License Agreement ("Agreement") carefully before clicking the "I Agree" button, downloading or using "Ajiant" ("Application"). By clicking the "I Agree" button, downloading or using the Application, you are agreeing to be bound by the terms and conditions of this Agreement. This Agreement is a legal agreement between you (either an individual or a single entity) and "Ajiant" and it governs your use of the Application made available to you by "Ajiant". If you do not agree to the terms of this Agreement, do not click on the "I Agree" button and do not download or use the Application. The Application is licensed, not sold, to you by "Ajiant" for use strictly in accordance with the terms of this Agreement. License Subject to the condition that you have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("the License"): Installation and use: You shall have the non-exclusive, non-transferable right to download, install and use the Application solely for your personal, non-commercial purposes strictly in accordance with the terms of this Agreement. Termination of the License: The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the
6 Chọn phiên bản backend để cài đặt		 File vedr_backend_setup_3.3.0.deb hỗ trợ cài đặt 2 phiên bản EDR và EDP: EDR: chỉ có tính năng của EDR EDP: có thêm tính năng Antivirus
		Select production type to install Choose an option and press Enter To exit, select 'Cancel' or press ESC 1 EDR (Endpoint Detection & Response) 2 EDP (EDR + AntiVirus) <0k>
7	Nhập địa chỉ của	Sau khi bộ cài DEB được unpack ra /opt/docker , sẽ đến phần cấu hình cài đặt VEDR Backend.
	server	

Page | **17**



		Enter public virtual IP to install VEDR <ok> <cancel></cancel></ok>
		Enter BACKUP public virtual ip or leave empty if not set <0k> <cancel> 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</cancel>
8	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 Found existing certificate ! Reuse certificate from the previous installation at path /opt/docker/nginx/certs/cert.crt ? Yess < 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.



Enter common name (CN) ajiant.com <pre></pre>
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.
Select DNS or IP SANs to generate certificate [*] ajiant.com domain [*] iant.com domain [*] localhost domain [*] 127.0.0.1 ip [] 192.168.129.136 ip [] 172.17.0.1 ip
Nếu agent kết nối qua tên miền thì nhập tên miền vào ô DNS SANs.
Enter extra DNS SANs or IP SANs (Leave empty to start generating certificate) <0k> <cancel></cancel>
Nhập thời gian hết hạn chứng thư theo ngày (mặc định là 3650):



		Enter expire days 3650 <0k> <cancel></cancel>
		<pre>Kết quả sẽ sinh 2 file trong thư mục: /opt/docker/nginx/certs/ cert.crt cert.key Common name: edr.viettel.com.vn DNS SANs: edr.viettel.com.vn localhost IP SANs: 127.0.0.1 192.168.129.136 Successfully generated certificate Certificate: /opt/docker/nginx/certs/cert.crt Drivete Kertificate /opt/docker/nginx/certs/certs/cert.crt Drivete Kertificate /opt/docker/nginx/certs/certs/cert.crt Drivete Kertificate /opt/docker/nginx/certs/certs/cert.crt Drivete Kertificate /opt/docker/nginx/certs/certs/certs/cert Certificate /opt/docker/nginx/certs/certs/cert Certificate /opt/docker/nginx/certs/certs/cert Certificate /opt/docker/nginx/certs/certs/cert Litteficate /opt/docker/nginx/certs/certs/cert</pre>
9	Nhập đường dẫn cert inspect	Enter inspect certificate file path or leave empty if not set <0k> <cancel> <0k> <cancel> Nếu không dùng cert inspect để rỗng và enter bỏ qua bước này. Nếu có dùng cert inspect thì nhập đường dẫn cert inspect. Chon OK Script</cancel></cancel>
		sẽ copy file cert_insp vào: /opt/docker/config/cert_insp.crt
10	Tạo bộ cài đặt agent	Khi được xác nhận tạo bộ cài agent không, chọn Yes để tiếp tục.

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



		Final step: Build agent installer Build agent installer now ? <pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre>			
		Nhập phiên bản bộ cài agent hoặc ấn Enter để lấy phiên bản mặc định tự sinh			
		VEDR build version: 3.3.0 <ok> <cancel></cancel></ok>			
		Chờ khoảng 10 phút để server build bộ cài agent (build agent windows có thể đến 5 phút 1 lần build do phải khởi đôna máv ảo vbox)			
		Nếu quá trình cài đặt thành công, server sẽ sinh ra 2 file MSI (cho windows), 1 file DEB, 2 files RPM và 1 file DMG trong thư mục: /opt/docker/repo/public/			
		 ajiant_windows_3.3.0_x64_full.msi ajiant_windows_3.3.0_x86_full.msi ajiant_ubuntu_3.3.0_x64_full.deb ajiant_centos7_3.3.0_x64.rpm ajiant_centos6_3.3.0_x64.rpm ajiant_macos_3.3.0_x64_full.dmg 			
11	Khởi động server vedr backend	Final step ! Start VEDR server now ?			
		<yes> <no></no></yes>			

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

		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	Initializing data ! Initializing data on the first instalation ? Yes> Yes> 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. Change portal password :		
		Xác nhận password đã nhập		
		Confirm root password:		
		<0k> <cancel></cancel>		
		Nếu thành công thì password mới sẽ được thiết lập cho user root.		





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:		
		<pre>\$ sudo dpkg -i haproxy-keepalived/\$(lsb_release -s -c)/*.deb</pre>		
		Có thể chạy gộp 2 lệnh trên thành 1 lệnh duy nhất:		
		<pre>\$ tar -zxf haproxy-keepalived.tgz && sudo dpkg -i haproxy- keepalived/\$(lsb_release -s -c)/*.deb</pre>		
2	Cấu hình	Quy hoạch 01 địa chỉ virtual ip (VIP) cùng dải với ip 2 node AllInOne		
	keepalived	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		
		}		
		<pre>vrrp_script chk_haproxy {</pre>		
		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 ens160="" eth0="" interface,="" vd:=""></net>		
		virtual_ipaddress {		
		<vip> dev <net ens160="" eth0="" interface,="" vd:=""></net></vip>		
		}		
		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

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 25



		}	
		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></vip>	
		\$ telnet <vip> 443</vip>	
3	Cấu hình cluster	Mở file /opt/docker/docker-compose.yml	
	cho cassandra	Sửa cấu hình service Cassandra trên 2 node:	
		+ Network_mode: host	
		+ CASSANDRA_BROADCAST_ADDRESS= <ip hiện="" node="" tại=""></ip>	
		+ CASSANDRA_RACK=<2 node nhập giá trị khác nhau, vd: rack1,rack2>	
		+ CASSANDRA_SEEDS= <danh 2="" clusters,="" cả="" của="" gồm="" ip="" node="" sách=""></danh>	
		<pre>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 - HEAP_NEWSIZE=500M - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.131 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.132 - CASSANDRA_BROADCAST_ADDRESS=10.0.0.132 - CASSANDRA_AUTO_BOOTSTRAP=false volumes: /data:/var/lib/cassandra /log:/var/log/cassandra /java:/usr/share/java</pre>	
		Khởi động lại Cassandra trên 2 node:	
		\$ cd /opt/docker/	
		\$ docker-compose up -d cassandra	

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | **26**



	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-Cassandral:/opt/docker\$ /opt/docker/cassandra/nodetool.sh status Datacenter: dc1 ====================================			
4	Cấu hình cluster	Mở file /opt/docker/elasticsearch/elasticsearch.yml			
	cho elasticsearch	Sửa các cấu hình như sau:			
		+ network.host: 0.0.0.0			
		+ discovery.zen.ping.unicast.hosts: [" <ip 1="" node="">", "<ip 2="" node="">"]</ip></ip>			
		cluster.name: "ES-EDR"			
		node.name: ES network.host: 0.0.0.0			
		<pre>http.cors.enabled: true http.cors.allow-origin: "*"</pre>			
		<pre>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	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):			
	chính sang node dự phòng	Sinh cặp key ssh:			
		\$ ssh-keygen			
		Copy public key sang node 2:			
		\$ ssh-copy-id <user>@<ip-node-2></ip-node-2></user>			
		Thử ssh sang node 2. Nếu không cần nhập mật khẩu là OK:			

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

		\$ ssh <user>@<ip-node-2></ip-node-2></user>
		Chạy thử lệnh sau để đồng bộ thư mục từ node 1 sang node 2:
		\$ rsync -avrdelete /opt/docker/repo/ <user>@<ip-node- 2>:/opt/docker/repo/</ip-node- </user>
		Tại node 1, chạy lệnh "crontab -e" và thêm dòng cấu hình sau:
		0 */10 * * * rsync -avrdelete /opt/docker/repo/ <user>@<ip-node- 2>:/opt/docker/repo/</ip-node- </user>
6	Kiểm tra hoạt động của các dịch vụ	Bật trình duyệt vào portal qua VIP: <u>https://<vip>/login</vip></u> Thử kiểm tra agents đã cài đặt có online không.

3.6. Các bước cài đặt backend MultiNode

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.

3.6.1. Cấu hình các node máy ảo

Cấu hình cài đặt các máy ảo trên mỗi 1 server vật lý:

Để tiện cấu hình về sau, khi cài OS nên đặt chung tài khoản và mật khẩu/key ssh, chung mật khẩu sudo giữa các node.

STT	Loại node VM	Cấu hình	Ghi chú
1	Loadbalancer	CPU: 8 virtual core	Ldirectord
		RAM: 4 GB	Corosync
		HDD: 40 GB	Pacemaker
		Network: 1 IP DCN + 1 IP dải nội bộ 10.0.0/24	
2	Docker manager	CPU: 8 virtual core	Docker manager
		RAM: 8 GB	Microservices
		HDD: 80 GB	Docker registry
		Network: 1 IP dải nội bộ 10.0.0.0/24	
3	Queue	CPU: 16 virtual core	Rabbitmq
		RAM: 12 GB	Logstash
		HDD: 120 GB	Nats streaming
		Network: 1 IP dải nội bộ 10.0.0.0/24	Redis

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



4	Database	CPU: 16 virtual core	Elasticsearch
		RAM: 32 GB	Mongodb
		HDD: 2 TB	
		Yêu cầu HDD: - Tốc độ đọc >= 200 MB/s - Tốc độ ghi >= 100 MB/s	
		Network: 1 IP dải nội bộ 10.0.0.0/24	
5	Cassandra	CPU: 16 virtual core	Cassandra
		RAM: 16 GB	
		HDD: 120 GB	
		Network: 1 IP dải nội bộ 10.0.0.0/24	
6	Correlation	CPU: 12 virtual core	Correlation engine
		RAM: 16 GB	
		HDD: 40 GB	
		Network: 1 IP dải nội bộ 10.0.0.0/24	
Tổng		Tổng:	
		CPU: 76 virtual core	
		RAM: 88 GB	
		HDD: 2.4 TB	

Giữa các server vật lý cần có đường truyền tốc độ cao (khuyến nghị sử dụng đường truyền tối thiểu 1Gbs). Khi cài đặt xong các máy ảo cần test thử tốc độ mạng tại các node giữa các server vật lý khác nhau.

Chú ý kiểm tra tốc độ đọc ghi ổ cứng của node elasticsearch:

- Lệnh kiểm tra tốc độ đọc:

\$ hdparm -Tt /dev/sda

- Lệnh kiểm tra tốc độ ghi:

\$ dd if=/dev/sda of=largefile bs=1M count=100

- Lệnh kiểm tra độ trễ ổ cứng:

\$ ioping -c 10.

- Lệnh kiểm tra IOPS:

\$ fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1 --name=tempfile -filename=tempfile --bs=4k --iodepth=64 --size=4G --readwrite=randrw --rwmixread=75

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 29



3.6.2. Cấu hình network interfaces

Tại các node cần xác định 1 IP làm local virtual ip. Ví dụ: 10.0.0.100 Khi cấu hình network interfaces, cần đặt gateway là local virtual ip. Ví dụ với node có IP 10.0.0.101:

The primary network interface
network:
version: 2
ethernets:
ens33:
addresses: [10.0.0.101/24]
gateway4: 10.0.0.100

Riêng node Loadbalancer cần có 2 network interfaces. Chỉ đặt gateway cho interface có ip public, không đặt gateway cho interface dải local.

Ví dụ LB1 có ip local 10.0.0.11 và ip public 10.30.161.11:

#	t The primary network interface
n	network:
	version: 2
	ethernets:
	ens33:
	addresses: [10.0.0.11/24]
	ens38:
	addresses: [10.30.161.11/24]
	gateway4: 10.30.161.1

3.6.3. Cài đặt backend MultiNode

Bước	Thực hiện
1	Cài đặt các node VM theo cấu hình ở trên.
	Đồng bộ thời gian cho các server trong cụm multimode: có thể dùng giải pháp NTP.

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

L



	<mark>Chú ý:</mark> thời gian server không đúng có thể gây ra lỗi license, timestamp event log, timestamp alert,
	Đồng thời trên mỗi node VM (trừ các node LB) cài đặt các gói phần mềm cần thiết như sau.
	Copy 2 file sau đặt chung vào 1 thư mục: - Gói phần mềm cần thiết cho Ubuntu 20: packages.tgz - Script cài đặt: install-common-requiments.sh
	Chạy lệnh cài đặt các gói:
	\$ sudo bash install-common-requirements.sh
	ubuntu@ajiant-staging-dockermanager-3:~/setup\$ ll total 103244 drwxrwxr-x 2 ubuntu ubuntu 4096 Dec 30 07:01 ./ drwxr-xr-x 6 ubuntu ubuntu 4096 Dec 30 07:01/ -rw-rw-r 1 ubuntu ubuntu 1659 Dec 21 11:15 install-common-requirements.sh -rw-rw-r 1 ubuntu ubuntu 105709503 Dec 21 09:18 packages.tgz ubuntu@ajiant-staging-dockermanager-3:~/setup\$
	Chú ý quan sát quá trình cài đặt gói thành công không.
2	Trên node lb cài đặt các gói cần thiết của LoadBalancer theo các bước sau:
	• Lựa chọn 1: loadbalancer dùng bộ giải phảp pacemaker, corosync, ldirectord.
	Copy file lb-packages-ubuntu20.tgz vào 2 node Loadbalancer
	Giải nén bộ file cài đặt:
	\$ tar -zxf lb-packages-ubuntu20.tgz
	Kết quả giải nén ra 2 thư mục pacemaker-corosync và ldirectord-ipvsadm :
	Cài đặt các gói DEB:
	\$ sudo dpkg -i pacemaker-corosync/*.deb
	\$ sudo dpkg -i ldirectord-ipvsadm/*.deb
	Có thể chạy gộp 3 lệnh trên thành 1 lệnh duy nhất:
	\$ tar -zxf lb-packages-ubuntu18.tgz && sudo dpkg -i pacemaker-corosync/*.deb && sudo dpkg –i ldirectord-ipvsadm/*.deb
	• Lựa chọn 2: loadbalancer dùng bộ giải pháp haproxy, keepalived
	Copy file haproxy-keepalived.tgz vào 2 node loadbalancer
	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
	Phần cấu hình 2 node Loadbalancer sẽ ở phần tiếp theo (dùng ansible playbook)
3	Cài đặt node aiiant registry
-	Chọn node làm ajiant docker registry (thường chọn node manager1).
	Chạy script cài đặt các gói cần thiết theo yêu cầu nếu chưa cài ở bước 1:
	\$ sudo bash install-common-requirements.sh
	 Đưa các file cài đặt ansible sau vào node registry: install-ansible.sh ansible.tgz
	Cài đặt gói ansible:
	\$ sudo bash install-ansible.sh
	Tạo thư mục setup, chuẩn bị file ansible_playbook_3.3.0.zip và copy vào trong thư mục setup của node registry:
	\$ mkdir setup && cd setup
	Giải nén file zip:
	\$ unzip ansible_playbooks_3.3.0.zip

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com


	Chuan bị folder vbox và copy vào trong folder setup /
	ubuntu@ajiant-staging-dockermanager-1:~/setup\$ ll vbox/ total 192916 drwxrwxr-x 3 ubuntu ubuntu 4096 Dec 30 14:04 ./ drwxrwxr-x 6 ubuntu ubuntu 4096 Dec 30 14:02/ drwxr-xr-x 2 root root 4096 Dec 21 08:48 focal/ -rw-rw-r 1 ubuntu ubuntu 1814 Dec 21 09:30 install_vbox.sh -rw-rw-r 1 root root 11134336 Nov 9 10:10 Oracle_VM_VirtualBox_Extension_Pack-6.1.26.vbox-extpack -rw-rw-r 1 ubuntu ubuntu 93194508 Dec 21 09:09 vbox-packages.tgz -rw-rw-r 1 ubuntu ubuntu 93194508 Dec 30 14:04 Win7x86.tar.gz ubuntu@ajiant-staging-dockermanager-1:~/setup\$
	Chạy lệnh sau để cài ajiant_registry:
	<pre>\$ sudo bash install_ajiant_registry.sh</pre>
	Xem chi tiết quá trình thực hiện cài đặt tại mục 3.5.4
4	Cấu hình ansible theo các bước sau: Bước 1: Cấu hình file hosts : đổi tên file template có sẵn host.x.x.template thành file hosts . Mở file hosts điền thông tin ip của các node theo loại dịch vụ chạy trên node. - registry: điền ip nội bộ của node registry - elasticsearch: điền ip nội bộ các node database - cassandra: điền ip nội bộ các node cassandra - mongodb: điền ip nội bộ các node database - ms: điền ip nội bộ các node docker managers - controlserver: điền ip nội bộ các node docker managers - repo: điền ip nội bộ các node docker managers - nats: ip các node chạy nats streaming server

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 33

L



	 rabbitmq: điền ip nội bộ các node queue redis: điền ip nội bộ các node queue correlation và con điền in nội bộ các node correlation
	 lb1: ip nôi bô node loadbalancer 1
	- lb2: ip nội bộ node loadbalancer 2
	 loadbalancer: ip nội bộ các node loadbalancer
	- managers: điền ip nội bộ các node docker managers
	 workers: điện ip nội bộ các node ngoại trừ node docker managers [allware] cấu hình hiến tổng thể khi chay angible tooka angible ware
	- [all:vars] cau ninh bien tong the kni chạy ansible tasks: ansible_user,
	• PUBLIC VIP: địa chỉ tên miền hoặc public virtual IP của server
	 LOCAL_VIP: local virtual IP của server (chú ý LOCAL_VIP trùng với gateway cấu hình ở mục 3.2). Để trống LOCAL_VIP nếu không có
	aai mang noi bo.
	 REGISTRY HOST: điền ip nội bộ các node registry
	Bước 2: Cấu hình file group_vars : Mở file group_vars/all.yml và cấu hình các biến sau: - microservices_hosts: cấu hình danh sách hostname của các node chạy
	micro services
	 rabbitmq_nosts: cau ninn dann sach nostname cua cac node se chay rabbitmq server
	- correlation hosts: cấu hình danh sách hostname của các node sẽ chạy
	correlation engine
	 redis_hosts: cấu hình danh sách hostname của các node sẽ chạy redis
	server
	 registry_nosts, cau ninn dann sach nostname cua node registry rack_node_labels; cau hinh tag số hiệu rack cho các node, các node chay
	cùng server vật lý cần có tag chung số hiệu rack
5	Chạy ansible playbook để cấu hình thiết lập môi trường docker swarm, cho các node (trừ LB) cùng tham gia docker swarm
	\$ ansible-playbook -i hosts init-swarm.yml -vkK
	SSH password:
	BECOME password[defaults to SSH password]:
	Nhập password ssh và password để lên quyền root
	Quan sát quá trình cài đặt xem có thành công không.
	Khi cài đặt thành công, kiểm tra danh sách node trong swarm:
	\$ sudo docker node ls

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

	ubuntu@ajiant-staging-dockermanager-l:-/setup\$ sudo docker node ls [sudo] password for ubuntu: ID H0STNAME STATUS AVAILABILITY MANAGER STATUS ENGINE VERSION ch0mrolfvr7i8skh5112z5gf2 ajiant-staging-correlation-1 Ready Active 19.03.15 mpju9nisiBa30u0ma9z4tv ajiant-staging-correlation-2 Ready Active Reachable 19.03.15 npju9nisiBa30u0ma9z4tv ajiant-staging-dockermanager-1 Ready Active Reachable 19.03.15 nptrvsilagz4leswad29bryk ajiant-staging-dockermanager-2 Ready Active Reachable 19.03.15 q0gxthloid9k050mjpyr01n ajiant-staging-queue-1 Ready Active Leader 19.03.15 q00gxthloid9k050mjpyr01n ajiant-staging-queue-2 Ready Active 19.03.15 ubuntu@ajiant-staging-dockermanager-1:/setups Như vậy tất cả các node (trừ LB) đã cùng ở trong docker swarm. 19.03.15 Chú ý: kiểm tra các HOSTNAME ở trên có giống hostname cấu hình trong 19.03.15			
6	group_vars/all.yml không ! Chỉ làm bước này khi bước trên thành công			
	Ś sudo bash install ajiant services sh			
	SSH password.			
	BECOME password[defaults to SSH password]:			
	Nhập password ssh và password để lên quyền root			
7	Chạy lệnh sinh bộ cài agent (yêu cầu phải cài trước virtualbox và unpack gói máy ảo):			
	\$ cd /opt/ajiant && sudo bash gen_agent_installer.sh			
	Khi kết thúc sinh bộ cài agent thì sẽ sinh ra 2 file MSI (cho windows), 1 file DEB, 2 files RPM và 1 file DMG trong thư mục: /opt/ajiant/repo/public/			
	 ajiant_windows_3.3.0_x64_full.msi ajiant_windows_3.3.0_x86_full.msi ajiant_ubuntu_3.3.0_x64_full.deb ajiant_centos7_3.3.0_x64.rpm ajiant_centos6_3.3.0_x64.rpm ajiant_macos_3.3.0_x64_full.dmg 			
	Chạy đồng bộ repo từ registry ra các node thuộc nhóm repo:			
	\$ sudo ansible-playbook -i hosts playbook/sync-repo.yml			
8	Vào 2 node Loadbalancer kiểm tra cài đặt LB:			
	\$ sudo crm status			

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com


3.6.4. Cài đặt AJiantRegistry

viettel

securitv

STT	Thực hiện
1	Trên node registry, chạy file shell script:
	\$ sudo bash install_ajiant_registry.sh
3	Nếu có các file cài đặt ajiant_registry_setup_3.3.0.deb thì sẽ được hiện ra trong danh sách file muốn cài đặt.


	Installing ajiant backend multi node Select a package file to install: ajiant_registry_setup_3.3.0.deb2667025560(bytes)			
	<0k> <cancel></cancel>			
	Lựa chọn đúng file muốn cài và chọn OK hoặc ấn Enter để tiếp tục			
4	Accept EULA, chấp nhận điều khoản cài đặt			
	Accept EULA ? End-User License Agreement ("Agreement") Last updated: July 18, 2019 Please read this End-User License Agreement ("Agreement") carefully before clicking the "I Agree" button, downloading or using "Ajiant" ("Application"). By clicking the "I Agree" button, downloading or using the Application, you are agreeing to be bound by the terms and conditions of this Agreement. This Agreement is a legal agreement between you (either an individual or a single entity) and "Ajiant" and it governs your use of the Application made available to you by "Ajiant". If you do not agree to the terms of this Agreement, do not click on the "I Agree" button and do not download or use the Application. The Application is licensed, not sold, to you by "Ajiant" for use strictly in accordance with the terms of this Agreement. License Subject to the condition that you have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("the License"): Installation and use: You shall have the non-exclusive, non-transferable right to download, install and use the Application solely for your personal, non-commercial purposes strictly in accordance with the terms of this Agreem			

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 37



5	Sau khi bộ cài DEB được unpack ra /opt/ajiant , sẽ đến phần cấu hình cài đặt VEDR Backend.					
	Enter public virtual IP to install VEDR <ok> <cancel></cancel></ok>					
	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.					
6	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					
	Found existing certificate ! Reuse certificate from the previous installation at path /opt/docker/nginx/certs/cert.crt ?					
	<yes> <no></no></yes>					
7	Trong màn hình tiến thao (trường hơn tạo mới chứng thư)					
/	Nhập CommonName (nhập tập miềp hoặc public in cửa coruct)					
	Nhập Commonivame (nhập tên miện noặc public lp của server).					
	iviac dinn la ajlant.com . Co the nhập tên miền mà agent kết nói lên server vào CommonName.					



Enter comm	on name (C	N)	
ajiant.com			
<0k>		<cancel></cancel>	
Nhập DNS SANs và IP SANs từ c	anh sách tùy ch	iọn.	
Chú ý: trong danh sách IP SANs <mark>đến server.</mark>	phái có tên miể	ên hoặc public ip để	agent có thể kế
Select DN	3 or IP SANs to g	enerate certificate	
[<mark>*</mark>] ajiant. [*] *.ajian	com domain t.com domain		
[*] localho [*] 127.0.0	st domain .1 ip		
[*] 192.168 [] 172.17.	.129.136 ip 0.1 ip		
<	0k>	<cancel></cancel>	
Néu agent kết nối qua tên miềr	n thì nhân tên m	uiền vào ô DNS SAN	
	i in mập tên n		
Enter extra	DNS SANs or IF	SANs (Leave empty	/
Enter extra to start ger	DNS SANs or IF erating certif) SANs (Leave empty Ficate)	/
Enter extra to start ger	DNS SANs or IF merating certif Nk>	<pre>> SANs (Leave empty ficate) <cancel></cancel></pre>	/
Enter extra to start ger <(DNS SANs or IF herating certif)k>	<pre>> SANs (Leave empty icate) <cancel></cancel></pre>	
Enter extra to start ger <(DNS SANs or IF herating certi1)k>	<pre>> SANs (Leave empty ficate) <cancel></cancel></pre>	
Enter extra to start ger <(Nhập thời gian hết hạn chứng t	DNS SANs or IF herating certif)k> hư theo ngày (r	<pre>> SANs (Leave empty ficate) <cancel> nặc định là 3650):</cancel></pre>	
Enter extra to start ger <(Nhập thời gian hết hạn chứng t Enter expir	DNS SANs or IF herating certi1)k> hư theo ngày (r e days	<pre>9 SANs (Leave empty ficate) <cancel> nặc định là 3650):</cancel></pre>	
Enter extra to start ger <(Nhập thời gian hết hạn chứng t Enter expir 3650	DNS SANs or IF herating certi1)k> hư theo ngày (r e days	<pre>? SANs (Leave empty ficate)</pre>	
Enter extra to start ger Nhập thời gian hết hạn chứng t Enter expir 3650	DNS SANs or IF herating certi1)k> hư theo ngày (r e days 0k>	<pre>> SANs (Leave empty ficate) <cancel> nặc định là 3650): <cancel></cancel></cancel></pre>	



	Kất quả cã cinh 2 file trong thự mục: lont loùint loonfiel						
	Kết quả sẽ sinh 2 file trong thư mục: /opt/ajiant/config/						
	- cert.crt - cert key						
	- Certiney						
	Khi tạo chứng thư thành công sẽ có thông báo như sau:						
	Common name: ajiant.com DNS SANs: ajiant.com *.ajiant.com localhost IP SANs: 127.0.0.1						
	192.168.129.136						
	Successfully generated certificate Certificate: /opt/ajiant/config/cert.crt Private Key: /opt/ajiant/config/cert.key						
	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/ajiant/config/cert_insp.crt						
	Enter inspect certificate file path or leave empty if not set						
	<ok> <cancel></cancel></ok>						
8	Chọn ip của docker registry trong danh sách (cần chọn dải nội bộ để các node VM khác truy cập)						
	Select an Ajiant registry IP ? 172.17.0.1 docker0 192.168.129.136 ens33						
	<ok> <cancel></cancel></ok>						
9	Khởi tạo registry:						

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | **40**



	Final step ! Start Ajiant registry and initialize data now ? <yes> <no> Chọn Yes để khởi tạo docker registry cho Ajiant backend.</no></yes>
10	Bộ cài multinode chỉ hỗ trợ cài đặt 2 phiên bản EDR và EDP, không hỗ trợ phiên bản EPP EDR: chỉ có tính năng của EDR EDP: có thêm tính năng Antivirus Select production type to install Choose an option and press Enter To exit, select 'Cancel' or press ESC 1 EDR (Endpoint Detection & Response) 2 EDP (EDR + AntiVirus)
	<0k> <cancel> Theo quá trình cài đặt diễn ra đến khi kết thúc thành công.</cancel>

3.7. Hướng dẫn nâng cấp hệ thống

Lưu ý trước khi nâng cấp hệ thống cần backup những file sau:

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

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

3.7.1. Mô hình AllInOne

Chú ý:

- Với mô hình AllInOne cần backup thêm file sau để phục hồi khi cần:
- /opt/docker/docker-compose.yml
- Việc nâng cấp version backend cần thực hiện lần lượt theo thứ tự 2.0.0 -> 3.0.0 -> 3.1.0 ->
 3.3.0

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 41



- File bộ cài backend vừa sử dụng vừa để cài mới vừa để nâng cấp từ version cũ.
- Khi thực hiện nàng cấp, các files agent của nhóm update release sẽ tự động được cập nhật.
 Do đó nếu không muốn update agent hàng loạt thì khuyến nghị tạo nhóm update khác (ví dụ: pre_release), sau đó chuyển tất cả agents sang nhóm pre_release, rồi mới chuyển dần các agent sang nhóm release.

Cụ thể như sau:

Bước	Tên	Thực hiện				
1	Kiểm tra tài	Yêu cầu ổ cứng còn trống khoảng 10 GB trở lên.				
	thống cũ	Kiểm tra ổ cứng trống bằng lệnh:				
	_	\$ df -h				
2	Chạy script cài đặt	Copy các files sau lên server đặt cùng 1 thư mục setup: - install_vedr_backend.sh - vedr_backend_setup_3.3.0.deb				
		Vào thư mục setup ở trên, chạy script:				
		\$ sudo bash install_vedr_backend.sh				
		Nếu có các file cài đặt vedr_backend_setup_3.3.0.deb thì sẽ được hiện ra trong danh sách file muốn cài đặt.				
		Select a package file to install:				
		<pre>vedr_backend_setup_3.3.0.deb2185408896(bytes)</pre>				
		<0k> <cancel></cancel>				
		Lựa chọn đúng tile muốn cài và chọn OK hoặc ấn Enter để tiếp tục.				



		Trong quá trình nâng cấp, trình cài đặt phát hiện có phiên bản backend được cài trước đó, cần xác nhận có dừng tất cả dịch vụ lại trước khi cài bản mới không (chọn YES) Warning ! Found existing docker-compose.yml at /opt/docker/docker-compose.yml Stop existing VEDR backend before installing the newer version ? <yes></yes>			
3	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. Accept EULA ? End-User License Agreement ("Agreement") Last updated: July 18, 2019 Please read this End-User License Agreement ("Agreement") carefully before clicking the "I Agree" button, downloading or using "Ajiant" ("Application"). By clicking the "I Agreee" button, downloading or using the Application, you are agreeing to be bound by the terms and conditions of this Agreement. This Agreement is a legal agreement between you (either an individual or a single entity) and "Ajiant" and it governs your use of the Application made available to you by "Ajiant". If you do not agree to the terms of this Agreement, do not click on the "I Agree" button and do not download or use the Application. The Application is licensed, not sold, to you by "Ajiant" for use strictly in accordance with the terms of this Agreement. License Subject to the condition that you have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights ("the License"): Installation and use: You shall have the non-exclusive, non-transferable right to download, install and use the Application solely for your personal, non-commercial purposes strictly in accordance with the terms of this Agreement. Termination of the License: The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the MON			
4	Chọn phiên bản backend để cài đặt	 File vedr_backend_setup_3.3.0.deb hỗ trợ cà đặt 2 phiên bản EDR và EDP: EDR: chỉ có tính năng của EDR EDP: có thêm tính năng Antivirus 			

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

		Select production type to install Choose an option and press Enter To exit, select 'Cancel' or press ESC 1 EDR (Endpoint Detection & Response) 2 EDP (EDR + AntiVirus) <0k>
5	Nhập địa chỉ của server	Sau khi bộ cài DEB được unpack ra /opt/docker , sẽ đến phần cấu hình cài đặt VEDR Backend.
6	Khởi tạo chứng thư (certificate) cho hệ thống	 Nếu quá trình cài đặt phát hiện chứng thư cũ đã tồn tại khi nâng cấp version backend Chọn Yes nếu muốn dùng chứng thư cũ (recommend) Chọn No nếu muốn thiết lập lại chứng thư mới



	1	
		Found existing certificate ! Reuse certificate from the previous installation at path /opt/docker/nginx/certs/cert.crt ? <pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre> <pre> </pre>
7	Tạo bộ cài đặt agent	Khi được xác nhận tạo bộ cài agent không, chọn Yes để tiếp tục. Final step: Build agent installer Build agent installer now ? Yfes: <no> Nhập phiên bản bộ cài agent hoặc ấn Enter để lấy phiên bản mặc định tự sinh VEDR build version: 3.3.0 <0k> <0k></no>
		Chờ khoảng 10 phút để build bộ cài agent (<i>build agent windows có thể đến 5 phút 1 lần build do phải khởi động máy ảo virtual box</i>) Nếu quá trình cài đặt thành công, sẽ sinh ra 2 file MSI (cho windows), 1 file DEB, 2 files RPM và 1 file DMG trong thư mục: /opt/docker/repo/public/ - ajiant_windows_3.3.0_x64_full.msi - ajiant_windows_3.3.0_x86_full.msi - ajiant_ubuntu_3.3.0_x64_full.deb - ajiant_centos7_3.3.0_x64_rpm - ajiant_centos6_3.3.0_x64_rpm - ajiant_macos_3.3.0_x64_full.dmg

Page | **45**



8	Khởi động server vedr backend	Final step ! Start VEDR server now ? <yes> <no> 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</no></yes>
9	Khởi tạo dữ liệu database	Initializing data ! Initializing data on the first instalation ? Initializing data base Initializing data

Page | **46**



		Change portal password Enter root password: <0k> <cancel></cancel>
		Xác nhận password đã nhập
		Change portal password Confirm root password: <0k> <cancel></cancel>
10	Kiểm tra lại	Khi khởi động thành công, chạy script sau để kiểm tra các dịch vụ:
	cac dịch vụ đang chạy, các	\$ cd /opt/docker \$ sudo docker-compose ps
	port ket nor	Ноặс
		\$./list-containers.sh
		Nếu tất cả các service ở trạng thái "UP" là OK.

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

ubuntu@ajiant-autotest-aio	:/opt/docker\$./list-containers.sh	1	
Name	Command	State	Ports
ControlServer HelpDesk MicroApi MicroNeb agent_management agent_policy_manager alert app_control artifact_handler artifact_handler artifact_handler artifact_handler consul consul containment containment control_server carrelation cronjobs crontab	/ControlServer python /HelpbeskRepeater.py /microregistry=consul api /microregistry=consul /msAgentDicityManagent /msAgentDicityManager /msApentUpdateManager /msApentUpdateManager /msApentUpdateManager /msAuthentLeation /bin/sh -c /bls_log_parser sh run.sh /docker-entrypoint.sh cass /docker-entrypoint.sh cass /docker-entrypoint.sh cass /docker-entrypoint.sh cass /bin/bash /entrypoint-cron /bin/bash /entrypoint-cron	Up Up Up Up Up Up Up Up Up Up Up Up Up	7000/tcp, 7001/tcp, 7199/tcp, 127.0.0.1:9042->9042/tcp, 9160/tcp
<pre>deploy_tool handler endpoint_firewall es event_handler group_management haproxy irflow logstash logstash_correlation logstash_evt_collector mongo nats1 nats2 nats3_req_handler nginx process_analysis rabbitmq redis2 response_scenario_handler siem_api ved_web.vescc vedr_web.vescc vedr_portal ved_query_parser_api ves_log_parser</pre>	<pre>/#sDeployToolHandler /#sEndpointFivHandler /#sEndpointFivHandler /#sEventHandler /docker-entrypoint.sh hapr /msIRFlow /LiveResponse /docker-entrypoint.sh -f / /docker-entrypoint.sh -f / /docker-entrypoint.sh -f / /docker-entrypoint.sh - p 24 docker-entrypoint.sh - p 24 docker-entrypoint.sh - p 34 /msNatSRedHandler /bin/sh - c crond && nginx /ProcessAnalysis docker-entrypoint.sh rabbi docker-entrypoint.sh rabbi docker-entrypoint.sh rabbi docker-entrypoint.sh rabbi docker-entrypoint.sh rabbi docker-entrypoint.sh redis docker-entrypoint.sh redis docker-entrypoint.sh redis docker-entrypoint.sh redis docker-entrypoint.sh redis /wer.web.sccketio /vedr.web.vescc gunicorm -v 1 -b 127.0.9.1 /bin/sh -c nde index.js /VESLogParser</pre>	. 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	127.0.0.1:27017->27017/tcp, 28017/tcp 127.0.0.1:6379->6379/tcp 127.0.0.1:6380→6379/tcp
Kiểm tra các p	oort dịch vụ:		
\$ telnet <pub \$ telnet <pub \$ telnet <pub \$ telnet <pub \$ telnet <pub \$ telnet <pub< th=""><th>LIC_IP> 8888 LIC_IP> 5672 LIC_IP> 80 LIC_IP> 443 LIC_IP> 4443 LIC_IP> 8443</th><th></th><th></th></pub<></pub </pub </pub </pub </pub 	LIC_IP> 8888 LIC_IP> 5672 LIC_IP> 80 LIC_IP> 443 LIC_IP> 4443 LIC_IP> 8443		
Thử vào porta bản theo tài li	Il đăng nhập vào h ệu test UAT.	iệ th	ống và kiểm tra một số tính năng cơ

3.7.2. Mô hình MultiNode

Với mô hình MultiNode hiện tại chỉ hỗ trợ cài mới, chưa hỗ trợ nâng cấp hệ thống.

Khi nâng cấp cần đội giải pháp tham gia thực hiện.

3.8. 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, <mark>khuyến nghị sử dụng cách</mark> <mark>kích hoạt license offline</mark> theo các bước sau:

Bước	Tên	Thực hiện			
1	Tạo license	Gửi các thông tin qua email cho PM của dự án:			
	key cho từng khách hàng	 Họ tên, số điện thoại và địa chỉ email của đầu mối bên khả 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 đà license	Lưu ý: họ tên của đầu mối bên khách hàng sẽ hiển thị trên trang thông tin license		
		📶 AJIANT	License Informa	tion	×
		About VCS-aJiant	 Your license is activa 	ated.	Upgrade License
		License Information	CUSTOMER NAME	₽hạm Công Hiếu	
		Account	THE NUMBER OF AGENTS	3000	
		Information	STARTED DATE	2021/02/01 17:52:01	
		Change Password	EXPIRED DATE	2031/01/30 17:52:01	
			© Copyright of Viettel (license.viettelcybersec	yber Security – Branch of Viettel Group. For r urity.com	nore information, please visit
2	Lấy token	Đăng nhập portal V Information > Enter	CS-aJiant, click v r your license > (ào icon thông tin U Offline activation	lser > License

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



			x
		🔃 ΔΙΙΔΝΤ	C License Information
		About VCS-aJiant	License is required. You need a license to access the full features of VCS-aJiant. You can get an Enter your license
		License Information	activation key from VCS-aJiant license management (http://license.viettelcybersecurity.com).
		Account	
		Information	
		Change Password	
			© Copyright of Viettel Cyber Security – Branch of Viettel Group. For more information, please visit license.viettelcybersecurity.com
		License Activat	ion ×
		 Direct activati 	on Offline activation
		You can enter your an activation key fo	license key to get an activation request token, then use this token to obtain or importing into VCS-aJiant.
		1 Enter your li	icense kev here:
			Get token
		2 You need al	icense to access the full features of VCS-a light. You can get an activation key
		from VCS-aJ	liant license management (http://license.viettelcybersecurity.com).
		3 Import your	activation key into VCS-aJiant.
		Enter your lie	cense key Browse Import activation key
		Nhập license ke	y vào Enter your license key here , click nút Get token, hệ
		thống sẽ cho tải	i về file offline_request.txt
3	Kích hoạt	Gửi file offline	request.txt cho PO để PO tạo tiếp activation key dưới dạng
	license	1 file text.	
		Sau khi PO gửi l	ại activation key, import file text chứa activation key vào
		mục Import you	ur activation key into VCS-aJiant

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com 

L	icense Activation	\times
C	Direct activation Offline activation 	
Y. a	ou can enter your license key to get an activation request token, then use this token to obta n activation key for importing into VCS-aJiant.	in
	1 Enter your license key here:	
	Enter your license key Get token	
	You need a license to access the full features of VCS-aJiant. You can get an activation a from VCS-aJiant license management (http://license.viettelcybersecurity.com).	œy
	3 Import your activation key into VCS-aJiant.	
	RwuzfTKcTYCjiRVuUgPLDLL Browse	У

3.9. Đăng nhập Portal

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

https://<ajiant-ip>

	AJIANT
Username	\boxtimes
Password	Ð
	LOGIN
	LOON

Đăng nhập bằng tài khoản quản trị đã được cung cấp

3.10. 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/

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



Index of /repo/

<u>/</u>		
<u>release/</u>	28-Dec-2021 10:33	-
<pre>ajiant_centos6_3.3.0_x64_full.rpm</pre>	28-Dec-2021 11:04	52827752
<pre>ajiant_centos7_3.3.0_x64_full.rpm</pre>	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
<pre>ajiant_windows_3.3.0_x64_full.msi</pre>	28-Dec-2021 11:03	67727360
<u>ajiant_windows_3.3.0_x86_full.msi</u>	28-Dec-2021 11:03	63311872

3.11. Hướng dẫn cài đặt các thành phần của mô hình MSSP

3.11.1. Cài đặt server forwarder

Liên hệ Phòng Hạ Tầng & Công Nghệ của VCS để lấy hướng dẫn triển khai server forwarder.

3.11.2. Cài đặt agent

Khi cài đặt agent MSSP, chọn Next 3 lần, đến bước Settings config:

Ajiant Setup		-)
Settings config				
Input config for settings and then clic	c next to continue.			
Config:				
Server IP Address:				_
Customer ID:				
Certificate file full path:				
	Back	Next	Cano	cel

Nhập các thông tin sau:

- Server IP Address: nhập ip forwarder
- Customer ID: nhập ID của khách hàng đã được cấp

- Certificate file full path: nhập đường dẫn ip forwarder được sinh ở bước trước

Các bước còn lại thực hiện như cũ.

3.12. Hướng dẫn thay certificate cho Portal

<mark>Chú ý: hướng dẫn thay certificate cho portal sau chỉ áp dụng với bộ cài AllInOne phiên bản 3.3.0</mark> Các bước thực hiện thay certificate cho portal:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



- Bước 1: Copy cert mới (bao gồm 1 file .key và 1 file .crt) vào thư mục /opt/docker/tools/change_portal_cert/
- Bước 3: vào thư mục change_portal_cert gõ lệnh:
 \$ cd /opt/docker/tools/change_portal_cert/
 \$ sudo bash change_portal_cert.sh
 Output hiện "Nginx restarted" tức là đã thay cert thành công

4. HƯỚNG DẪN CÀI ĐẶT AGENT

4.1. Hướng dẫn cài đặt trên Windows

4.1.1. Yêu cầu đảm bảo cài đặt

<u>Hệ điều hành:</u>

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)

4.1.2. Hướng dẫn cài đặt

a. Với bộ cài cho server on premise

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/

<u>··/</u>		
<u>release/</u>	28-Dec-2021 10:33	-
<pre>ajiant_centos6_3.3.0_x64_full.rpm</pre>	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
<u>ajiant_windows_3.3.0_x86_full.msi</u>	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 <u>https://<server-ip>/repo/</u> theo version mới nhất.

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



Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



🛃 Ajiant Setup		_			×
Destination Folder					
Click Next to install to the default folder or o	dick Change to	choose anothe	er.		S
Install Ajiant to:					
C:\Program Files\Ajiant\					
Change					
	Bade	Naut	1	6	
	Back	Next		Cano	el
🛃 Ajiant Setup		_	-		×
Ready to install Ajiant		-	-		×
Ajiant Setup Ready to install Ajiant Click Install to begin the installation. Click B installation settings. Click Cancel to exit the	ack to review o e wizard.	or change any o	- of your		×
Ready to install Ajiant Click Install to begin the installation. Click B installation settings. Click Cancel to exit the	ack to review o e wizard.	or change any o	- of your		×
Ready to install Ajiant Click Install to begin the installation. Click B installation settings. Click Cancel to exit the	ack to review o e wizard.	or change any o	- of your		×





b. Với bộ cài cho server MSSP

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.

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 và file certificate xuống các máy cần cài đặt. Cấu hình tham số cài đặt cho bộ cài VCSaJiant như sau:

Msiexec.exe /i <setup_file>.msi IP="<Server_IP>" ID="<Customer_ID>" CERT="<Cert_File_FullPath>" /qn

Trong đó:

- Setup_file: là tên file msi được đẩy xuống máy
- Server_IP: là địa chỉ IP của server forwarder
- Customer_ID: là ID của khách hàng, được cung cấp sẵn
- Cert_File_FullPath: là đường dẫn fullpath của file certificate.

Ví dụ: Msiexec.exe /i Ajiant_3.3.0_x64.msi IP="1.2.3.4" ID="VCS" CERT="c:\certificate\vcs.crt" /qn

Cài đặt trực tiếp:

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi

T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | 56



B1. Tải bộ cài (x86 và x64) thông qua địa chỉ <u>https://<server-ip>/repo/</u> theo version mới nhất.
 B2. Click đúp bộ cài, tiến hành cài đặt theo các bước (cần quyền administrator để thực hiện cài đặt)

访 Ajiant Setup	
< Contract of the second secon	Welcome to the Ajiant Setup Wizard
	The Setup Wizard will install Ajiant on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
	Back Next Cancel
闄 Ajiant Setup	
End-User License Agreen Please read the following lice	nent ense agreement carefully
English Version: End-User License Agr Last updated: July 18, Please read this End- carefully before clickin using "Ajiant" ("Applic By clicking the "I Agre Application, you are a conditions of this Agre This Agreement is a lo individual or a single	eement ("Agreement") , 2019 User License Agreement ("Agreement") ng the "I Agree" button, downloading or sation"). ee" button, downloading or using the greeing to be bound by the terms and eement. egal agreement between you (either an entity) and "Ajiant" and it governs your cense Agreement
	Print Back Next Cancel

Viettel Cyber Security



🗒 Ajiant Setup	
Destination Folder Click Next to install to the default folder or dick Change to choose another.	
Install Ajiant to:	
C:\Program Files\Ajiant\ 	
<u>B</u> ack Next	Cancel

Nhập các thông tin cài đặt:

- Server IP Address: là địa chỉ IP của server forwarder
- Customer ID: là ID của khách hàng, được cung cấp sẵn
- Certificate file full path: là đường dẫn fullpath của file certificate.

😸 Ajiant Setup		×
Settings config		
Input config for settings and the	en dick next to continue.	
Config:		
Server IP Address:	12.3.4	-
Customer ID:	lvcs	
Certificate file full path:	C:\certificate\vcs.crt	
	Rade Novet Cancel	





Please wait while the Setup Wizard installs Ajiant.

Status:

<u>B</u>ack Cancel Next





4.1.3. Kiểm tra cài đặt

B1. Đăng nhập vào portal tập trung

English
Sign in Utername
Password Estroit yout password? Sign in
Version 3.3.0 (packe:) © 2021 Vetter Cyber Security - Branch of Vettel Group

B2. Vào mục quản lý agent (Agent Management)

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 60



Image: Control Image:		tting / Agent man	agement											
Image: State in the s	Agent management													Guidelia
Concern Concern <t< th=""><th>Type to search by queries</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>First Ping</th><th></th><th>Last Ping</th><th></th></t<>	Type to search by queries										First Ping		Last Ping	
Image: control Image: contro Image: control Image: c	6 result(s)											Ł. Vi	w column	~
Image: States Image: S	C1 NAME		STATUS	GROUP	UPDATE GROUP	LAST PING		FIRST PING	8	IP DCN	POLICY		VERSIO	
Name Norm Norm <th< td=""><td>Aliant-Agent-Ubunt</td><td>userver18</td><td>Offline</td><td>Default</td><td>Release</td><td>28/12/2021 10:25:08</td><td>5</td><td>17/12/2021 11:14:10</td><td>-</td><td>10.255.250.107</td><td>full_features</td><td>5</td><td>3.3.0</td><td></td></th<>	Aliant-Agent-Ubunt	userver18	Offline	Default	Release	28/12/2021 10:25:08	5	17/12/2021 11:14:10	-	10.255.250.107	full_features	5	3.3.0	
Nume Nume <th< td=""><td>C Centos6</td><td></td><td>Offline</td><td>Default</td><td>Release</td><td>29/12/2021 15:18:39</td><td>9</td><td>29/12/2021 13:35:56</td><td></td><td>10.61.188.2</td><td>full_features</td><td>s</td><td>3.3.0</td><td></td></th<>	C Centos6		Offline	Default	Release	29/12/2021 15:18:39	9	29/12/2021 13:35:56		10.61.188.2	full_features	s	3.3.0	
Network Network <t< td=""><td>Phulas-Mac-Mini.Lo</td><td>cal</td><td>Offline</td><td>Default</td><td>Release</td><td>27/12/2021 10:16:33</td><td>3</td><td>27/12/2021 09:59:10</td><td></td><td>10.61.188.2</td><td>test_av</td><td></td><td></td><td></td></t<>	Phulas-Mac-Mini.Lo	cal	Offline	Default	Release	27/12/2021 10:16:33	3	27/12/2021 09:59:10		10.61.188.2	test_av			
Image Image <th< td=""><td>Aliant-Agent-Centos</td><td>s7 testhostname</td><td>Offline</td><td>Default</td><td>Release</td><td>28/12/2021 10:28:32</td><td>2</td><td>17/12/2021 15:46:54</td><td></td><td>10.255.250.93</td><td>full_features</td><td>s</td><td>3.3.0</td><td></td></th<>	Aliant-Agent-Centos	s7 testhostname	Offline	Default	Release	28/12/2021 10:28:32	2	17/12/2021 15:46:54		10.255.250.93	full_features	s	3.3.0	
ordine Bute Nue BLIDBELIDER DUIDELIDER DUIDELIDER Service Se	SETTING		Online	Default	Release	30/12/2021 18:16:27	7	17/12/2021 15:12:22		10.255.250.51	full_features	5	3.3.0	
Aver memory is a constrained by a constrain	Policy setting		Offline	Default	Release	20/12/2021 17:29:36	5	20/12/2021 15:36:48		10.61.188.2	default			
Save Info Network Interfaces MOST MAME DESKTOP-13NBN8F 169.254.154.10.3 HOST D0 9d53cf6e-9c30-4184-addb-deb50b44cade 1P V4 169.254.154.10.3 SETUP VERSION N/A 00ff52:25c.idde9 SETUP VERSION N/A 00ff52:25c.idde9 PLATFORM Microsoft Windows 10 Education 1P V4 169.254.218.473a.4 PLATFORM VERSION 10.0.17134 Build 17134 1PV 4 169.254.97.116 PLATFORM FAMILY Standalone Workstation 1P V4 169.254.97.116 PLATFORM FAMILY Standalone Workstation 1P V4 169.254.97.116 OFFault Gateway 388,608 192.168.1.1 CORES 4 00.00000 192.168.1.1 MODEL NAME Intel(R) Core(TM) 15-6200U CPU @ 2.3006HZ 203.113.188.1 203.113.188.1	Agent DESKTOP Agent DESKTOP Agent ID 2F225A3253 First ping: 18/06/2011 POLICY UPDATE GROUP	hông t -13NBN 229FDEC1 9 15:16:26 Select ar release	Ein máy BF 2E0C34F5BCI Last pin n Option	イ Vừa Cài (19 - 19 - 19 - 19 - 19 - 19 - 19 - 19 -	đặt 22:40	· · · · · · · · · · · · · · · · · · ·							• ON	LINE
HOST NAME DESKTOP-13NBN8F HOST NAME DESKTOP-13NBN8F HOST NAME 9d53cf6e-9c30-4184-ad4b-deb50b44cade NA N/A SETUP VERSION N/A N/A IP V4 169.254.243.164 MAC 1P V4 169.254.243.164 N/A IP V4 169.254.243.164 IP V4 169.254.97.116 IP V4 IP V4 169.254.97.116 IP V4	Info	Jave				Ne	etwork In	terfaces						
HOST ID 9d53cf6e-9c30-4184-ad4b-deb50b44cade MAC 00:ff:82:c5:dd:e9 SETUP VERSION N/A IP V6 fe80:::88ec:429c:34d8:9a67 OS windows IP V6 fe80:::88ec:429c:34d8:9a67 OS windows IP V6 fe80:::88ec:429c:34d8:9a67 IP V6 fe80:::88ec:429c:34d8:9a67 IP V6 fe80:::801:9da8:2f8a:16a IP V6 fe80:::801:9da8:2f8a:16a IP V6 fe80:::801:9da8:2f8a:16a IP V6 fe80:::91:901:9da8:2f8a:16a IP V6 fe80:::91:94:2f3:164 IP V6 fe80:::91:94:2f3:164 IP V6 fe80:::91:84:b7:41:2167:6174 IP V6 fe80:::91:84:b7:41:2167:6174 IP V6 fe80:::91:94:f2:3:c1 Default Gateway 192:168.1.1 PHYSICAL MEMORY 8;388,608 192:168.1.1 CORES 4 203:113.188.1 MHZ 2400.00000 105:2000 CPU @ 2.30GHZ MODEL NAME Intel(IP) Core(TM) 15-62000 CPU @ 2.30GHZ 203:113.131.3	HOST NA	ME DES	KTOP-13NB	N8F				IP V4	169.254	.154.103				
HOSTID 9d53cf6e-9c30-4184-ad4b-deb50b44cade MAC 00:ff:82:c5:dd:e9 SETUP VERSION N/A IP V4 169.254.243.164 OS windows IP V4 169.254.243.164 PLATFORM Microsoft Windows 10 Education MAC 00:ff:82:c5:dd:e9 PLATFORM VERSION 10.0.17134 Build 17134 MAC 00:ff:82:c5:dd:e9 PLATFORM VERSION 10.0.17134 Build 17134 IP V4 169.254.97.116 PLATFORM VERSION 10.0.17134 Build 17134 IP V6 fe80::9184:b741:2167:6174 IP V5 5tandalone Workstation MAC 04:02:b9:df:23:c1 PHYSICAL MEMORY 8,388,608 192:168.1.1 CORES 4 200.00000 203.113.188.1 MMC 203.113.131.3 203.113.131.3								IP V6	fe80::88	ec:429c:34d8	:9a67			
SETUP VERSION N/A Ethernet 2 NAME Ethernet 2 IP V4 169.254.243.164 IP V4 169.254.243.164 IP V6 fe80::5601:9da8:2f8a:f3a4 MAC 00:ff:ae:e0:5c:99 PLATFORM Microsoft Windows 10 Education PLATFORM VERSION 10.0.17134 Build 17134 PLATFORM FAMILY Standalone Workstation ARCHITECTURE amd64 PHYSICAL MEMORY 8,388,608 192.168.1.1 DEfault Gateway CORES 4 MHZ 2400.00000 MODEL INAME Intel(R) Core(TM) 15-6200U CPU @ 2.30GHZ MODEL INAME Intel(R) Core(TM) 15-6200U CPU @ 2.30GHZ	HOST	ID 9d5	3cf6e-9c30-4	184-ad4b-deb50	b44cade			MAC	00:ff:82:	c5:dd:e9				
SETUP VERSION N/A OS windows IP V4 169.254.243.164 IP V6 fe80::5801:9da8:2f8a:f3a4 IP V6 fe80::5801:9da8:2f8a:f3a4 MAC 00:ff:ae:e0:5c:99 NAME Ethernet 6 IP V4 169.254.243.164 IP V6 fe80::5801:9da8:2f8a:f3a4 MAC 00:ff:ae:e0:5c:99 NAME Ethernet 6 IP V4 169.254.97.116 IP V6 fe80::9184:b741:2167:6174 IP V6 fe80::9184:b741:2167:6174 MAC a4:02:09:df123:c1 Default Gateway 192.168.1.1 PHYSICAL MEMORY 8,388,608 192.168.1.1 CORES 4 203.113.188.1 MMZ 2400.00000 2.30GHz MODEL INAME Intel((R) Core(TM) I5-6200U CPU @ 2.30GHz 203.113.131.3								NAME	Etherne	t 2				
OS windows PLATFORM Microsoft Windows 10 Education PLATFORM VERSION 10.0.17134 Build 17134 PLATFORM VERSION 10.0.17134 Build 17134 PLATFORM FAMILY Standalone Workstation ARCHITECTURE amd64 PHYSICAL MEMORY 8,388,608 CORES 4 ARCHITECTURE 192.168.1.1 DNS Server DNS Server CORES 4 MHZ 2400.00000 MODEL INAME Intel(R) Core(TM) 15-6200U CPU @ 2.30GHZ NEUROPE INFORMENTED 203.113.131.3	SETUP VERSI	ON N/A						IP V4	169.254	.243.164				
os windows in in the instrumentation of the construction of the								IP V6	fe8058	01-0da8-2f8a-	f3a4			_
PLATFORM Microsoft Windows 10 Education NAME Ethernet 6 PLATFORM VERSION 10.0.17134 Build 17134 IP V4 169.254.97.116 PLATFORM FAMILY Standalone Workstation IP V6 fe80::9184:b741:2167:6174 ARCHITECTURE amd64 MAC a4:02:b9:dfi:23:c1 PHYSICAL MEMORY \$388,608 192.168.1.1 CORES 4 203.113.188.1 MODEL INAME Intel(R) Core(TM) I5-6200U CPU @ 2.30GHz 203.113.131.3		os win	dows					MAC	00.ff.ae	-01-5c-00	1904			
Induction Induction <thinduction< th=""> Induction <thinduction< th=""> Induction <thinduction< th=""> <thinduction< th=""> <thind< td=""><td>ΡΙ ΔΤΕΟ</td><td>RM Mici</td><td>rosoft Windo</td><td>ws 10 Education</td><td></td><td></td><td></td><td>NAME</td><td>Etherne</td><td>t 6</td><td></td><td></td><td></td><td></td></thind<></thinduction<></thinduction<></thinduction<></thinduction<>	ΡΙ ΔΤΕΟ	RM Mici	rosoft Windo	ws 10 Education				NAME	Etherne	t 6				
PLATFORM VERSION 10.0.1/134 Build 1/134 IP V6 fe80:::9184:b741:2167:6174 PLATFORM FAMILY Standalone Workstation MAC a4:02:b9:df:23:c1 ARCHITECTURE amd64 Default Gateway PHYSICAL MEMORY 8,388,608 192.168.1.1 COVES 4 200.00000 203.113.188.1 203.113.131.3 MODEL NAME Intel(R) Core(TM) I5-5200U CPU @ 2.30GHz 203.113.131.3 203.113.131.3								IP V4	169.254	.97.116				
PLATFORM FAMILY Standalone Workstation ARCHITECTURE amd64 PHYSICAL MEMORY 8,388,608 PHYSICAL MEMORY 8,388,608 CPUs DVS Server CORES 4 2400,000000 203,113,188.1 MMC 203,113,131.3	PLATFORM VERSI	ON 10.0	.17134 Build	17134				IP V6	fe80::91	84:b741:2167	:6174			
ARCHITECTURE amd64 Default Gateway PHYSICAL MEMORY 8,388,608 192.168.1.1 CPUs DNS Server DNS Server CORES 4 203.113.188.1 MDD EL NAME Intel(R) Core(TM) I5-6200U CPU @ 2.30GHz 203.113.131.3	PLATFORM FAM	ILY Star	ndalone Worl	kstation				MAC	a4:02:b	9:df:23:c1				
PHYSICAL MEMORY 8,388,608 192.168.1.1 CPUs DNS Server CORES 4 203.113.188.1 MODEL NAME Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 203.113.131.3	ARCHITECTU	IRE amo	164			De	efault Gat	eway						
CPUs DNS Server CORES 4 203.113.188.1 MHZ 2400.000000 203.113.188.1 MODEL NAME Intel(R) Core(TM) I5-6200U CPU@ 2.30GHz 203.113.131.3	PHYSICAL MEMO	0RY 8,38	8,608			1	192.168.1.1							
CORES 4 203.113.188.1 MHZ 2400.000000 203.113.188.1 MODEL NAME Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 203.113.131.3	CPUs					DI	NS Server							
MHZ 2400.000000 MODEL NAME Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 203.113.131.3 VENOR ID Gospitalization	COR	ES 4					203.113.188	8.1						
MODEL NAME Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 203.113.131.3 VENDOR ID Gravitalistal	M	HZ 240	00.000000			4	200.110.100							
	MODEL NAM	VE Int	el(R) Core(TA	(I) i5-620011 CPU	© 2.30GHz	2	203.113.131	1.3						
	VENDOR	ID Go	nuineIntel	.,	2.2.000112									

4.1.4. 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*

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

Page | 61

L



O	Programs and Features – 🗆 X					
÷	← → × ↑ 👩 « All Control Panel Items » Programs and Features v Ö Search Programs and Features P					
	Control Panel Home	Uninstall or change a program				
	View installed updates	To uninstall a program, select it from the list and then	click Uninstall, Change, or Repair.			
•	Turn Windows features on or					
	off	Organize 🕶 Uninstall Change Repair	*== *==	□ ?		
		Name	Publisher	Installed On		
		📧 Ajiant	Viettel Cyber Security	10/1/2019		
		Microsoft OneDrive	Microsoft Corporation	10/1/2019		
		Oracle VM VirtualBox Guest Additions 5.2.6	Oracle Corporation	2/7/2018		
		<		>		
		Viettel Cyber Security Product version: 1.0 Size: 64	0.1 I.6 MB			

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



0	Programs and Features		_	
~	→ × ↑ 🛐 « All C	control Panel Items > Programs and Features v 🖸 Search	n Programs and Fea	atures 🔎
	Control Panel Home	Uninstall or change a program		
	View installed updates	To uninstall a program, select it from the list and then click Uninstall, Ch	ange, or Repair.	
•	Turn Windows features on	or		
	off	Organize 🔻 Uninstall Change Repair	· ·	
		Programs and Features		Installed On
			urity	10/1/2019
		Are you sure you want to uninstall Ajiant?	ation	10/1/2019
			511	2/1/2010
		In the future, do not show me this dialog box Yes No		
	L			
		<		>
		Viettel Cyber Security Product version: 1.0.1		
		Size: 64.6 MB		

4.2. Hướng dẫn cài đặt trên Ubuntu và CyOS

4.2.1. Yêu cầu đảm bảo cài đặt

<u>Phiên bản OS</u>: tương thích cài đặt với các máy Ubuntu 18.04 x64 Desktop, Ubuntu 18.04 x64 Server, CyOS x64

<u>Phiên bản linux kernel</u>: 4.15, 4.18, 5.0 Các phiên bản khác, VCS-aJiant sẽ thiếu hai tính năng gồm Event Log và Network Containment

Cấu hình phần cứng:

Yêu cầu tối thiểu:

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

<u>Kết nối mạng:</u>

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

L



4.2.2. Hướng dẫn cài đặt

B1. Tải bộ cài agent ubuntu thông qua địa chỉ https://<server-ip>/repo/ theo version mới nhất.

- B2. Chạy lệnh sau để cài đặt: sudo dpkg -i <đường dẫn tới package>
 - Ví dụ: sudo dpkg -i ajiant_ubuntu_3.3.0_x64.deb

<pre>File Edit View Search Terminal Help DKMS: build completed. ajiant: Running module version sanity check. Original module</pre>		thanhln9@thanhln9-VirtualBox: ~/Desktop	0 😣
DKMS: build completed. ajiant: Running module version sanity check. - Original module - No original module exists within this kernel - Installation - Installing to /lib/modules/4.15.0-29-generic/updates/dkms/ depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	File Edit View Sea	rch Terminal Help	
ajiant: Running module version sanity check. - Original module - No original module exists within this kernel - Installation - Installing to /lib/modules/4.15.0-29-generic/updates/dkms/ depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9.VirtualBox:~/Desktop\$	DKMS: build comp	leted.	
Running module version sanity check. - Original module - No original module exists within this kernel - Installation - Installing to /lib/modules/4.15.0-29-generic/updates/dkms/ depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	aiiant:		
 Original module No original module exists within this kernel Installation 	Running module ve	ersion sanity check.	
- No original module exists within this kernel - Installation - Installing to /lib/modules/4.15.0-29-generic/updates/dkms/ depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	- Original modul	le	
 Installing to /lib/modules/4.15.0-29-generic/updates/dkms/ depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$ 	- No original	module exists within this kernel	
depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	- Installing	to /lib/modules/4.15.0-29-generic/updates/d	kms/
depmod DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$			
DKMS: install completed. Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	depmod		
Install kernel module here. DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	DKMS: install cor	mpleted.	
DkmsInstall return success install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	Install kernel mo	odule here.	
install kernel module return 0 VEDRDrvSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	DkmsInstall retur	rn success	
VEDRDFVSetup return 0 Install ajiant agent successfully ! thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	install kernel mo	odule return 0	
thanhln9@thanhln9-VirtualBox:~/Desktop\$ thanhln9@thanhln9-VirtualBox:~/Desktop\$	VEDRDrvSetup retu	urn v	
thanhln9@thanhln9-VirtualBox:~/Desktop\$	thanhln9@thanhln9	9-VirtualBox:~/DesktopS	
thanhln9@thanhln9-VictualBox:~/DesktonS	thanhln9@thanhln9	9-VirtualBox:~/Desktop\$	
enannens genannens ver eageboxt verkeapy	thanhln9@thanhln9	9-VirtualBox:~/Desktop\$	

4.2.3. Kiểm tra cài đặt

Tương tự phần Windows

4.2.4. Hướng dẫn gỡ cài đặt

Chạy lệnh sau để gỡ cài đặt: sudo dpkg -r ajiant

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



thanhln9@thanhln9-VirtualBox: ~/Desktop	● 🛛 😣
File Edit View Search Terminal Help	
Version: 1.0.0 Kernel: 4.15.0-29-generic (x86_64)	
Status: This module version was INACTIVE for this kernel. depmod	
DKMS: uninstall completed.	
Deleting module version: 1.0.0 completely from the DKMS tree.	
Done. DkmsUninstall last error code 0 uninstall kernel module return 0 VEDRDrvSetup return 0	
VESSvc: no process found VESConfigurationManager: no process found VESConnectionManager: no process found VESUpdater: no process found	
VESCollector: no process found VESResponse: no process found	

4.3. Hướng dẫn cài đặt trên CentOS6 và CentOS7

4.3.1. Yêu cầu đảm bảo cài đặt

Phiên bản OS: tương thích cài đặt với các máy Centos6 và CentOS7

Phiên bản linux kernel:

- CentOS6: 2.6.32-754
- CentOS7: 3.10.0-1160, 3.10.0-1127, 3.10.0-1062, 3.10.0-957, 3.10.0-862, 3.10.0-693, 3.10.0-514

Các phiên bản khác, VCS-aJiant sẽ thiếu hai tính năng gồm Event Log và Network Containment

Cấu hình phần cứng:

Yêu cầu tối thiểu:

- o RAM 2GB
- CPU 1 core
- o 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).

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com



4.3.2. Hướng dẫn cài đặt

<u>Cài đặt bằng dòng lệnh:</u>

B1. Tải bộ cài linux thông qua địa chỉ https://<server-ip>/repo/ theo version mới nhất.

B2. Chạy lệnh sau để cài đặt: sudo rpm -i <đường dẫn tới package>

Ví dụ: sudo rpm -i ajiant_centos7_3.3.0_x64_full.rpm

centos@centos7:~/Downloads _						
File Edit View Search Terminal Help						
total 37784						
-rw-rw-r 1 centos centos 38690528 Mar 26 21:46 ajiant_centos7_1.0.2_x86_64_fu						
(contos@contos7_Downloads]\$_rnmi_aijant_contos7_1_0_2_x86_64_full_rnm						
error: cap't create transaction lock on (var/lib/rpm/ rpm lock (Permission denie						
d)						
[centos@centos7 Downloads]\$ sudo rpm -i ajiant centos7 1.0.2 x86 64 full.rpm						
[sudo] password for centos:						
Pre Install Started.						
Post Install Started.						
Created symlink from /etc/systemd/system/multi-user.target.wants/VESSvc.service						
to /usr/lib/systemd/system/VESSvc.service.						
ajiant 3.10.0-1062.el7.x86 64.ko						
ajiant_3.10.0-1127.8.2.el7.x86_64.ko						
ajiant_3.10.0-514.el7.x86_64.ko						
ajiant_3.10.0-693.el7.x86_64.ko						
ajiant_3.10.0-862.el7.centos.x86_64.ko						
ajiant_3.10.0-957.el7.x86_64.ko						
[VEDRDrvSetup]: InstallManual successfully						
[VEDRDrvSetup]: install kernel module return 0						
[VEDRDrvSetup]: VEDRDrvSetup return 0						
Install driver successfully !						
Install agent successfully !						
[centos@centos7 Downloads]\$						

4.3.3. Kiểm tra cài đặt

Tương tự phần Windows

4.3.4. Hướng dẫn gỡ cài đặt

Chạy lệnh sau để gỡ cài đặt: sudo rpm -e ajiant



centos@centos7:~

File Edit View Search Terminal Help
[centos@centos7 ~]\$ sudo rpm -r ajiant
[sudo] password for centos:
rpm: arguments to --root (-r) must begin with a /
[centos@centos7 ~]\$ sudo rpm -r ajiant
rpm: arguments to --root (-r) must begin with a /
[centos@centos7 ~]\$ sudo rpm -e ajiant
Pre Uninstall Started.
[VEDRDrvSetup]: uninstall kernel module return 0
[VEDRDrvSetup]: VEDRDrvSetup return 0
warning: file /usr/local/bin/ajiant/VESSvc.service: remove failed: No such file
or directory
Post Uninstall Started.
Uninstall Started.
Uninstall successfully.
[centos@centos7 ~]\$

4.4. Hướng dẫn cài đặt trên MacOS

4.4.1. Yêu cầu đảm bảo cài đặt

Phiên bản OS: tương thích cài đặt với các máy MacOS Catalina, Bigsur, Monterey

Cấu hình phần cứng: dùng cho Mac mini hoặc macbook đời 2016 trở về sau

<u>Kết nối mạng:</u>

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

4.4.2. Hướng dẫn cài đặt

<u>Hướng dẫn disable SIP để có thể chạy được các ứng dụng ngoài App Store.</u> B1. Restart lại máy đến khi thấy màn đen, bấm giữ phím **Command + R** để vào chế độ Recovery. Với Mac M1 thì sau khi restart, giữ phím nguồn để vào chế độ Recovery.

B2. Sau khi máy đã vào chế độ Recovery, chọn mục Utilities -> Terminal

B3. Gõ lệnh csrutil disable

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 67

п х



B4. Enter và máy hiển thị System Integrity Protection is off là đã thành công.

B5. Gõ reboot để máy khởi động lại

<u>Cài đặt bằng dòng lệnh:</u>

B1. Tải bộ cài MacOS thông qua địa chỉ <u>https://<server_ip>/repo/</u> theo version mới nhất.

B2. Click đúp vào bộ cài vừa tải về để mở giao diện Ajiant_setup như hình:



B3: Mở ứng dụng Termial, gõ lệnh theo cấu trúc:

sudo bash ./install.sh [server_address] [update_port]

Lưu ý: trong trường hợp thay đổi update_port thì cần phải nhập thêm địa chỉ update_port đang thiết lập. Nếu không thay đổi update port mặc định là 8443 thì không cần nhập địa chỉ update port. Ví dụ: *sudo bash /Volumes/ajiant_setup/install.sh 10.30.161.3*

B4. Cấp quyền cho phép phần mềm Ajiant được phép truy cập các thư mục:

Mở ứng dụng System Preferences/ Security & Privacy chọn lần lượt thứ tự các bước từ 1 đến 4 như hình:

Viettel Cyber Security

Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com Page | 68





Cài đặt hoàn tất sẽ hiển thị thông báo thành công ngay trên cửa sổ Terminal.





4.4.3. Kiểm tra cài đặt

Tương tự phần Windows

4.4.4. Hướng dẫn gỡ cài đặt

B1: Mở file ajiant_setup tại bộ cài đã tải trên server về

Finder File Edit View	Go Window Help	🕮 U.S. 🖻 🖘 🗿 Q 📓 Thu Dec 30 5:14
	●●● 〈 〉 Setup 正 0 篇 * ① ② ③ * Q; Freelts Discontin	Loged 1
	A Application A Application Dexity Dex	
	Taga a Red 0 Grange 9 Valor 9 Valor 9 Forpi	syndiapone 1732 2.291
	- 😫 🎫 🥏 📅 🥌 😑 🧮 🗃 📟 🚿 🛃 🎯 🔤 📘 🍼 🚍	

B2: Mở terminal chạy file uninstall.sh để gỡ cài đặt. Lệnh: sudo bash /Volumes/ajiant_setup/uninstall.sh

Page | 70



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

Mô hình AllinOne	Mô hình MultiNode			
Thay lại file <i>docker-compose.yml</i> vào /opt/docker/docker-compose.yml	Thay lại file <i>ajiant-stack.yml</i> vào /opt/ajiant/ajiant-stack.yml			
Chạy lệnh:	Chạy lệnh:			
\$ docker-compose up –d	\$./DeployStack.sh			
Kiểm tra lại:				
\$./list-containers.sh				
Xem các service có ở trạng thái " Up " không				
Chờ một thời gian và kiểm tra lại các thông tin sa	u:			
 Portal có đăng nhập được không ? 				
- Có agent online không ?				
- Có thấy log event gửi lên không ?				
- Kiểm tra rabbitmq management xem các log có được xử lý hết 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: <u>soc247@viettel.com.vn</u>
- Bộ phận chăm sóc khách hàng, Công ty An ninh mạng Viettel
 Email: <u>cskh_anm@viettel.com.vn</u>

Viettel Cyber Security Keangnam Building - Landmark 72, Pham Hung st., Nam Tu Liem dist., Hanoi T: (+84) 971 360 360 E: vcs.sales@viettel.com.vn | W: www.viettelcybersecurity.com

Page | **72**