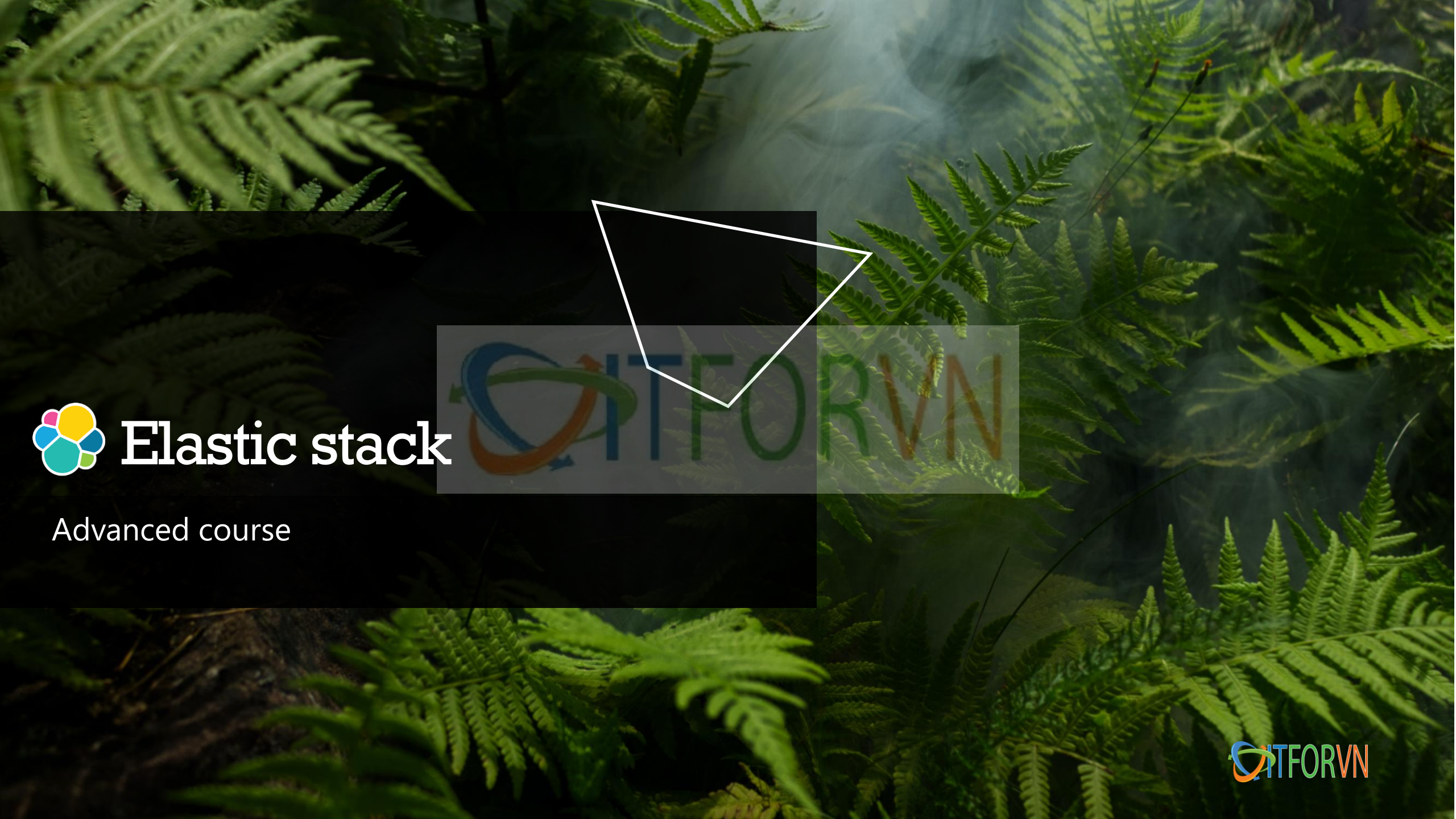
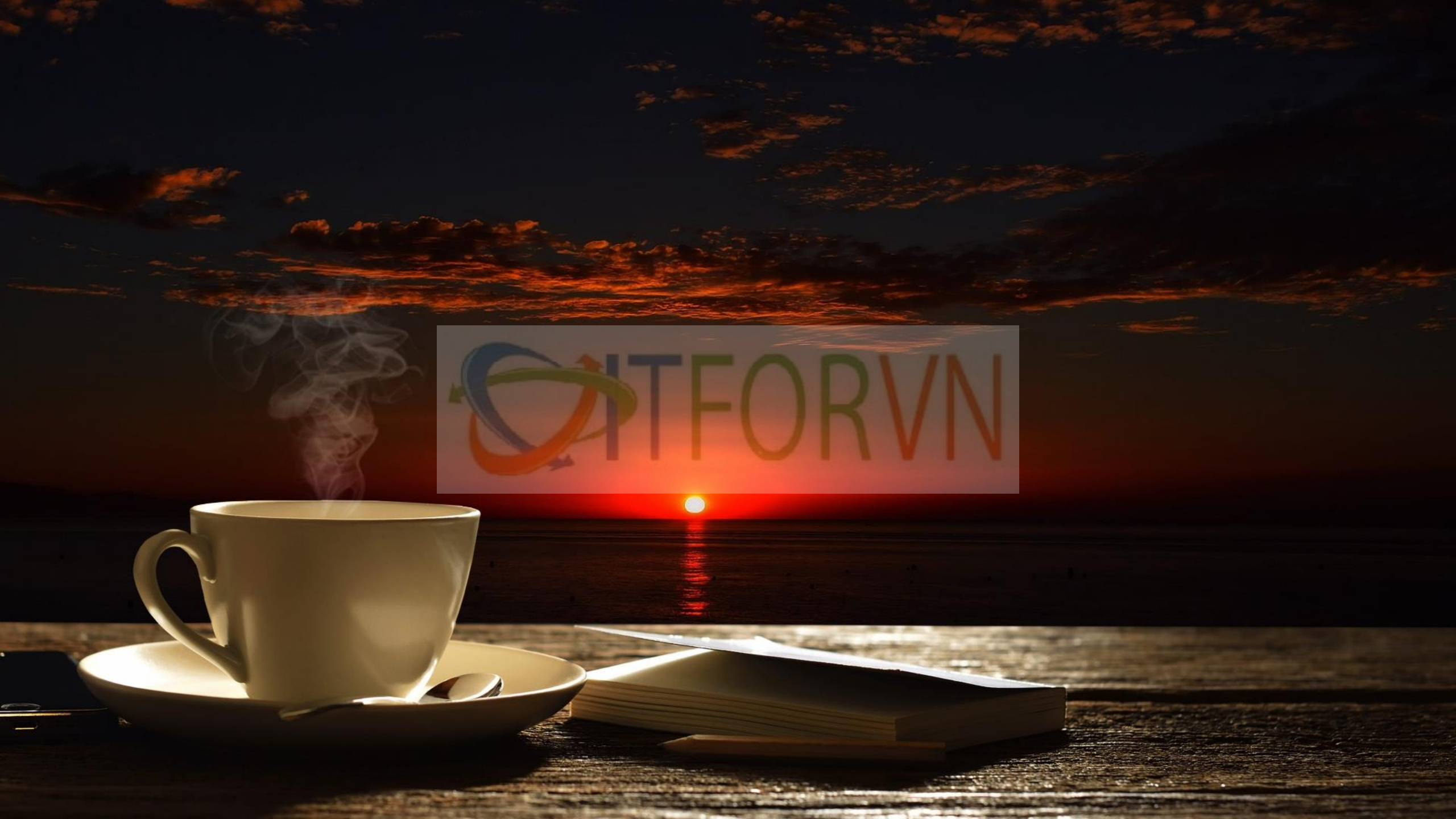


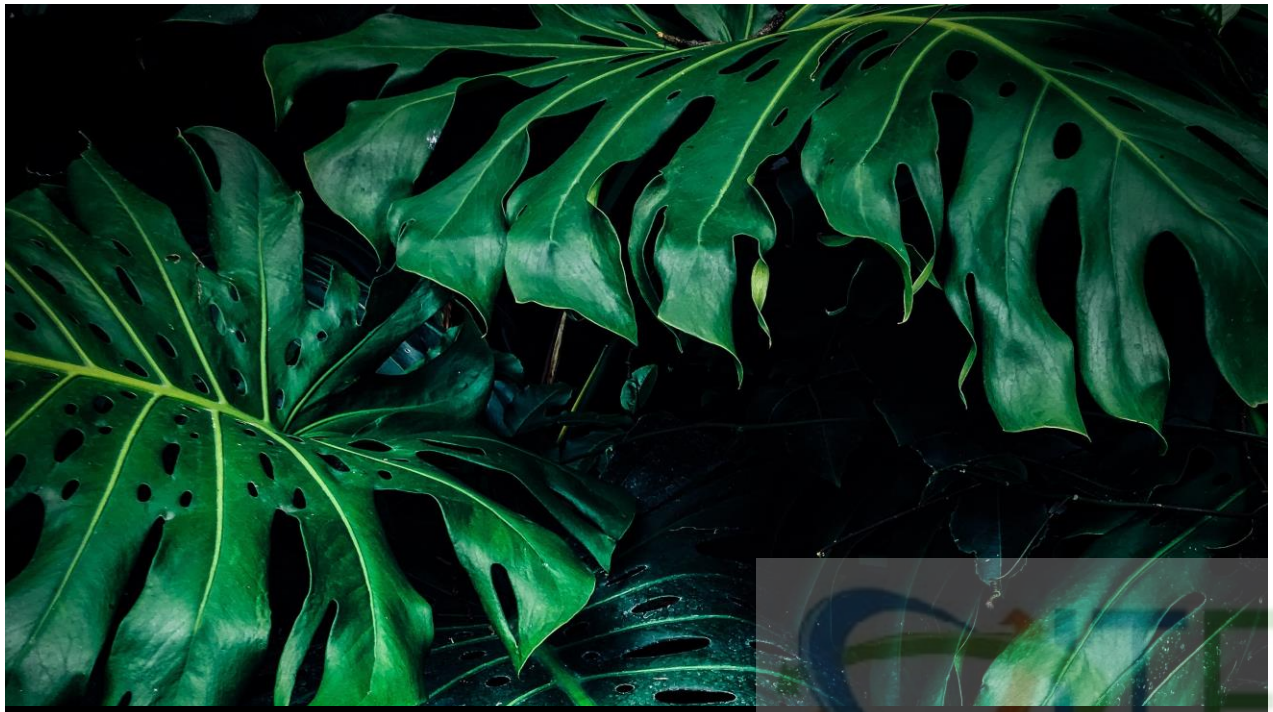
Elastic stack

Advanced course

Course contents

- Centralized Logging Management
- Logstash advanced
- Kibana advanced
- APM – Application Performance Monitoring
- Alerting


ITFORVN



01 – Centralized Logging

Centralized Logging Management

- Strategy
- Tools

Logs

- Logs – là một phần quan trọng của bất kì hệ thống nào. Cung cấp thông tin thiết yếu về cách một hệ thống đang hoạt động hiện tại, và nó đã hoạt động thế nào trong quá khứ.
- Logs cung cấp thông tin về lỗi, các vấn đề đang xảy ra, xu hướng hoạt động của ứng dụng.

```
Jul 11 15:43:10 ELK-1 sshd[24349]: Accepted publickey for ubuntu from 172.16.253.1 port 53232 ssh2: RSA SHA256:GiFydT79kgN9T
Xc45JwmFgsxkMltdRRsveWm4/s+olw
Jul 11 15:43:10 ELK-1 sshd[24349]: pam_unix(sshd:session): session opened for user ubuntu by (uid=0)
Jul 11 15:43:10 ELK-1 systemd-logind[861]: New session 20 of user ubuntu.
Jul 11 15:43:13 ELK-1 sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jul 11 15:43:15 ELK-1 sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Jul 11 15:43:15 ELK-1 sudo:   ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/su
Jul 11 15:43:15 ELK-1 sudo: pam_unix(sudo:session): session opened for user root by ubuntu(uid=0)
Jul 11 15:43:15 ELK-1 su: (to root) ubuntu on pts/1
Jul 11 15:43:15 ELK-1 su: pam_unix(su:session): session opened for user root by ubuntu(uid=0)
```

```
172.16.253.1 - - [11/Jul/2021:15:46:01 +0000] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0) Gecko/201
00101 Firefox/89.0"
172.16.253.1 - - [11/Jul/2021:15:46:01 +0000] "GET /favicon.ico HTTP/1.1" 404 134 "http://172.16.253.14/" "Mozilla/5.0 (X11; Ubuntu; L
inux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0"
172.16.253.1 - - [11/Jul/2021:15:46:11 +0000] "GET /admin.php HTTP/1.1" 404 134 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0)
Gecko/20100101 Firefox/89.0"
172.16.253.1 - - [11/Jul/2021:15:46:19 +0000] "GET /wp-admin/ HTTP/1.1" 404 134 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:89.0)
Gecko/20100101 Firefox/89.0"
```

Centralized Log Management system

- CLM – một loại hệ thống/giải pháp có nhiệm vụ hợp nhất tất cả dữ liệu log, lưu trữ, cung cấp giao diện hợp nhất cho phép truy cập dữ liệu log, phân tích, hoặc đưa ra cảnh báo. Tất cả thao tác liên quan dữ liệu log được thực hiện một cách dễ dàng, hiệu quả.

- Một hệ thống CLM có các lợi ích:
  - Hợp nhất dữ liệu log từ nhiều nguồn.
  - Thực thi chính sách lưu trữ dữ liệu log theo thời gian.
  - Tìm kiếm dữ liệu log.
  - Mô hình hóa dữ liệu log.
  - Cảnh báo dựa trên dữ liệu log.
  - Cung cấp dữ liệu log mà không cần quyền truy cập hệ thống.
  - ….

Centralized Log Management strategy

- Standard protocol
- One place for all logs
- Disk persistence
- Life-cycle of logs

Centralized Log Management solution

- Life-cycle of logs
- Syslog-ng Store Box
- Syslog-ng Open source
- Datadog
- Graylog
- SolarWinds Kiwi syslog server

syslog

Syslog – overview

- Syslog – System Logging Protocol, một giao thức tiêu chuẩn để gởi nhật ký hệ thống (system log), thông báo sự kiện đến một máy chủ (server) chỉ định – syslog server.
- Syslog mặc định có trên các thiết bị chạy Linux hoặc Unix, trên các thiết bị mạng (router, switch, firewall), trên các ứng dụng trên nền tảng Linux hoặc Unix. *(Windows không sử dụng Syslog mà sử dụng Windows Event Log riêng của Microsoft)*
- Một số đặc điểm:
  - Chỉ có thể push, không thể pull.
  - Syslog server thường là local trên chính thiết bị sử dụng syslog (syslog local).
  - Syslog server remote thường cho mục đích CLM (syslog remote).
  - Syslog remote mặc định sử dụng UDP và port 514.
- 2 standard syslog message format:
  - BSD-syslog hay legacy-syslog: RFC 3164
  - IETF-syslog: RFC 5424

Syslog – legacy structure

- <PRI> <HEADER> <MSG>
  - PRI: thông số tínht toán độ ưu tiên của message
  - HEADER: chứa các thông tin định danh về message
  - MSG: chứa thông điệp được sinh ra bởi ứng dụng
- PRI: (facility value * 8) + (severity value)
- HEADER:
  - Timestamp: *Mmm dd hh:mm:ss*
  - Hostname || IP address
- MSG:
  - Application
  - Message

- Sample: **<133>Apr 01 10:20:07 elasticsearch-01 syslogd: restart**

Syslog – IETF structure

- <HEADER> <STRUCTURED-DATA><MSG>
- HEADER:
  - PRI
  - VERSION (only be 1)
  - ISOTIMESTAMP (ISO 8601: yyyy-mm-ddThh:mm:ss+-ZONE)
  - HOSTNAME
  - APPLICATION
  - PID
  - MESSAGEID
- STRUCTURED-DATA: meta-information
- MSG: message

Syslog – softwares

- Syslog: original syslog in 1980, lightweight, nhưng không flexible.
- Rsyslog: 2004, bổ sung các tính năng advanced:
  - Listen trên UDP, TCP cho remote logging từ các nguồn khác đổ về.
  - Modules.
  - Filter message.
  - Default on modern Linux distro.
  - https://www.rsyslog.com
- Syslog-ng: 1998, “next generation”:
  - Clearly syntax.
  - Flexible.
  - Listen trên UDP, TCP cho remote logging từ các nguồn khác đổ về.
  - Best for CLM.
  - https://www.syslog-ng.com

Syslog – softwares

- Syslog: original syslog in 1980, lightweight, nhưng không flexible.
- Rsyslog: 2004, bổ sung các tính năng advanced:
  - Listen trên UDP, TCP cho remote logging từ các nguồn khác đổ về.
  - Modules.
  - Filter message.
  - Default on modern Linux distro.
  - https://www.rsyslog.com
- Syslog-ng: 1998, “next generation”:
  - Clearly configuration syntax.
  - Encrypted transport.
  - Listen trên UDP, TCP cho remote logging từ các nguồn khác đổ về.
  - Best for CLM.
  - https://www.syslog-ng.com

Syslog – rsyslog

- Sử dụng standard BSD syslog protocol (RFC 3164).
- Rsyslog bổ sung (extend) các tính năng sau từ original syslog:
  - ISO 8601 timestamp with millisecond granularity and time zone information.
  - The addition of the name of relays in the host fields to make it possible to track the path a given message has traversed
  - Reliable transport using TCP
  - Support GSS-API and TLS
  - Logging directly into various database engines.
  - Support for RFC 5424, RFC 5425, RFC 5426
  - Support for RELP
  - Support for buffered operation modes where messages are buffered locally if the receiver is not ready
  - Ccomplete input/output support for systemd journal

(ref: https://en.wikipedia.org/wiki/Rsyslog)

Syslog – message size

- BSD-syslog or legacy-syslog messages:
  - Độ dài toàn bộ "message" không vượt quá 1kB.

- IETF-syslog:
  - Độ dài toàn bộ "message" không vượt quá 64kB.

- Syslog-ng:
  - Hỗ trợ độ dài lớn, quy định bởi tham số log-msg-size(). Có giá trị mặc định là 65536 bytes, tối đa 256MB.
  - Trong hầu hết trường hợp, không nên set log-msg-size() vượt quá 10MB.

syslog-ng

syslog-ng by Quest

Syslog-ng

- Installation: **sudo apt install syslog-ng**
- Main configuration:

```
source s_net { udp(ip(172.16.253.10) port(514)); };
source s_net { tcp(ip(172.16.253.10) port(514)); };
```

- Sample:

```
destination d_local {
    file("/var/log/syslog-ng/messages_${HOST}");
};
log {
    source(s_net);
    destination(d_local);
};
```

```
destination d_local {
    file("/var/log/syslog-ng/messages_${HOST}");
    owner("root")
    group("root")
    perm(0777)
};
```

Syslog-ng – logs to remote

- Rsyslog – logs to remote syslog server:
  - TCP port 514: ***.*** **@@<remote_host>**
  - UDP port 514: ***.*** **@<remote_host>**

- Syslog-ng – logs to remote syslog server:

```
destination d_syslog_tcp {
    syslog("192.168.1.118" transport("tcp") port(514));
};
destination d_syslog_udp {
    syslog("192.168.1.118" transport(“udp") port(514));
};
```

Syslog-ng – filter

facility()	Filter messages based on the sending facility.
filter()	Call another filter function.
host()	Filter messages based on the sending host.
inlist()	File-based whitelisting and blacklisting.
level() or priority()	Filter messages based on their priority.
match()	Use a regular expression to filter messages based on a specified header or content field.
message()	Use a regular expression to filter messages based on their content.
netmask() or netmask6()	Filter messages based on the IP address of the sending host.
program()	Filter messages based on the sending application.
source()	Select messages of the specified syslog-ng OSE source statement.
tags()	Select messages having the specified tag.

(ref: https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.16/administration-guide/53)

Syslog-ng – template

```
template t_demo {
    template("${ISODATE} ${HOST} ${MESSAGE}\n");
};

template t_demo "${ISODATE} ${HOST} ${MESSAGE}\n";


destination d_file {
    file("/var/log/messages" template(t_demo));
};


destination d_file {
    file ("/var/log/messages" template("${ISODATE} ${HOST} ${MESSAGE}\n") );
};


destination d_file {
        file("/var/log/${YEAR}.${MONTH}.${DAY}/${HOST}.log");
};
```

(ref: https://www.syslog-ng.com/technical-documents/doc/syslog-ng-open-source-edition/3.16/administration-guide/57)