Auditbeat Yüklenmesi - Jump server

Bu işlemler Fizz Prod ortamında Jump Server 'a yapılmaktadır.

https://jira.etiya.com/browse/FSP-84 taskı üzerinden **Auditbeat Yüklenmesi - Jump server** yapılmaktadır.

Task hakkında açıklama ve eklentiler şu şekildedir :

Fizz prod jump serverda "auditbeat" ajanı yüklü olmadığı/çalışmadığı için loglarını göremiyoruz.

Yüklü olup olmadığını "systemctl status auditbeat" ile kontrol edebilirsiniz.

Yüklü değil ise aşağıdaki adımları takip ederek yükleyebilirsiniz

1-Download and install the public signing key:
sudo rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

2-Create a file with a .repo extension (for example, elastic.repo) in your /etc/yum.repos.d/ directory and add the following lines:
[elastic-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md

3-sudo yum install auditbeat

4-sudo systemctl enable auditbeat

5-copy "auditbeat.yml" to /etc/auditbeat/auditbeat.yml

6-copy "logstash-forwarder.crt" to /etc/auditbeat/logstash-forwarder.crt

7-sudo systemctl restart auditbeat

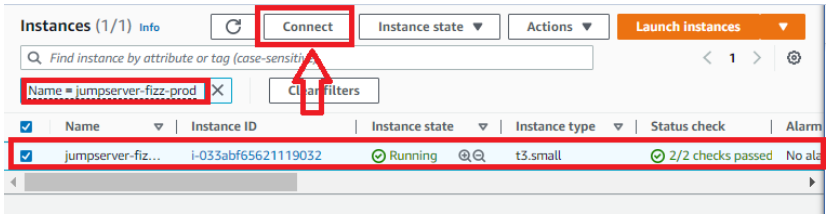
30 saniye bekleyip çalıştığından emin olmak için;
1- systemctl status auditbeat - Running gelmeli
2- journalctl -f -u auditbeat - ERROR verip crashlenen bir hata olmamalı

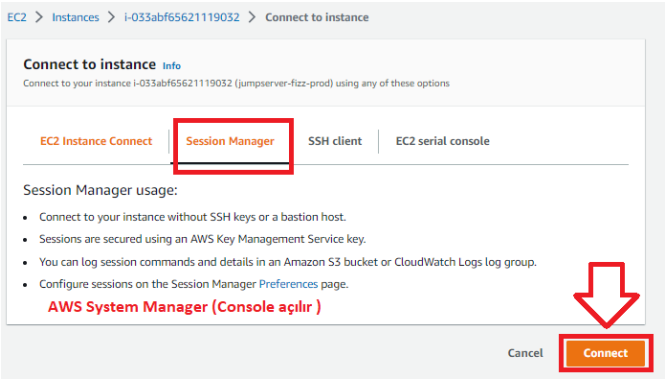

Auditbeat Yüklenmesi -JumpServer.rar


logstash-forwarder.crt


auditbeat.yml

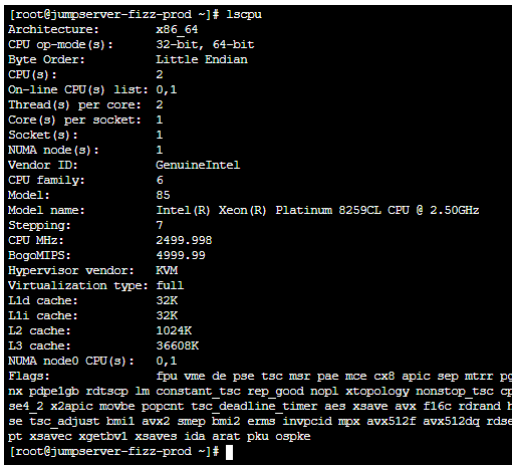
AWS Fizz Prod açılır ve **EC2 ->Instance -> jumpserver-fizz-prod** şecilere **Connect** butonuna gidilir.





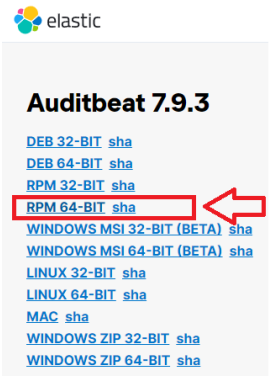
Jump Server 'ın console ekranına bağlanmak için **Session Manager -> Connect** butonuna gidilir.

- ➔ **sudo su -** (root user'a bağlanılır)
- ➔ **lscpu** (sunucunuzda bulunan işlemci veya işlemciler hakkında yararlı bilgiler sağlar. İşlemcinin mimarisini, model adını, hızını, sanallaştırma türünü ve en önemlisi de mevcut çekirdek sayısını gösterir)



- ➔ **Auditbeat** ilgili link üzerinde (https://www.elastic.co/downloads/past-releases/auditbeat-7-9-3) **lscpu** sunucunun işlemci kapasitesine göre kontrol edilerek **local** bilgisayara indirilir.

  Bu kısımda Jump Server içerisinde **Auditbeat** kurulumu yapılacağı için **rpm** uzantılı dosya indirilmiştir.



➔ **SecureCRT** üzerinden **Fizz Prod Jump Server** açılır.

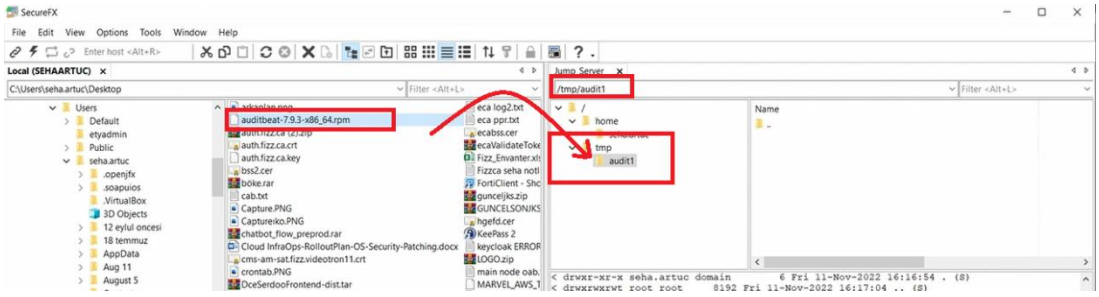
➔ **cd /tmp** (**tmp** dizinine gidilir)

➔ **mkdir autit1** (**audit1** isimli klasör oluşturulur)

➔ **Locale** bilgisayara indirilen **auditbeat-7.9.3-x86_64.rpm , auditbeat.yml , logstash-forwarder.crt** dosyaları **SecureFX** üzerinde locale 'den **Jump Server** 'ın **/tmp/audit1** dizinine atılır.


logstash-forwarder.crt


auditbeat.yml



AWS Consele Ekranı

Rpm uzantılı dosya Jump Server 'a atıldıktan sonrasında **AWS consele** ekranına gidilir.

➔ **cd /tmp/audit1** (sunucuya **rpm** uzantılı dosyanın yüklenip yüklenmediği kontrol edilir)

➔ **chown root:root auditbeat-7.9.3-x86_64.rpm** (owner ve group user **root** olarak verilir)

➔ **chown root:root auditbeat.yml logstash-forwarder.crt** (owner ve group user **root** olarak verilir)

```
[root@jumpserver-fizz-prod ~]# cd /tmp/audit1
[root@jumpserver-fizz-prod audit1]# ls -lrt
total 25712
-rw-r--r-- 1 root root 26317650 Nov 11 13:14 auditbeat-7.9.3-x86_64.rpm
```

```
[root@jumpserver-fizz-prod audit1]# ll
total 25712
-rw-r--r-- 1 root                root         26317650 Nov 11 13:14 auditbeat-7.9.3-x86_64.rpm
-rw-r--r-- 1 seha.artuc domain users      1937 Nov 11 13:34 auditbeat.yml
-rw-r--r-- 1 seha.artuc domain users      1241 Nov 11 13:34 logstash-forwarder.crt
```

➔ **rpm -ivh auditbeat-7.9.3-x86_64.rpm** (sunucuya yüklenilen rmp uzantılı dosyanın kurulumu gerçekleşir)

Not : rpm -i komutu ile paket kurulur. "**vh"** ile birlikte kullanıldığında **yükleme** işleminin ne durumda olduğunu göstermektedir.

```
[root@jumpserver-fizz-prod audit1]# rpm -ivh auditbeat-7.9.3-x86_64.rpm
warning: auditbeat-7.9.3-x86_64.rpm: Header V4 RSA/SHA512 Signature, key ID d88e42b4: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:auditbeat-7.9.3-1                ################################# [100%]
[root@jumpserver-fizz-prod audit1]#
```

➔ **systemctl enable auditbeat** (servisi devreye almak için kullanılabilir)

```
[root@jumpserver-fizz-prod audit1]# systemctl enable auditbeat
Created symlink from /etc/systemd/system/multi-user.target.wants/auditbeat.service to /usr/lib/systemd/system/auditbeat.service.
[root@jumpserver-fizz-prod audit1]#
```

➔ **systemctl stop auditbeat** (Servis durdurulur)

➔ **cd /etc/audibeat** (audibeat dizinine gidilir)

```
[root@jumpserver-fizz-prod audit1]# systemctl stop auditbeat
[root@jumpserver-fizz-prod audit1]# cd /etc/auditbeat/
[root@jumpserver-fizz-prod auditbeat]# ls -lrt
total 280
-rw-r--r-- 1 root root 212470 Oct 16  2020 fields.yml
-rw------- 1 root root   8845 Oct 16  2020 auditbeat.yml
-rw-r--r-- 1 root root  57635 Oct 16  2020 auditbeat.reference.yml
drwxr-xr-x 2 root root     40 Nov 11 13:26 audit.rules.d
[root@jumpserver-fizz-prod auditbeat]# cp auditbeat.yml auditbeat.ym_orj
```

➔ **cp auditbeat.yml auditbeat.yml_orj** (auditbeat.yml kopyalanır ve yedeği alınır)

```
[root@jumpserver-fizz-prod auditbeat]# cp auditbeat.yml auditbeat.ym_orj
[root@jumpserver-fizz-prod auditbeat]# ls -lrt
total 292
-rw-r--r-- 1 root root 212470 Oct 16  2020 fields.yml
-rw------- 1 root root   8845 Oct 16  2020 auditbeat.yml
-rw-r--r-- 1 root root  57635 Oct 16  2020 auditbeat.reference.yml
drwxr-xr-x 2 root root     40 Nov 11 13:26 audit.rules.d
-rw------- 1 root root   8845 Nov 11 13:38 auditbeat.ym_orj
```

➔ **cd /tmp/audit1** (dizinine gidilir)

➔ **cp auditbeat.yml /etc/audibeat** (auditbeat dizinindeki **auditbeat.yml** ezilir, auditbeat.yml_orj olarak yedeği alınmıştır)

➔ **cp logstash-forwarder.crt /etc/audibeat** (sertifika auditbeat dizinine kopyalanır)

➔ **systemctl start auditbeat** (servis başlatılır)

➔ **systemctl status auditbeat** (servis kontrol edilir)

```
[root@jumpserver-fizz-prod auditbeat]# systemctl start auditbeat
[root@jumpserver-fizz-prod auditbeat]# systemctl status auditbeat
● auditbeat.service - Audit the activities of users and processes on your system.
   Loaded: loaded (/usr/lib/systemd/system/auditbeat.service; enabled; vendor preset: disabled)
   Active: active (running) since Fri 2022-11-11 13:40:17 UTC; 15s ago
     Docs: https://www.elastic.co/products/beats/auditbeat
 Main PID: 21444 (auditbeat)
   CGroup: /system.slice/auditbeat.service
           └─21444 /usr/share/auditbeat/bin/auditbeat --environment systemd -c /etc/auditbeat/auditbeat.yml --pa

Nov 11 13:40:22 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:22.005Z        INFO        [auditd]
Nov 11 13:40:22 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:22.056Z        INFO        [auditd]
Nov 11 13:40:22 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:22.056Z        INFO        [auditd]
Nov 11 13:40:22 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:22.056Z        ERROR        [auditd]
Nov 11 13:40:23 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:23.554Z        INFO        [file_integri
Nov 11 13:40:26 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:26.283Z        WARN        [process]
Nov 11 13:40:26 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:26.288Z        WARN        [process]
Nov 11 13:40:26 jumpserver-fizz-prod auditbeat[21444]: 2022-11-11T13:40:26.290Z        WARN        [process]
```