SPLUNK INSTALLATION

- Splunk Enterprise Package aşağıdaki link üzerinden indirebilir ve ya wget uri ‘ı alınır.

  https://www.splunk.com/en_us/download/splunk-enterprise.html?locale=en_us

  Notes: (rpm ve ya tgz file olarak download edilebilir.)

- Splunk Kurulum paketini çalıştırmadan önce splunk ‘ı hangi user ile çalıştırmak istiyorsanız o user ‘ı oluşturmanız gerekmektedir.

  useradd splunk

  groupadd splunk (Düzeltilebilir.)

  User ‘ın oluştuğunu kontrol etmek için aşağıdaki komutu çalıştırabilirsiniz.

  cat /etc/passwd |grep splunk

- İndirmiş olduğunuz tgz ve ya rpm file aşağıdaki komutlar ile istediğiniz path ‘a çıkarabilirsiniz.

  tar -xzvf splunk-version.tgz -C /opt
  rpm -ivh splunk-version.rpm –prefix=”/opt”

- Kurulum yapacağınız path’in owner’lığını aşağıdaki komut ile değiştirmelisiniz.

  chown -R splunk:splunk /opt/splunk

- Yetkiyi verdikten sonra splunk servisini aşağıdaki komut ile ilk defa çalışmasını sağlayabiliriz. Bu aşamada administrator user ve password bilgisi istenmektedir.

  /opt/splunk/bin/splunk start –accept-license

  Splunk servis aşağıdaki best practise konfiglerin yapılması için durdurulmuştur.

  /opt/splunk/bin/splunk stop

- Linux servisinde varsayılan değerlerde kullanılan maximum process ve açılabilecek maximum dosya sayısının değiştirilmesi için /etc/security/limits.conf üzerinde aşağıdaki değişiklerin yapılması gerekmektedir.

  “https://docs.splunk.com/Documentation/Splunk/9.2.0/Troubleshooting/ulimitErrors”

For Example :

[Manager]

DefaultLimitFSIZE=-1

DefaultLimitNOFILE=64000

DefaultLimitNPROC=16000

Limit 'lerin oluştuğunu kontrol etmek için ;

ulimit -a

- Splunk servisinin reboot işlemleri sonrası otomatik olarak splunk user'ın dan başlatmak istiyorsak aşağıdaki komutu çalıştırabilirsiniz.

/opt/splunk/bin/splunk enable boot-start -user splunk

Bu komut linux sunucusu üzerinde **/etc/init.d/** altında **splunk** isminde bir dosya oluşturmaktadır.Oluşan bu dosyayı bi komutu ile açıp aşağıdaki link 'den yararlanıp güncelleyebilirsiniz.

"https://docs.splunk.com/Documentation/Splunk/9.2.0/Admin/ConfigureSplunktostartatboottime"

RETVAL=0
USER=splunk //Eklenecek olan satır//

- Linux sunucuları üzerinde yer alan Transparent Hugepege (THP) kısıtlamasını kaldırmak için link'te yer alan değişiklik yapılmaktadır.

"https://community.splunk.com/t5/Monitoring-Splunk/How-do-I-disable-Transparent-Huge-Pages-THP-and-confirm-that-it/m-p/124490

Daha sonrasında aşağıdaki komutlar sırasıyla çalıştırılarak splunk servisi yeniden ayağı kaldırılır ve check edilir.

chown -R splunk:splunk /opt/splunk

/opt/splunk/bin/splunk start

ps -ef |grep splunk