โหลด repo สำหรับลง syslog-ng

wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm

rpm -Uvh epel-release-latest-7.noarch.rpm

cd /etc/yum.repos.d/

wget https://copr.fedorainfracloud.org/coprs/czanik/syslog-ng324/repo/epel-7/czanik-syslog-ng325-epel-7.repo  
yum repolist

[[[Section 1]]]

NOTSCORED | 1.1.20 | PATCH | Ensure noexec option set on removable media partitions   
 - skip เพราะ removable media partitions ได้set option noexec ไว้อยู่แล้ว

SCORED | 1.1.22 | PATCH | Disable Automounting   
 - skip เพราะ autofs ไม่ได้ install ไว้

SCORED | 1.4.2 | PATCH | Ensure bootloader password is set  
 - skip เพราะ ใน default ตั้งให้skipไว้

SCORED | 1.5.4 | PATCH | Ensure prelink is disabled  
 - skip เพราะ ไม่ได้ลงprelinkไว้

NOTSCORED | 1.8 | PATCH | Ensure updates, patches, and additional security software are installed  
 - skip เพราะ defaults ตั้งไว้ว่าไม่ต้องอัพเดต เราสามารถไปตั้งให้อัพเดตได้ใน playbook ที่เอาไว้เรียกใช้งาน

ตัวอย่าง   
vars:

    ignore\_errors: false

    ignore\_unreachable: true

    rhel7cis\_level1: true

    rhel7cis\_level2: true

rhel7cis\_update:true

[[[section 2]]]

เป็นส่วนที่เกี่ยวกับการเปิดปิดservice ที่skipส่วนใหญ่นั้น defaults ได้ตั้งไว้ให้ปิดservice เหล่านั้น และบางส่วนก็อาจจะเป็นเพราะไม่ได้ลงcilentของservice เหล่านั้น

[[[section 3]]]

เป็นส่วนที่กี่ยวกับการตั้งกฎของiptable ซึ่งในระบบปฏิบัติการของredhatรู่นใหม่ๆนั้นไม่ได้ใช้iptableแล้ว เปลี่ยนมาใช้firewalld แทน โดยที่firewalld นั้นได้ตั้งกฎไว้อยู่แล้ว ส่วนนี้ก็เลยไม่ต้องตั้งค่าอะไร

[[[section 4]]]

SCORED | 4.1.2 | PATCH | Ensure auditd service is enabled  
skip ได้ไม่เป็นไร เพราะ service นี้เป็นserviceที่เปิดไว้อยู่แล้ว

เป็นส่วนที่เกี่ยวกับการตั้งค่าเก็บค่าlog ซึ่งมันต้องการ log address สำหรับเก็บlog โดยdefaults ได้ตั้งไว้ให้skip

[[[section 5]]]

SCORED | 5.1.8 | PATCH | Ensure at/cron is restricted to authorized users

- skip เพราะ ค่าdefaultsนั้นปิดไม่ให้เปิดใช้การจำกัดสิทธ์การloginของroot ซึ่งถ้าเปิดใช้งาน ก็จะไม่ใช้สามารถใช้งานrootได้

SCORED | 5.2.8 | PATCH | Ensure SSH root login is disabled  
 - skip เพราะ ต้องการไม่ให้ปิดการใช้งานSSH สำหรับ root

SCORED | 5.4.4 | PATCH | Ensure default user umask is 027 or more restrictive  
 - error เพราะ ไม่มีdirectory ปลายทาง แต่ก็ไม่ผลไว้กับระบบเพราะเป็นแค่การbackup

[[[section 6]]]

SCORED | 6.2.6 | PATCH | Ensure root PATH Integrity  
 - skip ได้ไม่มีผลเสียอะไรเพราะ แต่ต้องการทำการrun scripts เท่านั้น