

Ako na bezpečné konfiguračné zmeny v systéme Cisco NX-OS



Dátové centrá spoločnosti VNET a.s. poháňa sieťová platforma Cisco Nexus. Toto unifikované riešenie má implementované množstvo funkcií, zabezpečujúcich vysokú dostupnosť a automatizáciu poskytovaných služieb.

K ním patrí aj modul operačného systému NX-OS, ktorý umožňuje v konfigurácii vytvoriť záchytný bod, tzv. **Checkpoint**. Následne je možné sa k tomuto bodu konfigurácie jednoducho vrátiť, tzv. **Rollback**. Z tohto vyplýva, že užívateľ má možnosť návratu k pôvodnej funkčnej konfigurácii, v prípade úprav, ktoré spôsobia neočakávaný stav siete.

Základné použitie funkcie Configuration Checkpoint & Rollback

Podme sa pozrieť na základne možnosti funkcie. V systéme NX-OS si nasledujúcim príkazom vytvoríme záchytný bod (Checkpoint) s konkrétnym názvom (NovyBod) a voliteľným popisom (Testujeme funkciu Checkpoint):

```
Nexus# checkpoint NovyBod description Testujeme funkciu Checkpoint
Done
```

Nasledujúcim príkazom overíme stav záchytného bodu:

```
Nexus# show checkpoint summary
1) NovyBod:
Created by admin
Created at Sat, 10:36:45 02 Feb 2019
Size is 27,425 bytes
User Checkpoint Summary
-----
Description: Testujeme funkciu checkpoint
```

Následne vykonáme testovaciu úpravu konfigurácie:

```
Nexus# configure
Enter configuration commands, one per line. End with CNTL/Z.
Nexus(config)# hostname ZmenaNazvu
ZmenaNazvu(config)# interface ethernet 2/1
ZmenaNazvu(config-if)# description ZmenaPopisu
ZmenaNazvu(config-if)# end
ZmenaNazvu#
```

Predtým, ako obnovíme pôvodný stav systému zo záchytného bodu (NovyBod), vzájomne porovnáme konfigurácie zo záchytného bodu a aktuálnej bežiacej konfigurácie:

```
ZmenaNazvu# show diff rollback-patch checkpoint NovyBod running-config
Collecting Running-Config
#Generating Rollback Patch
```

```
!!
```

```
!
```

```
hostname ZmenaNazvu
```

```
!
```

```
interface Ethernet2/1
```

```
description ZmenaPopisu
```

Na aplikáciu pôvodnej konfigurácie zo záchytného bodu (NovyBod) použijeme tento príkaz:

```
ZmenaNazvu# rollback running-config checkpoint NovyBod verbose
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
#Generating Rollback Patch
Executing Rollback Patch
=====
`conf t`
`interface Ethernet2/1`
`no description ZmenaPopisu`
`exit`
`hostname Nexus`
=====
Generating Running-config for verification
Generating Patch for verification
Verification is Successful.
```

Rollback completed successfully.

Lokálnu databázu záchytných bodov je možné ručne vymazať príkazom:

```
Nexus# clear checkpoint database
Done
```

Základné parametre funkcie Configuration Checkpoint & Rollback

V predošlej časti sme si stručne popísali základnú činnosť modulu **Configuration Checkpoint & Rollback**, ďalej si bližšie popíšeme túto funkciu.

- Záchytné body (Checkpoints) sa ukladajú do internej systémovej databázy, ktorá nie je dostupná pre bežného užívateľa
- Záchytné body sú perzistentné a synchronizované medzi riadiacimi **Supervisor** modulmi
- Maximálny počet vytvorených záchytných bodov je 10 (ďalšie body sa cyklicky prepisujú)
- Záchytný bod nie je možné importovať na iné Nexus zariadenie, ako to, na ktorom bol vytvorený
- V danom časovom úseku môže len jeden užívateľ vykonávať činnosť **Checkpoint & Rollback**
- Záchytné body sa zmažú zo systémovej databázy použitím príkazov **write erase** a **reload**
- Záchytné body sú lokálne pre dané NX-OS zariadenie (Switch)
- Názvy záchytných bodov musia byť unikátne

- Funkcia **Rollback** je dostupná aj zo súborového úložiska **Bootflash** (na toto úložisko sa nevzťahuje limit 10 záchytných bodov), pomocou nasledujúceho príkazu vytvoríme checkpoint **checkpoint file bootflash:DalsiBod**

- Záchytné body sa ďalej vytvárajú automaticky pri týchto zmenách:

1. Vypnutím danej funkcie systému (Feature) pomocou príkazu **no feature**
2. Vypršanie licencie pre danú funkciu systému
3. Vypnutím inštancie L3 smerovacieho protokolu

- Funkcia **Rollback** má tieto ďalšie parametre:

1. Parameter **atomic** je predvolená možnosť, ktorá aplikuje záchytný bod, ak nedošlo ku žiadnej chybe
2. Parameter **verbose** vypíše postupnosť príkazov, ktoré sa aplikujú z daného záchytného bodu
3. Parameter **best-effort** ignoruje akékoľvek chyby a aplikuje záchytný bod
4. Parameter **stop-at-first-failure** aplikuje záchytný bod po prvú chybu

V tomto blogu sme si predstavili modul systému NX-OS, ktorý zabezpečuje ochranu a rýchly návrat k pôvodnej funkčnej konfigurácii. Tento a ďalšie moduly operačného systému zabezpečujú spoľahlivý chod sieťovej infraštruktúry v dátových centrách spoločnosti VNET. Máte aj vy ďalšie typy a postrehy pre systém NX-OS? Pokojne sa s nimi podel'te v komentároch.