Assigning Administrative Roles

Kurumlarda her iş için personellere gerektiği kadar bilgi ve yetki verilmesi istenir. Bu durum network için de geçerlidir. Networkten sorumlu kullanıcıların cihazlar üzerinde gerçekleştirebileceği işlemler de sınırlandırılmalıdır. IOS yazılımında bu işlemi gerçekleştirebilmek için Privileged Level ve Role-Based CLI olmak üzere iki seçenek bulunmaktadır.

Privileged Level

Privileged Level yönteminde toplamda kullanılabilecek 16 seviye bulunmaktadır. Bu seviyelerde kullanıcıların kullanabileceği komutlar tanımlanır ve kullanıcılar bu seviyelere atanır. Bu atamadan sonra kullanıcılar tanımlı oldukları seviyenin komutlarına kullanabilir. Bu seviyeler;

- Level 0, kullanıcı cihaz üzerinde sadece "**enable**", "**disable**", "**exit**", "**help**" ve "**logout**" komutlarını kullanabimektedir (Yeni komutlar eklenemiyor).
- Level 1, kullanıcının cihaz üzerinde hiçbir konfigürasyon gerçekleştiremediği seviyedir.
- Level 2 - Level 14, bu aralıktaki seviyeler için temel seviyede komutların kullanılmasına izin verilmektedir. Ek olarak bu aralıktaki seviyelerde kullanılmak üzere yeni komut tanımları eklenebiliyor.
- Level 15, kullanıcının cihaz üzerinde tam yetkiye sahip olduğu seviyedir.

Privileged seviyelerinde (2-14) kullanılabilecek komut setine eklemeler yapmak istendiğinde "**privilege <Mode> {level <Level> | reset} <Command>"** komutuyla hangi seviyede, hangi kullanıcı modunda, hangi komutların kullanılabileceği tanımlanabiliyor Tanımlamalarda dikkat edilmesi gereken konulardan biri de bir Privilege seviyesinde kullanılmasına izin verilen komutlar, tanımlandığı seviyenin üstünde bulunan seviyelerinde de kullanılmasına izin veriliyor. Örnek olarak;

- "**Privilege exec level 2 configıre terminal**" → Level 2 için Privileged Exec modda "configure terminal" komutunun kullanımına izin verir.
- "**Privilege configure level 10 line**" → Level 10 için Globla konfigürasyon modunda "line" komutunu kullanmasına izin verir ama Console veya VTY hattına giriş yapılamaz. Giriş yapabilmesi için "**Privilege config level 10 line console 0**" gibi tanımlanması gerekiyor.
- "**Privilege line level 10 password**" → Level 10 için Line konfigürasyon modunda parola atanmasına izin verir.

Privileged seviyelerine yeni kullanıcı hesabı oluşturulurken atama yapabilmek için "**username <Username> privilege <Level> secret <Password>**" komutu, var olan bir kullanıcı hesabını farklı seviyeye atanmak için "**username <Username> privilege <Level>**" komutu kullanılıyor.

Privileged seviyeleri arasında geçiş yapabilmek için öncelikle tanımlanan Privileged seviyelerine "**enable secret level <Privileged Level> <Password>**" komutuyla parola atanması gerekiyor (Seviyelere parola atamanmadan geçilmek istendiğinde hata mesajı alınıyor). Bu durumda bir kullanıcı daha yüksek bir Privileged seviyesine geçmek istediğinde geçmek istediği Privilege seviyesinin parolasını sorulacaktır (Privileged seviyelerine parola atandıktan sonra "**enable <Privileged Level>** " komutuyla geçiş yapılabiliyor).

> |→ Bulunduğunuz Privileged seviyesinden daha yüksek bir Privileged seviyesine geçiş yapıyorsanız parola sorulacaktır ama bulunduğunuz Privileged seviyesinde daha düşük bir Privileged seviyesine geçiş yapıyorsanız parola sorulmuyor.

```
R1(config)#username admin-X1 privilege 15 secret Admin123
R1(config)#username jn-Z2 privilege 8 secret Senior123
R1(config)#username jr-Z1 privilege 2 secret Junior123
R1(config)#enable secret EnableLevel15
R1(config)#enable secret level 8 EnableLevel8
R1(config)#enable secret level 2 EnableLevel2
R1(config)#privilege exec level 2 configure terminal
R1(config)#privilege config level 8 line console 0
R1(config)#privilege configure level 8 line console 0
R1(config)#privilege line level 8 password
```

|→ Bu konfigürasyon sonunda Level 2 seviyesine dahil kullanıcı sadece Global konfigürasyon moduna girebilirken Level 8 seviyesine dahil bir kullanıcı Console portuna girerek parola ataması gerçekleştirebilir.

Privileged Level Yönteminin Olumsuz Yönleri

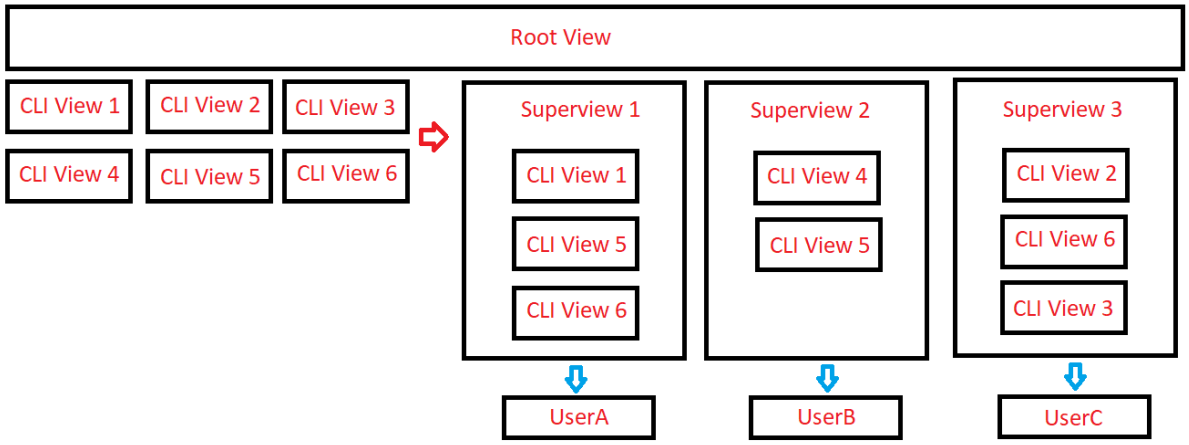
- Düşük seviyelerde tanımlanan bir komut yüksek seviyelerde de kullanılabiliyor. Yani kullanıcı veya seviye bazlı tanımlamalar yapılamıyor.
- Birden fazla sözcük içeren komutlar için ayrı ayrı kural tanımı yapılması gerekiyor. Örneğin;
    - line console 0
    - line vty 0 14
    - line aux 0
- Seviyelerde kullanılabilecek her komut satır satır tanımlanıyor.

Role Based CLI

Role Based CLI yöntemini anlayabilmek için bilinmesi gereken üç terim bulunuyor. Bunlar;

- Root View, cihaz üzerinde bulunan tüm komutların kullanılabildiği kapsamdır. Sadece Root View yeni bir CLI View veya Superview konfigürasyonu yaparak bunu kullanıcılara uygulayabilir.
- CLI View, kullanıcıların CLI üzerinde kullanabileceği komut listelerinin tanımlandığı yapılardır. Cihaz üzerinde sadece 15 CLI View oluşturabilmektedir.
- Superview, tanımlanan CLI View'lerin kullanılarak oluşturulan bir nevi kullanıcı profilleridir.

Role Base CLI yöntemi özetle, kullanıcıların CLI üzerinde kullanabileceği komutlar CLI View adı verilen bir yapı içerisinde tanımlanarak CLI View'ler oluşturuluyor. Oluşturulan CLI View'ler kullanılarak birnevi kullanıcı profilleri (Superview) oluşturuluyor (Bir kullanıcıya birde fazla CLI View ataması yapılabilyor). Son olarak da oluşturulan Superview'ler kullanıcılara tanımlanıyor.



Role Based CLI Konfigürasyonu

- Konfigürasyona cihaz üzerinde AAA etkinleştirilerek başlanıyor. Bunun için Global konfigürasyon modunda "**aaa new-model**" komutu kullanılıyor. Ardından "**enable secret**" komutuyla enable girişine parola atanması gerekiyor (Enable modu için tanımlanan parola sayesinde Root View yetkilerine sahip olmak için kullanılacak).
- AAA etkinleştirildikten sonra View konfigürasyonu yapabilmek için Privileged Exec modunda dönülerek "**enable [view]**" komutu kullanılarak Root View yetkilerine sahip olunuyor.
    - Bu kısımda parola isteniyor. Parola bilgisi olarak Enable girişine tanımlanan parola bilgisi giriliyor (Root View yetkilerine sahip olunuyor).

```
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#enable secret SecLab
R1(config)#exit
R1#
*Mar  1 00:24:10.987: %SYS-5-CONFIG_I: Configured from console by console
R1#enable view
Password:

R1#
*Mar  1 00:24:24.139: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
```

- Root View yetkilerine sahip olunduktan sonra konfigürasyona CLI View'ler oluşturmaya başlanarak devam ediliyor. Yeni bir CLI View oluşturmak veya var olan bir CLI View üzerinde düzenlemeler yapabilmek için Global konfigürasyon modunda "**parser view <View Name>**" komutu kullanılıyor.
    - Oluşturulan CLI View'e parola ataması yapılmadan içerisinde tanımlamalar yapılmasına izin verilmiyor. Bu nedenle ilk olarak "**secret <Password>**" komutuyla bir parola tanımlanıyor.
    - Parola tanımlandıktan sonra "**command <UserMode> (include | include-exclusive | exclude) [all] [interface <Interface Name> | <Command>]**" komutuyla kullanımına izin verilecek komutlar tanımlanıyor. Bu tanımlamaya örnek verek gerekirse;
        - "**commands exec include show version**" → Enable modunda sadece "show version" komutunun kullanılabilmesi sağlanıyor.
        - "**command exec include all show**" → Enable modunda bütün show komutlarının kullanılabilmesini sağlıyor.
        - "**commands configure include all interfaces**" → Global konfigürasyon modunda bütün arayüzlere girebilmesi sağlanıyor.
        - "**commands interface include no shutdown**" → Interface konfigürasyon modunda portları açabilmesi sağlanıyor.

```
R1(config)#parser view NewCLIView1
R1(config-view)#secret SecLab1
R1(config-view)#commands exec include show hardware
R1(config-view)#commands exec include show version
R1(config-view)#commands exec include show inventory
R1(config-view)#exit
R1(config)#parser view NewCLIView2
R1(config-view)#secret SecLab2
R1(config-view)#commands exec include all show
R1(config-view)#exit
R1(config)#parser view NewCLIView3
R1(config-view)#secret SecLab3
R1(config-view)#commands exec include all configure
R1(config-view)#exit
*Mar  1 00:00:59.951: %PARSER-6-VIEW_CREATED: view 'NewCLIView1' successfully created.
*Mar  1 00:00:59.967: %PARSER-6-VIEW_CREATED: view 'NewCLIView2' successfully created.
*Mar  1 00:00:59.983: %PARSER-6-VIEW_CREATED: view 'NewCLIView3' successfully created.
R1(config)#
```

- CLI View'de tanımlamalar yapıldıktan sonra bu listeler kullanılarak bir nevi kullanıcı profilleri / Superview'ler oluşturuluyor. Bunu için "**parse view <Supeview Name> superview**" komutu kullanılıyor.
    - Oluşturulan Superview için öncelikle "**secret <Password>**" komutuyla parola atanması gerekiyor (Aksi taktirde CLI View uygulanmasına izin vermiyor).
    - Parola atamasından sonra "**view <CLI View Name>**" komutuyla oluşturulan CLI View'ler Superview'e tanımlanıyor.

```
R1(config)#parser view NewSuperview1 superview
R1(config-view)#secret SecLabSuper1
R1(config-view)#view NewCLIView1
R1(config-view)#view NewCLIView3
R1(config-view)#exit
R1(config)#parser view NewSuperview2 superview
R1(config-view)#secret SecLabSuper2
R1(config-view)#view NewCLIView2
R1(config-view)#view NewCLIView3
R1(config-view)#exit
R1(config)#parser view NewSuperview3 superview
R1(config-view)#secret SecLabSuper3
R1(config-view)#view NewCLIView1
R1(config-view)#exit
*Mar  1 00:06:41.191: %PARSER-6-SUPER_VIEW_CREATED: super view 'NewSuperview1' successfully created.
*Mar  1 00:06:41.203: %PARSER-6-SUPER_VIEW_EDIT_ADD: view NewCLIView1 added to superview NewSuperview1.
*Mar  1 00:06:41.203: %PARSER-6-SUPER_VIEW_EDIT_ADD: view NewCLIView3 added to superview NewSuperview1.
*Mar  1 00:06:41.203: %PARSER-6-SUPER_VIEW_CREATED: super view 'NewSuperview2' successfully created.
*Mar  1 00:06:41.203: %PARSER-6-SUPER_VIEW_EDIT_ADD: view NewCLIView2 added to superview NewSuperview2.
*Mar  1 00:06:41.207: %PARSER-6-SUPER_VIEW_EDIT_ADD: view NewCLIView3 added to superview NewSuperview2.
R1(config-view)#exit
*Mar  1 00:06:41.219: %PARSER-6-SUPER_VIEW_CREATED: super view 'NewSuperview3' successfully created.
*Mar  1 00:06:41.219: %PARSER-6-SUPER_VIEW_EDIT_ADD: view NewCLIView1 added to superview NewSuperview3.
R1(config)#
```

```
R1#enable view NewSuperview1
Password:

R1#
*Mar  1 00:22:54.003: %PARSER-6-VIEW_SWITCH: successfully set to view 'NewSuperview1'.
R1#?
Exec commands:
  configure   Enter configuration mode
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information

R1#sh ?
  flash:     display information about flash: file system
  hardware   Hardware specific information
  inventory  Show the physical inventory
  parser     Show parser commands
  slot0:     display information about slot0: file system
  version    System hardware and software status

R1#
```

```
R1#enable view NewSuperview2
Password:

R1#?
Exec commands:
  configure   Enter configuration mode
  credential  load the credential info from file system
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  show        Show running system information

R1#
*Mar  1 00:24:28.955: %PARSER-6-VIEW_SWITCH: successfully set to view 'NewSuperview2'.
R1#sh ?
  aaa                     Show AAA values
  aal2                    Show commands for AAL2
  access-expression       List access expression
  access-lists            List access lists
  accounting              Accounting data for active sessions
  adjacency               Adjacent nodes
  alarm-interface         Display information about a specific Alarm
                          Interface Card
  aliases                 Display alias commands
  alignment               Show alignment information
  alps                    Alps information
  appfw                   Application Firewall information
  appletalk               AppleTalk information
  arap                    Show Appletalk Remote Access statistics
  archive                 Archive of the running configuration information
  arp                     ARP table
  async                   Information on terminal lines used as router
                          interfaces
  auto                    Show Automation Template
  backhaul-session-manager  Backhaul Session Manager information
  backup                  Backup status
  bcm560x                 BCM560x HW Table
  --More--
```

- Bu işlemlerden sonra oluşturulan Superview'ler kullanıcılara "**username <Username> view <Superview Name>**" komutuyla tanımlanıyor (Yeni kullanıcı oluşturuluyorsa "**username <Username> view <Superview Name> secret <Password>**" şeklinde tanımlanıyor).

```
R1(config)#username NewUser1 view NewSuperView1 secret Pass1
R1(config)#username NewUser2 view NewSuperView2 secret Pass2
R1(config)#username NewUser3 view NewSuperView3 secret Pass3
R1(config)#
```

Role Based CLI yöntemi Privileged Level yöntemiyle kıyaslandığında

- Role Base CLI yönteminde birden fazla sözcük içeren komutlar için ayrı ayrı tanımlama yapılmasına gerke kalmıyor. Tanımlamalarda “all” kelimesi kullanılarak bütün alternatiflere izin verilebiliyor.
- Role Base CLI yönteminde hiyerarşik bir seviyelendirme yapısı olmadığı için tanımlanan komut setleri kullanıcı bazlı uygulanıyor (bir seviyede tanımlanan komut seti üst seviyeler için de geçerli olmuyor).
-

NOT

- Oluşturulan Superview’lere“**enable view <Superview Name>**” komutuyla geçiş yapılabiliyor (Geçiş yapabilmek için ilgili Superview’in parolasını bilmeniz gerekiyor).

Kontrol Komutları

- sh parser view
- sh run
- sh privilege