

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING



New Behavior on Local User's Access and Local User Fallback when External Authentication is Configured

Prepared for: Cisco DNA Customer, Solutions Support

Prepared by: Tomas de Leon, Technical Leader

May 3, 2020

Document number: 05032020_v1

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING

RBAC - EXTERNAL AUTHENTICATION FALLBACK

New Behavior

With the new Wolverine Release (2.1.x.x), There has been some changes in behavior on Local User's Access and Local User Fallback. In previous releases of the Cisco DNA Center and External Authentication is Enabled, the Cisco DNA Center would fallback to Local User Authentication if the AAA Authentication didn't go thru. This behavior has changed in the new Wolverine Release (2.1.x.x). The Local User Authentication fallback will occur only when the AAA Server is NOT Reachable.

In addition with the changes, Maglev CLI admin user authentication has also changed when External Authentication is ENABLED. The Local User "admin" will fail authentication unless the proper AAA Server configuration takes this into account. If using ISE, the problem arises if you used "admin" as the username when setting up ISE. You may see Authentication failures for the Cisco DNA Center Local User "admin".

Working with the Changes

In order to address this change, you can chose some different options:

1. Revert back to the Older Local User Authentication workflow using the "[magctl rbac external_auth_fallback enable](#)".
2. Use the "[maglev login -u <username>](#)" command to assign a new "Admin" user that can be used for the Maglev CLI on the Cisco DNA Center.
3. Configure the ISE or AAA server to Authenticate the "admin" user for Super-Admin-Role permissions.

I have included some examples for Options 1 & 2 below.

Reference Information:

- Cisco DNAC Version 2.1.1.0 [2.1.210.72138]
- Cisco ISE version 2.6.0.156 Patches 1,2

CISCO SYSTEMS - CX CENTERS ENTERPRISE NETWORKING**OPTION #1 - REVERT BACK TO THE OLDER LOCAL USER AUTHENTICATION WORKFLOW USING THE “MAGCTL RBAC EXTERNAL_AUTH_FALLBACK ENABLE”.**

In this example, External Authentication is enabled. Local Users will fail Login Attempts in the UI and CLI on the Cisco DNA Center. In order to Revert back to the old behavior "Where there are no authentication for admin user or local users" issue the following command:

CLI Commands:

```
$ magctl rbac --help
```

```
$ magctl rbac external_auth_fallback enable
```

For Example:

```
$ magctl rbac --help
```

```
Usage: magctl rbac [OPTIONS] COMMAND [ARGS]...
```

```
RBAC related operations
```

Options:

```
--help Show this message and exit.
```

Commands:

```
custom_role_reconciliation custom roles related operations
```

```
external_auth_fallback External authentication fallback related...
```

```
resource_type RBAC resource types related operations for...
```

```
$ magctl rbac external_auth_fallback enable
```

OPTION #2 - USE THE "MAGLEV LOGIN -U <USERNAME>" COMMAND TO ASSIGN A NEW "ADMIN" USER THAT CAN BE USED FOR THE MAGLEV CLI ON THE CISCO DNA CENTER.

In this example, External Authentication is enabled. Local Users will fail Login Attempts in the UI and CLI on the Cisco DNA Center. The Local User Authentication fallback will occur only when the AAA Server is NOT Reachable. The main issue is that the Local Maglev "admin" fails external authentication using the CLI. As a result, "maglev" command cannot be perform until a maglev user is authenticated. Use the following commands to assign a new maglev username to the Cisco DNA Center Cluster.

With External Authentication enabled, The local "admin" username will not work. You will need to identify the Cluster Admin Username that has Super-Admin-Role permissions and is configured on the External Authentication Servers.

CLI Commands:

```
$ maglev login --help
$ maglev login -u < external username >
$ cat .maglevconf | grep username
```

MAGLEV LOGIN BEHAVIOR FOR CISCO DNA CENTER RELEASE FOR WOLVERINE RELEASE (2.1.x.x)

For Example:

No External Authentication

```
Welcome to the Cisco DNA Center Appliance
Welcome to the Maglev Appliance
```

```
System load:          9.03
Usage of /:           55.8% of 46.81GB
Memory usage:         51%
Swap usage:           0%
Processes:            3354
Users logged in:      1
```

```
$ maglev login
[administration] password for 'admin':
User 'admin' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully
```

```
Welcome to the Cisco DNA Center Appliance
maglev@172.18.217.208's password:

Welcome to the Maglev Appliance

System information as of Sun May  3 03:35:24 UTC 2020

System load:                9.03
Usage of /:                 55.8% of 46.81GB
Memory usage:              51%
Swap usage:                 0%
Processes:                  3354
Users logged in:           1
IP address for enp69s0f0:   192.168.211.207
IP address for enp69s0f1:   1.1.1.207
IP address for enp53s0f0:   172.18.217.207
IP address for enp53s0f1:   172.18.242.207
IP address for docker0:    169.254.0.1
IP address for node-local-dns: 169.254.20.10
IP address for tunl0:      169.254.44.192

Last login: Sun May  3 03:31:18 2020 from 10.82.175.187

[Sun May 03 03:35:24 UTC] maglev@172.18.217.207 (maglev-master-1-1-1-207) ~
$ maglev login
[administration] password for 'admin':      ** Ext Auth Disabled
User 'admin' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully

[Sun May 03 03:35:36 UTC] maglev@172.18.217.207 (maglev-master-1-1-1-207) ~
$
```

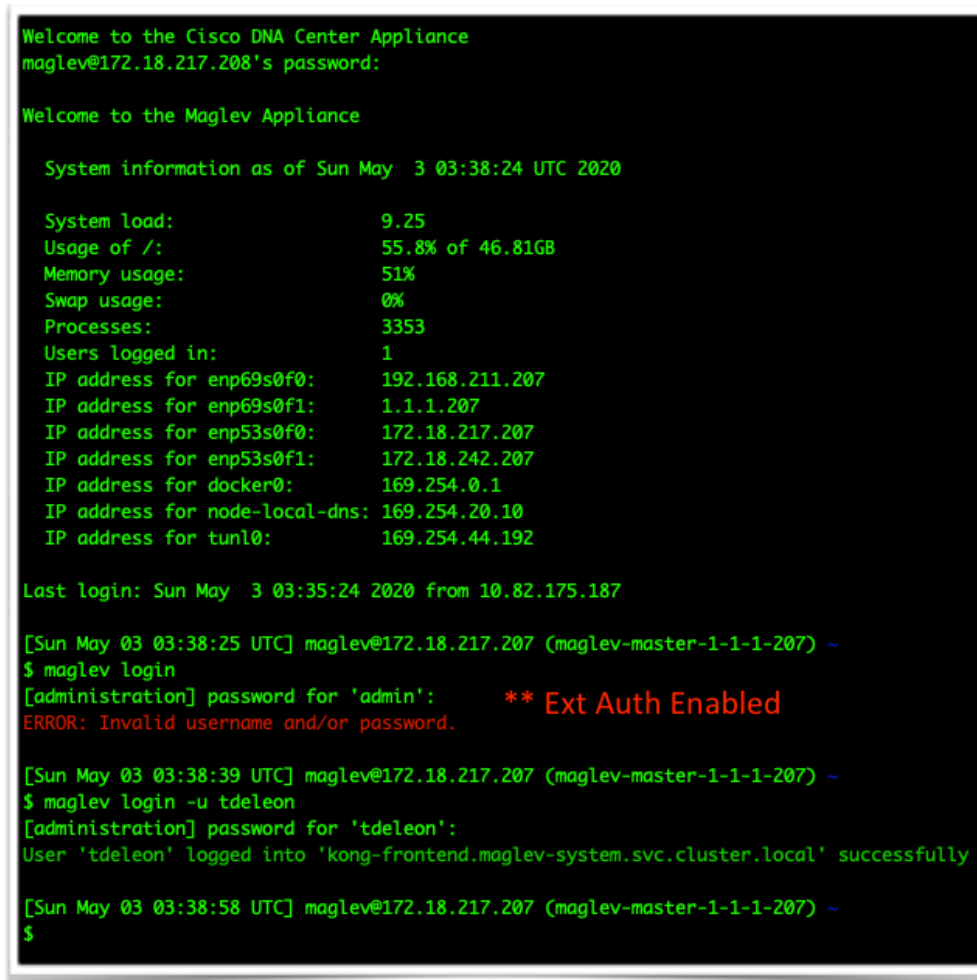
External Authentication Enabled

Welcome to the Cisco DNA Center Appliance
Welcome to the Maglev Appliance

```
System load:                9.25
Usage of /:                 55.8% of 46.81GB
Memory usage:              51%
Swap usage:                 0%
Processes:                  3353
Users logged in:           1
```

```
$ maglev login
[administration] password for 'admin':
ERROR: Invalid username and/or password.
```

```
$ maglev login -u tdeleon  
[administration] password for 'tdeleon':  
User 'tdeleon' logged into 'kong-frontend.maglev-system.svc.cluster.local' successfully  
  
$ cat .maglevconf | grep username  
username = tdeleon
```



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy
x \$ maglev login -u tdeleon						
May 03, 2020 03:38:58.371 AM	✓	🔍	tdeleon	Authorization	Authentication Policy	Default >> DNAC-SUPER-ADMIN-R...
May 03, 2020 03:38:58.359 AM	✓	🔍	tdeleon	Authentication	Default >> Default	
May 03, 2020 03:38:39.182 AM	✗	🔍	INVALID	Authentication	Default >> Default	
May 03, 2020 03:30:51.240 AM	✗	🔍	INVALID	Authentication	Default >> Default	** Local user "admin" access fails