Nexus 7000/5000 Internal Usernames that Execute Commands on the Nexus Platform Displayed in the Accounting Log

TAC **Document ID: 118107**

Contributed by Xinyi Li and Abhishek Pakrashi, Cisco TAC Engineers.

Oct 23, 2014

Contents

Introduction

This document describes the reason why undefined usernames appear in the logs of the Nexus switches in a vPC setup.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Nexus 7000
- Nexus 5000 in a vPC setup.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

With NX−OS running on Nexus 5000 and Nexus 7000 platforms, usernames such as "root", "_eemuser", "svc−isan" and "admin" could be observed in accounting logs, even though those usernames are not being

explicitly defined by the user. These usernames are pre−defined in the switch, and this document illustrates the conditions under which the aforementioned usernames could be observed in the accounting logs.

Username	*Explanation and Logs*

root	This test was performed on a Nexus 5000 switch.
	
	==========
	
	On Nexus 5000 when the command ***copy run start*** is run and when a configuration save is performed on it (copy run start), the user ***root*** shows up in the logs. See this example:
	
	`Tue May 6 05:25:28 2014:type=update:id=10.10.10.10@pts/0:user=admin:cmd=`
	` Performing configuration copy.`
	` Tue May 6 05:25:30 2014:type=start:id=vsh.20707:user=root:cmd=`
	` Tue May 6 05:25:31 2014:type=stop:id=vsh.20707:user=root:cmd=`
	` Tue May 6 05:25:35 2014:type=update:id=10.10.10.10@pts/0:user=admin:cmd=`
	` copy running−config startup−config (SUCCESS)`

__eemuser	This test was performed on Nexus 5000 switch with the EEM (Embedded Event Manager) feature supported.
	
	==========
	
	When an EEM script is configured on a Nexus 5000 switch, and a port down event is being detected, the EEM script will go into the interface configuration mode (in this case specifically for Fabric Extender (FEX) port Ethernet 114/1/1 for testing purposes), and bring it back up. See the example below:
	
	`Nexus5K# sh run eem`
	
	` !Command: show running−config eem`
	` !Time: Sun Apr 27 04:56:04 2014`
	
	` version 6.0(2)N2(4)`
	` event manager applet test`
	` event syslog pattern "ETHPORT−5−IF_DOWN_NONE"`
	` action 1.0 cli enable`
	` action 2.0 cli conf t`
	` action 3.0 cli interface ether 114/1/1`
	` action 4.0 cli no shut`
	` action 5.0 cli end`
	
	Log in to the Nexus 5000 with the username "admin1", which is configured locally. See this login session example:
	
	`Nexus1# show users`
	` NAME LINE TIME IDLE PID COMMENT`
	` admin1 pts/2 Apr 27 04:31 . 31579 (10.137.76.223) *`
	
	Manually shut down the port E114/1/1 on one of the FEX modules connected to the Nexus 5000. The port is bounced in this log:

```
2014 Apr 27 04:56:26 N5K−C5548UP %ETHPORT−5−IF_DOWN_NONE:
 Interface Ethernet114/1/32 is down (Transceiver Absent)
 2014 Apr 27 04:56:27 N5K−C5548UP %ETHPORT−5−IF_ADMIN_UP:
 Interface Ethernet114/1/32 is admin up.
```

In the accounting log, the user "eem_user" account did not perform a shutdown after "admin1" user performed a manual shut down of the port. See this example:

```
Sun Apr 27 04:56:25 2014:type=update:id=10.10.10.10@pts/2:user=admin1:
 cmd=configure terminal ; interface Ethernet114/1/1 (SUCCESS)
 Sun Apr 27 04:56:25 2014:type=update:id=10.10.10.10@pts/2:user=admin1:
 cmd=configure terminal ; interface Ethernet114/1/1 ; shutdown (REDIRECT)
 Sun Apr 27 04:56:26 2014:type=update:id=10.10.10.10@pts/2:user=admin1:
 cmd=configure terminal ; interface Ethernet114/1/1 ; shutdown (SUCCESS)
 Sun Apr 27 04:56:26 2014:type=start:id=vsh.32539:user=__eemuser:cmd=
 Sun Apr 27 04:56:27 2014:type=update:id=vsh.32539:user=__eemuser:cmd=configure
 terminal ; interface Ethernet114/1/1 (SUCCESS)
 Sun Apr 27 04:56:27 2014:type=update:id=vsh.32539:user=__eemuser:cmd=configure
 terminal ; interface Ethernet114/1/1 ; no shutdown (REDIRECT)
 Sun Apr 27 04:56:27 2014:type=update:id=vsh.32539:user=__eemuser:cmd=configure
 terminal ; interface Ethernet114/1/1 ; no shutdown (SUCCESS)
```

From the above timestamp and when the EEM script is triggered, the action for "no shut" is logged by user "eem_user".

This test was performed on a Nexus 7000.

svc−isan

```
====================================
```

When an EEM script is configured on the Nexus 7000, and a port admin shut event is being detected, the EEM script goes into the interface configuration mode (in this case specifically for FEX interface Ethernet 101/1/10 for testing purpose) and brings it back up. See this example:

```
event manager applet TEST
 event syslog pattern ".*ETHPORT−5−IF_DOWN_ADMIN_DOWN.*"
 action 1.0 cli enable
 action 2.0 cli conf t
 action 3.0 cli int e101/1/10
 action 4.0 cli no shut
 action 5.0 cli end
 action 6.0 syslog msg INTERFACE CHANGED TO ADMIN NO SHUT
\ action 7.0 syslog priority critical msg INTERFACE HAS BEEN CHANGED TO ADMIN UP
```

If E101/1/10 is shut down, the EEM script triggers and does not shut off the port. In the log, the below message is observed:

```
2014 Mar 12 07:12:37 Nexus_7000 %ETHPORT−5−IF_DOWN_ADMIN_DOWN:
 Interface Ethernet101/1/10 is down (Administratively down)
 2014 Mar 12 07:12:38 Nexus_7000 %ETHPORT−5−IF_ADMIN_UP:
```

```
Interface Ethernet101/1/10 is admin up .
2014 Mar 12 07:12:38 Nexus_7000 %VSHD-5-VSHD_SYSLOG_CONFIG_I:
Configured from vty by admin on vsh.23673
2014 Mar 12 07:12:38 Nexus_7000 %EEM_ACTION-2-CRIT:
INTERFACE HAS BEEN CHANGED TO ADMIN UP
```

In the accounting log and at the same timestamp, you see that shut down action was performed by admin, which is the account that has been used to login to the Nexus 7000. You see that the EEM is triggered and the configuration change by EEM is logged as svc-isan. See this accounting log from the Nexus 7000:

```
Wed Mar 12 07:12:37 2014:type=update:id=10.10.10.10@pts/0:user=admin:
cmd=switchto ; configure terminal ; interface Ethernet101/1/10 ;
 shutdown (REDIRECT)
Wed Mar 12 07:12:37 2014:type=update:id=10.10.10.10@pts/0:user=admin:
cmd=switchto ; configure terminal ; interface Ethernet101/1/10 ;
 shutdown (SUCCESS)
Wed Mar 12 07:12:38 2014:type=start:id=vsh.23673:user=svc-isan:cmd=
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isan:
cmd=configure terminal ; interface Ethernet101/1/10 (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isan:
cmd=configure terminal ; interface Ethernet101/1/10 ;
 no shutdown (REDIRECT)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isan:
cmd=configure terminal ; interface Ethernet101/1/10 ;
 no shutdown (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isan:
cmd=syslog msg INTERFACE CHANGED TO ADMIN NO SHUT (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isan:
cmd=syslog priority critical msg INTERFACE HAS BEEN CHANGED TO
 ADMIN UP (SUCCESS)
```

This test was performed on a pair of Nexus 5000s with config-sync.

admin

```
==============================================
```

The pre-configuration for config-sync on a pair of Nexus 5000s can be found here: Configuration Synchronization Operations.

This configuration was used in a switch-profile:

```
N5K1(config-sync-sp-if)# sh switch-profile buffer
```

```
switch-profile : Test
-----------------------------------------------------------
Seq-no  Command
-----------------------------------------------------------
2       interface Ethernet1/8
2.1       switchport
2.2       switchport mode trunk
2.3       switchport trunk allowed vlan 1-100
2.4       shutdown
```

Commit the change and push it over to the peer switch. Then confirm it has been applied

successfully:

```
N5K1(config-sync-sp-if)# commit
 Verification successful...
 Proceeding to apply configuration. This might take a while depending on
 amount of configuration in buffer.
 Please avoid other configuration changes during this time.
 Commit Successful
```

Now check for the accounting log on the N5K1, "test_user" which is the username that logged in to N5K1 has the configuration changes logged here:

```
Thu Mar 6 08:19:22 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface
 Ethernet1/8 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface
 Ethernet1/8 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (REDIRECT)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport mode trunk (REDIRECT)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport mode trunk (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742(sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport trunk allowed vlan 1-100  (REDIRECT)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport trunk allowed vlan 1-100 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 shutdown (REDIRECT)
Thu Mar 6 08:19:23 2014:type=update:id=ppm.23742 (sp-commit):
user=test_user:cmd= configure terminal ; interface Ethernet1/8 ;
 shutdown (SUCCESS)
Thu Mar 6 08:19:23 2014:type=stop:id=ppm.23742:user=test_user:
cmd=Thu Mar 6 08:19:23 2014:type=update:id=10.10.10.10@pts/1:
user=test_user:cmd= configure sync ; switch-profile Test ;
 commit (SUCCESS)
Thu Mar 6 08:19:23 2014:type=update:id=10.10.10.10@pts/1:
user=test_user:cmd= configure sync ; commit (SUCCESS)
```

See this peer Nexus 5000 switch, which has the configuration changes pushed over from N5K1. The accounting log reports around the same timestamp, and indicates that same configuration change has been made by "admin":

```
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit)
:user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (REDIRECT)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport mode trunk (REDIRECT)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport mode trunk (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport trunk allowed vlan 1−100 (REDIRECT)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 switchport trunk allowed vlan 1−100 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8
 (SUCCESS)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 shutdown (REDIRECT)
Thu Mar  6 08:19:23 2014:type=update:id=ppm.21880 (sp−commit):
user=admin:cmd= configure terminal ; interface Ethernet1/8 ;
 shutdown (SUCCESS)
```