

# Nexus 7000/5000 Internal Usernames that Execute Commands on the Nexus Platform Visualizzati nel log di accounting

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[radice](#)

[\\_emuser](#)

[svc-isan](#)

[admin](#)

## Introduzione

In questo documento viene descritto il motivo per cui alcuni nomi utente non definiti vengono visualizzati nei log degli switch Nexus in una configurazione vPC.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Nexus 7000
- Nexus 5000 in una [configurazione vPC](#).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Con NX-OS in esecuzione sulle piattaforme Nexus 5000 e Nexus 7000, nei log di accounting è possibile osservare nomi utente quali "root", "\_eemuser", "svc-isan" e "admin", anche se tali nomi utente non vengono definiti esplicitamente dall'utente. Questi nomi utente sono predefiniti nello switch e questo documento illustra le condizioni in cui i nomi utente sopra menzionati possono essere osservati nei log di accounting.

## Username Spiegazione e registri

Il test è stato eseguito su uno switch Nexus 5000.

=====

In Nexus 5000, quando viene eseguito il comando **copy run start** e viene eseguito un salvataggio della configurazione (copy run start), la **radice** utente viene visualizzata nei log. Vedere questo esempio:

radice

```
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)
```

Questo test è stato eseguito sullo switch Nexus 5000 con la funzionalità EEM (Embedded Event Manager) supportata.

=====

Quando si configura uno script EEM su uno switch Nexus 5000 e viene rilevato un evento di disattivazione della porta, lo script EEM entra in modalità di configurazione interfaccia (in questo caso in modo specifico per la porta Fabric Extender (FEX) Ethernet 14/1/1 a scopo di test) e lo riattiva. Vedere l'esempio seguente:

```
Nexus5K# sh run eem
```

```
!Command: show running-config eem
!Time: Sun Apr 27 04:56:04 2014
```

\_eemuser

```
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
```

Accedere a Nexus 5000 con il nome utente "admin1", configurato localmente. Vedere questo esempio di sessione di login:

```
Nexus1# show users
```

```
NAME          LINE          TIME          IDLE          PID COMMENT
```

admin1 pts/2 Apr 27 04:31 . 31579 (10.137.76.223) \*

Spegnere manualmente la porta E114/1/1 su uno dei moduli FEX collegati a Nexus 5000. La porta è rimbalzata nel seguente registro:

```
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.
```

Nel registro di accounting, l'account utente "eem\_user" non ha eseguito una chiusura dopo che l'utente "admin1" ha eseguito una chiusura manuale della porta. Vedere questo esempio:

```
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)
```

A partire dal timestamp sopra riportato e quando viene attivato lo script EEM, l'azione per "non chiudere" viene registrata dall'utente "eem\_user". Questo test è stato eseguito su un Nexus 7000.

=====

Quando si configura uno script EEM su Nexus 7000 e viene rilevato un evento di chiusura dell'amministratore della porta, lo script EEM entra in modalità di configurazione interfaccia (in questo caso in modo specifico per l'interfaccia FEX Ethernet 10/1/10 a scopo di test) e lo riporta stato attivo. Vedere questo esempio:

```
svc-isan 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
```

Se E101/1/10 è chiuso, lo script EEM si attiva e non spegne la porta. Nel registro viene visualizzato il seguente messaggio:

```
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
```

Nel registro di accounting e contemporaneamente all'indicatore orario, è possibile notare che l'azione di arresto è stata eseguita dall'amministratore, ovvero dall'account utilizzato per accedere a Nexus 7000. L'EEM viene attivato e la modifica della configurazione da parte di EEM viene registrata come svc-isn. Vedere questo registro di accounting da 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-isn:cmd=
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isn:
cmd=configure terminal ; interface Ethernet101/1/10 (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isn:
cmd=configure terminal ; interface Ethernet101/1/10 ;
no shutdown (REDIRECT)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isn:
cmd=configure terminal ; interface Ethernet101/1/10 ;
no shutdown (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isn:
cmd=syslog msg INTERFACE CHANGED TO ADMIN NO SHUT (SUCCESS)
Wed Mar 12 07:12:38 2014:type=update:id=vsh.23673:user=svc-isn:
cmd=syslog priority critical msg INTERFACE HAS BEEN CHANGED TO
ADMIN UP (SUCCESS)
```

Questo test è stato eseguito su una coppia di Nexus 5000 con config-sync.

=====

La preconfigurazione per la config-sync su una coppia di Nexus 5000 è disponibile qui: [Operazioni di sincronizzazione della configurazione](#).

Questa configurazione è stata utilizzata in un profilo di switch:

**admin**

```
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
```

Eseguire il commit della modifica e spostarla sullo switch peer. Confermare quindi che è stato applicato correttamente:

```
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
```

Verificare ora la presenza del registro di accounting sulla scheda N5K1, "test\_user" che è il no utente che ha eseguito il login alla scheda N5K1, dove sono registrate le modifiche alla configurazione:

```
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)
```

**Vedere questo switch Nexus 5000 peer, su cui sono state trasferite le modifiche alla configurazione da N5K1. Il log di accounting riporta circa lo stesso timestamp e indica che la stessa modifica di configurazione è stata apportata da "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)
```