

Risolvere i problemi relativi all'errore di aggiornamento di Expressway

Sommario

[Introduzione](#)

[Premesse](#)

[Componenti usati](#)

[Come procedere?](#)

[Procedura](#)

[Ulteriori informazioni](#)

Introduzione

In questo documento viene descritto come correggere un errore di aggiornamento di Expressway.

Premesse

In alcuni casi, mentre si aggiornano i server Expressway a una versione superiore, l'aggiornamento non riesce e viene visualizzato il seguente messaggio di errore:

System error: Post install script /tandberg/etc/postinstall.current.d/52-set_pubkeyalgorithms failed



Cisco Expressway-C

Status >

System >

Configuration >

Applications >

Users >

Maintenance >

System upgrade



System error: Post install script /tandberg/etc/postinstall.current.d/52-set_pubkeyalgorithms failed

[Return to upgrade page](#)

La causa principale di questo errore sono le voci di cifratura duplicate. L'idea principale di questo documento è quella di fornire i passaggi necessari per rimuovere le voci di cifratura duplicate nella configurazione.

Componenti usati

Expressway sulla versione X12.7.1.

Aggiornare il firmware alla versione X14.0.3.

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.

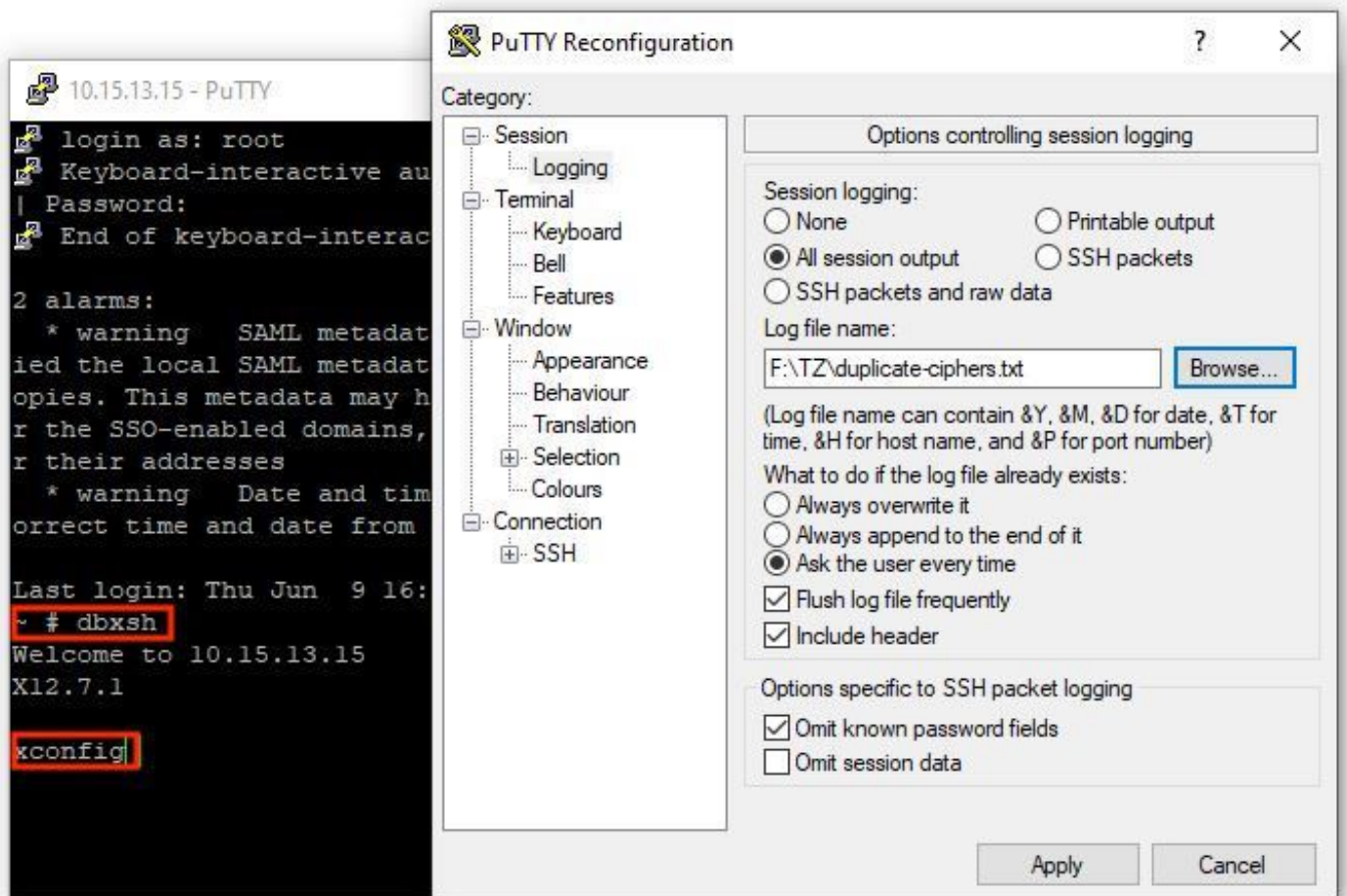
Come procedere?

In questo scenario, il primo passaggio consiste nel prelevare un file xconfig da Expressway. L'obiettivo è verificare quali cifrari sono duplicati.

 Nota: assicurarsi di utilizzare `root` anziché `admin` account per ottenere `xconfig` file.

Procedura

Accedi con `root` nel server Expressway per SSH, tipo `dbxsh`, quindi eseguire `xconfig`. Salvare l'output in un file `.txt` file.



Aprire il `xconfig`, cercare le voci di cifratura duplicate. Si consiglia di prendere nota delle voci duplicate. Mediante l'uso di Notepad++ (Windows) o Sublime Text (Mac), è possibile filtrare le parole `cipher` `uid`, quindi cercare i duplicati, come illustrato nell'esempio seguente:

```
1 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 uuid: "0276f859-fb9e-4e47-92fd-ea7f42cea988"
2 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 name: "RemoteSyslog1TLSProtocol"
3 xconfiguration cipher uuid 0276f859-fb9e-4e47-92fd-ea7f42cea988 value: "minTLSv1.0"
4 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 uuid: "085bcc06-46e8-4d4f-9a43-d6e9ebff7a67"
5 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 name: "UcClientTLSProtocol"
6 xconfiguration cipher uuid 085bcc06-46e8-4d4f-9a43-d6e9ebff7a67 value: "minTLSv1.0"
7 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 uuid: "1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0"
8 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 name: "RemoteSyslog3TLSCiphers"
9 xconfiguration cipher uuid 1cb8a665-2d5e-4c72-b6aa-6bc4a6770cf0 value: "ALL"
10 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 uuid: "1e768381-fc76-4713-94da-7f48484ba861"
11 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 name: "sshd_pfw_d_pubkeyalgorithms"
12 xconfiguration cipher uuid 1e768381-fc76-4713-94da-7f48484ba861 value: "x509v3-sign-rsa"
13 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 uuid: "1f803c71-6442-487e-86d1-202af7457b31"
14 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 name: "RemoteSyslog4TLSProtocol"
15 xconfiguration cipher uuid 1f803c71-6442-487e-86d1-202af7457b31 value: "minTLSv1.0"
16 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 uuid: "26afb85f-80ae-4569-9d48-cf30bf741430"
17 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 name: "sshd_pfw_d_pubkeyalgorithms"
18 xconfiguration cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430 value: "x509v3-sign-rsa"
19 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 uuid: "329946c9-d80a-42ee-b2cd-43bfc02998a7"
20 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 name: "sshd_pfw_d_kexalgorithms"
21 xconfiguration cipher uuid 329946c9-d80a-42ee-b2cd-43bfc02998a7 value: "ecdh-sha2-nistp384"
22 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 uuid: "45064c81-2e0c-42bd-a5dc-49a3ff2b0614"
23 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 name: "UcClientTLSCiphers"
24 xconfiguration cipher uuid 45064c81-2e0c-42bd-a5dc-49a3ff2b0614 value: "ALL"
25 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 uuid: "4f0bca0b-914a-496c-84cb-2a74bcbe0395"
26 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 name: "LDAPTLSProtocol"
27 xconfiguration cipher uuid 4f0bca0b-914a-496c-84cb-2a74bcbe0395 value: "minTLSv1.2"
28 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a uuid: "4f5ac5ca-2e15-4dc7-9162-5bb684425f7a"
29 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a name: "HTTPSProtocol"
30 xconfiguration cipher uuid 4f5ac5ca-2e15-4dc7-9162-5bb684425f7a value: "minTLSv1.0"
31 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b uuid: "588d2093-6bb3-44df-8e91-1a5a09fc303b"
32 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b name: "sshd_ciphers"
33 xconfiguration cipher uuid 588d2093-6bb3-44df-8e91-1a5a09fc303b value: "aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr"
34 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 uuid: "5cec77c9-3645-4484-980e-139ac6629954"
35 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 name: "RemoteSyslog2TLSCiphers"
36 xconfiguration cipher uuid 5cec77c9-3645-4484-980e-139ac6629954 value: "ALL"
37 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c uuid: "5e79851a-2ee9-44a7-9373-5887ba62546c"
38 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c name: "SMTPTLSProtocol"
39 xconfiguration cipher uuid 5e79851a-2ee9-44a7-9373-5887ba62546c value: "minTLSv1.2"
40 xconfiguration cipher uuid 6003cda6-afdc-4da1-9030-bdeaafdeb6f43 uuid: "6003cda6-afdc-4da1-9030-bdeaafdeb6f43"
41 xconfiguration cipher uuid 6003cda6-afdc-4da1-9030-bdeaafdeb6f43 name: "TMSProvisioningTLSProtocol"
42 xconfiguration cipher uuid 6003cda6-afdc-4da1-9030-bdeaafdeb6f43 value: "minTLSv1.2"
```

Nell'esempio viene mostrato che cipher `sshd_pfw_d_pubkeyalgorithms` ha una cifratura duplicata con un UUID (Universal Unique Identifier) diverso.

Una volta identificate tutte le cifrature duplicate, accedere al server Expressway dalla CLI con Putty root eliminare solo le voci duplicate, utilizzare le informazioni UUID in `dbxssh`.


Formato comando: `xdelete cipher uuid`

Esempio di cifratura eliminata nel file `xconfig`:

```
xdelete cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430
```

```
10.15.13.20 - PuTTY
xdelete cipher uuid 26afb85f-80ae-4569-9d48-cf30bf741430
OK
```

Ripetere la stessa procedura fino a eliminare tutte le voci duplicate.

 Nota: questa procedura può richiedere diversi tentativi fino a quando non vengono eliminate tutte le voci duplicate. Si consiglia di utilizzare un altro file `xconfig` per controllare due volte le cifrature.

Quindi, procedere con l'aggiornamento.

Ulteriori informazioni

ID bug Cisco [CSCvx35891](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).