Gestione dei server UCS serie C M3 e M4 che non supportano HTML5 dopo l'obsolescenza di Flash

Sommario

Introduzione

In questo documento vengono descritte le diverse procedure per accedere a Cisco Integrated Management Console (CIMC) o Virtual Keyboard Video Mouse (vKVM) e aggiornarli con il firmware che non supporta HTML5. Deprecazione post-flash.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- CIMC
- vKVM
- Cisco UCS serie C Rack Server

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Tuttavia, le informazioni di questo documento si basano esclusivamente su queste versioni software e hardware per la dimostrazione.

- UCS-C220-M4S
- CIMC versione 2.0(13g) e 3.0(3f)

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

In base all'annuncio di fine ciclo di vita di Adobe, Adobe prevede di deprecare i contenuti e il software basati su Flash dopo il 2020-12-31.

Problema

L'interfaccia utente Web (WebUI) delle versioni del software Cisco Integrated Management Controller (IMC) basate su Java potrebbe non funzionare dopo l'obsolescenza di Adobe Flash del 2020-12-31. Notifica: FN - 72014

> **Nota:** Per M3 Platform Server's HTML5-based Web UI interface for Cisco IMC non è disponibile su nessuna versione del software. Fare riferimento all'ID bug Cisco CSCvs11682.

> **Nota:** I server UCS serie M4 C dispongono di una WebUI basata su HTML5 con Cisco IMC 3.0(x), pertanto i server M4 non sono interessati. Tuttavia, il firmware di server 2.x o inferiore è interessato da tutti i server UCS serie C M3/M4.

Soluzioni

Metodi per accedere a CIMC per M3 per server piattaforma M4.

Èpossibile accedere al CIMC se si dispone ancora delle versioni precedenti del browser o di un qualsiasi browser di terze parti che supporta ancora la memoria flash.

Tuttavia, a causa di diversi fattori di sicurezza, Cisco sconsiglia questo metodo.

Collegamento diretto per avviare vKVM quando il CIMC non è accessibile

- Verificare che nel computer o nella macchina virtuale sia installata una versione Java compatibile.
- Se la versione CIMC è 2.x o 1.x, è necessario effettuare il downgrade della versione Java alla versione java7 u21 o Java7 u56 se si verifica un errore con la versione java corrente.
- Gli utenti devono consentire all'IP del CIMC di avviare vKVM nelle impostazioni Java.

Formato del collegamento:

```
https://x.x.x.x/kvm.jnlp?cimcAddr= x.x.x.x &tkn1=admin&tkn2=password
```

1. Sostituire <x.x.x.x> con l'indirizzo IP CIMC in entrambe le posizioni del collegamento (utilizzato due volte nel collegamento).

2. Sostituire <CIMC Username con il nome utente CIMC (generalmente admin) modificare solo se diverso da admin.

3. Sostituire <password> con la password CIMC corrente.

Esempio:

```
https://172.16.10.20/kvm.jnlp?cimcAddr=172.16.10.20&tkn1=admin&tkn2=cisco@123
```

Incollare il collegamento formattato con informazioni specifiche in un browser **Salvare/Conservare** il file JNLP e aprirlo in **Accetta/Continua/Sì** a tutti i popup, una volta avviato il KVM eseguire un HUU o aggiornare la versione del sistema operativo con l'ISO.

Uso dell'API XML per avviare vKVM

Èconsigliabile installare PowerShell e Java nella workstation.

Modificare le variabili **$cimcIP/$cimcUsername/$cimcPassword** e incollare lo script nella CLI di PowerShell per avviare KVM tramite API XML:

#Script Powershell per avviare Java KVM su Cisco IMC:

```
$cimcIP = "XX.XX.XX.XX"
$cimcUsername = "admin"
$cimcPassword = "password"
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
$Auth = @{uri = "https://$cimcIP/nuova";
                  Method = 'POST';
                                Body = "<aaaLogin inName='$cimcUsername'
inPassword='$cimcPassword'></aaaLogin>";
                               }
[xml]$AuthXML = Invoke-WebRequest @Auth -UseBasicParsing $AuthCookie =
$AuthXML.aaaLogin.outCookie $GetComputeAuthTokens = @{uri = "https://$cimcIP/nuova";
                  Method = 'POST';
                                Body = "<aaaGetComputeAuthTokens cookie='$AuthCookie'/>";
                               }
[xml]$GetComputeAuthTokensXML = Invoke-WebRequest @GetComputeAuthTokens -UseBasicParsing
$Token = $GetComputeAuthTokensXML.aaaGetComputeAuthTokens.outTokens -replace ",", "&tkn2="
$KVMurl = "https://$cimcIP/kvm.jnlp?cimcAddr=$cimcIP&cimcName=KVM&tkn1=$Token"
javaws "https://$cimcIP/kvm.jnlp?cimcAddr=$cimcIP&cimcName=KVM&tkn1=$Token"
```

La versione completa dell'API IMC è disponibile qui: Cisco IMC XML API Programmer's Guide.

Aggiornare CIMC dalla riga di comando

Èpossibile aggiornare il firmware CIMC con la CLI (solo per M4s).

Èquindi possibile avviare vKVM ed eseguire l'HUU normalmente.

Passaggio 1. Utilizzare la guida alla configurazione CLI disponibile sul collegamento incorporato e controllare il passaggio 11. della sezione **Recupero del firmware da Cisco** per i passaggi necessari per estrarre il file.

Passaggio 2. Aggiungere il file **CIMC.BIN** nel server **tftp/SCP/FTP** del sistema.

Passaggio 3. SSH sul server con l'indirizzo IP del CIMC. Eseguire quindi i comandi condivisi:

```
C-Series-III# scope cimc
C-Series-III /cimc# scope firmware
```

```
C-Series-III /cimc/firmware# update tftp172.16.10.29 /cimc.bin

Format :- update protocol IP /Path/Filename
```

Passaggio 4. Verificare quindi lo stato dell'aggiornamento tramite il comando **#Show detail**.

```
C-Series-III /cimc/firmware # show detail

Firmware Image Information:
Update Stage: DOWNLOAD  <<<<<<<<<<<<<===============
Update Progress: 5               <<<<<<<<<<<<<===============
Current FW Version: 2.0(13n)<<<<<<<<<<<<<===============
FW Image 1 Version: 4.0(2h) <<<<<<<<<<<<<===============
FW Image 1 State: BACKUP INACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: RUNNING ACTIVATED
Boot-loader Version: 2.0(13n).36
Secure Boot: ENABLED
```

Passaggio 5. Al termine del download, eseguire di nuovo il comando **#show detail**.

```
C-Series-III /cimc/firmware # show detail
Firmware Image Information:
Update Stage: NONE             <<<<<<<<<<<<<===============
Update Progress: 100           <<<<<<<<<<<<<===============
Current FW Version: 2.0(13n)<<<<<<<<<<<<<===============
FW Image 1 Version: 3.0(3f)  <<<<<<<<<<<<<=============== (This is the new image which is added
by the TFTP server)
FW Image 1 State: BACKUP INACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: RUNNING ACTIVATED
Boot-loader Version: 2.0(13n).36
Secure Boot: ENABLED
```

Passaggio 6. Digitare quindi **activate**.

```
C-Series-III /cimc/firmware # activate
This operation activates firmware 2 and reboot the BMC.
Continue?[y|N] Y
```

Passaggio 7. È previsto il riavvio del server e il ripristino della connettività tra 5 minuti. Sarà possibile verificare l'aggiornamento con lo stesso comando:

```
C-Series-III /cimc/firmware # show detail
Firmware Image Information:
Update Stage: NONE
Update Progress: 100
Current FW Version: 3.0(3f)  <<<<<<<<<<<<<=============== (Firmware got update from 2.0(13n) to
3.0(3f).
FW Image 1 Version: 3.0(3f)
FW Image 1 State: RUNNING ACTIVATED
FW Image 2 Version: 2.0(13n)
FW Image 2 State: BACKUP INACTIVATED
Boot-loader Version: 3.0(3f).36
Secure Boot: ENABLED
C-Series-III /cimc/firmware #
```

Passaggio 8. È possibile accedere a CIMC e avviare vKVM, quindi aggiornare il firmware con l'utility di aggiornamento dell'host.

Suggerimento: Non è necessario aggiornare il BIOS dalla CLI per ottenere l'aggiornamento CIMC per i server M4. Ma una volta che CIMC è aggiornato e accessibile dal browser. Assicurarsi di eseguire HUU e aggiornare tutti i componenti.

Per ulteriori informazioni, consultare la guida Cisco IMC Firmware Management: CLI Configuration Guide.

Informazioni correlate

- FN - 72012 - Versioni specifiche di UCS Manager interessate da Adobe Flash End-of-Life - Software
- FN - 72014 - (Cisco IMC) per server rack UCS M3 interessati dalla fine del ciclo di vita di Adobe Flash
- Documentazione e supporto tecnico – Cisco Systems