Administración de servidores UCS C-Series M3 y M4 que no admiten HTML5 después de la obsolescencia de Flash

Contenido

Introducción

Este documento describe los diferentes procedimientos para acceder y actualizar Cisco Integrated Management Console (CIMC) o Virtual Keyboard Video Mouse (vKVM) con el firmware que no admite HTML5. Depreciación post-Flash.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas.

- CIMC
- vKVM
- Servidor en rack de la serie C de Cisco UCS

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Sin embargo, la información en este documento se basa en estas versiones de software y hardware sólo para demostraciones.

- UCSC-C220-M4S
- CIMC versión 2.0(13g) y 3.0(3f)

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Mediante el anuncio del fin de vida útil de Adobe, Adobe planea depredar contenido y software basados en Flash después de 2020-12-31.

Problema

Es posible que la interfaz de usuario web (WebUI) de las versiones de software de Cisco Integrated Management Controller (IMC) basadas en Java no funcionen después de la obsolescencia de Adobe Flash en 2020-12-31. Aviso de problemas FN - 72014

> **Nota:** Para la interfaz de usuario web basada en HTML5 de M3 Platform Server para Cisco IMC no está disponible en ninguna versión de software. Refiérase al ID de bug de Cisco CSCvs11682.

> **Nota:** Los servidores UCS M4 C-Series tienen una interfaz de usuario web basada en HTML5 con Cisco IMC 3.0(x), por lo que los servidores M4 no se ven afectados. Sin embargo, cualquier firmware de servidor 2(x) o inferior se ve afectado para todos los servidores UCS C series M3/M4.

Soluciones

Métodos para acceder a CIMC para M3 para servidores de plataforma M4.

Se puede acceder al CIMC si todavía tienen las versiones anteriores del navegador o cualquier navegador de terceros que aún admita la memoria flash.

Sin embargo, debido a varios factores de seguridad, Cisco no recomienda este método.

Enlace directo para iniciar el vKVM mientras el CIMC está inaccesible

- Asegúrese de que tiene instalada una versión Java compatible en su ordenador o máquina virtual.
- Si la versión de CIMC es 2.x o 1.x, debe degradar la versión de java a la versión de java7 u21 o Java7 u56 si falla con la versión de java actual.
- Los usuarios deben permitir que la IP de CIMC inicie vKVM en los parámetros de Java.

Formato del enlace:

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

1. Reemplace <x.x.x.x> por la IP de CIMC en ambas ubicaciones del link (esto se utiliza dos veces en el link).

2. Reemplace <CIMC Username (Nombre de usuario CIMC) por el nombre de usuario CIMC (normalmente admin), sólo que sea diferente de admin.

3. Reemplace <password> por la contraseña CIMC actual.

Ejemplo:

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

Pegue el enlace formateado con información específica en un navegador **Guardar/Mantener** el archivo JNLP y ábralo **Aceptar/Continuar/Sí** a todas las ventanas emergentes, una vez que se inicie el KVM, ejecute un HUU o actualice la versión del sistema operativo con ISO.

Utilice la API XML para iniciar vKVM

Se recomienda instalar PowerShell y Java en la estación de trabajo.

Modifique las variables **$cimcIP/$cimcUsername/$cimcPassword** y pegue el script en la CLI de PowerShell para iniciar el KVM a través de la API XML:

#Powershell Script para iniciar Java KVM en 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 API completa de IMC se puede encontrar aquí: Guía del programador de API XML de Cisco IMC.

Actualizar el CIMC desde la línea de comandos

Puede actualizar el firmware CIMC con la CLI (sólo para M4s).

A continuación, puede iniciar vKVM y ejecutar el HUU de la forma habitual.

Paso 1. Utilice la Guía de Configuración de CLI que se encuentra en el enlace incrustado y marque el Paso 11. de la sección **Obtención del firmware de Cisco** para obtener los pasos necesarios para extraer el archivo.

Paso 2. Agregue el **CIMC.BIN** al servidor **tftp/SCP/FTP** en su sistema.

Paso 3. SSH al servidor con la dirección IP del CIMC. A continuación, ejecute los comandos compartidos:

```
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
```

Paso 4. Luego verifique el estado de la actualización mediante el 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
```

Paso 5. Ejecute el comando **#show detail** de nuevo una vez que se complete la descarga.

```
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
```

Paso 6. A continuación, escriba **activar**.

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

Paso 7. Ahora, se espera que el servidor se reinicie y se restablezca la conectividad en 5 minutos. Podrá verificar la actualización con el mismo 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 #
```

Paso 8. Puede iniciar sesión en CIMC y ejecutar vKVM y, a continuación, actualizar el firmware

con la utilidad de actualización de host.

> **Consejo:** Esto no es necesario para actualizar el BIOS desde CLI para lograr la actualización de CIMC para servidores M4. Pero una vez que CIMC se actualiza y se puede acceder a él desde el navegador. Asegúrese de ejecutar el HUU y actualizar todos los componentes.

Para obtener más detalles, consulte la guía de administración del firmware de Cisco IMC: Guía de configuración de CLI.

Información Relacionada

- FN - 72012 - Versiones específicas de UCS Manager afectado por el fin de vida útil de Adobe Flash - Software
- FN - 72014 - (Cisco IMC) para servidores en rack UCS M3 afectados por el fin de vida útil de Adobe Flash
- Soporte Técnico y Documentación - Cisco Systems