Gestion des serveurs UCS série C M3 et M4 qui ne prennent pas en charge HTML5 après déstabilisation de la mémoire Flash

Contenu

[Introduction](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Problème](#)
[Solutions](#)
[Lien direct pour lancer la vKVM lorsque la CIMC est inaccessible](#)
[Utiliser l'API XML pour lancer vKVM](#)
[Mettre à jour le CIMC à partir de la ligne de commande](#)
[Informations connexes](#)

Introduction

Ce document décrit les différentes procédures d'accès et de mise à niveau de Cisco Integrated Management Console (CIMC) ou de Virtual Keyboard Video Mouse (vKVM) avec le micrologiciel qui ne prend pas en charge HTML5. Dégradation post-Flash.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- CIMC
- vKVM
- Serveur rack Cisco UCS série C

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Cependant, les informations contenues dans ce document sont basées sur ces versions logicielles et matérielles à des fins de démonstration uniquement.

- UCSC-C220-M4S
- CIMC versions 2.0(13g) et 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Par l'annonce de fin de vie d'Adobe, Adobe prévoit de déprécier le contenu et les logiciels Flash après 2020-12-31.

Problème

L'interface utilisateur Web (WebUI) des versions du logiciel Cisco Integrated Management Controller (IMC) basées sur Java pourrait ne pas fonctionner après la désapprobation d'Adobe Flash le 2020-12-31. Avis sur le champ : FN - 72014

> **Note**: Pour l'interface utilisateur Web HTML5 de M3 Platform Server pour Cisco IMC, aucune version logicielle n'est disponible. Reportez-vous à l'ID de bogue Cisco CSCvs11682.

> **Note**: Les serveurs UCS M4 série C possèdent une interface Web HTML5 avec Cisco IMC 3.0(x), ce qui signifie que les serveurs M4 ne sont pas affectés. Cependant, tout microprogramme de serveur 2.x) ou inférieur est affecté pour tous les serveurs UCS série C M3/M4.

Solutions

Méthodes d'accès à CIMC pour M3 pour les serveurs de plate-forme M4.

Vous pouvez accéder au CIMC s'il dispose toujours des versions plus anciennes du navigateur ou de tout navigateur tiers qui prend toujours en charge la mémoire Flash.

Cependant, en raison de plusieurs facteurs de sécurité, Cisco ne recommande pas cette méthode.

Lien direct pour lancer la vKVM lorsque la CIMC est inaccessible

- Vérifiez qu'une version Java compatible est installée sur votre ordinateur ou votre machine virtuelle.
- Si la version CIMC est 2.x ou 1.x, vous devez rétrograder la version java vers la version java7 u21 ou Java7 u56 si elle échoue avec la version java actuelle.
- Les utilisateurs doivent autoriser l'adresse IP du CIMC à lancer le vKVM dans les paramètres Java.

Format du lien :

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

1. Remplacez <x.x.x.x> par l'adresse IP CIMC aux deux emplacements de la liaison (utilisée deux fois dans la liaison).

2. Remplacer <Nom d'utilisateur CIMC par le nom d'utilisateur CIMC (généralement admin) ne changez qu'il est autre qu'admin.

3. Remplacez <password> par le mot de passe CIMC actuel.

Exemple :

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

Collez le lien formaté avec des informations spécifiques dans un navigateur **Enregistrer/Conserver** le fichier JNLP et ouvrez-le **Accepter/Continuer/Oui** à toutes les fenêtres contextuelles, une fois le KVM lancé, exécutez un HUU ou mettez à niveau la version du système d'exploitation avec l'ISO.

Utiliser l'API XML pour lancer vKVM

Il est recommandé d'installer PowerShell et Java sur la station de travail.

Modifiez les variables **$cimcIP/$cimcUsername/$cimcPassword** et collez le script dans l'interface de ligne de commande PowerShell pour lancer la KVM via l'API XML :

#Powershell Script pour lancer Java KVM sur 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"
```

L'API IMC complète est disponible ici : Guide du programmateur d'API XML IMC de Cisco.

Mettre à jour le CIMC à partir de la ligne de commande

Vous pouvez mettre à niveau le micrologiciel CIMC avec l'interface de ligne de commande (CLI) (pour M4 uniquement).

Ensuite, vous pouvez lancer vKVM et exécuter l'HUU comme d'habitude.

Étape 1. Utilisez le Guide de configuration de l'interface de ligne de commande figurant sur la liaison intégrée et cochez la case Étape 11. de la section **Obtention du micrologiciel auprès de Cisco** pour les étapes d'extraction du fichier.

Étape 2. Ajoutez le **CIMC.BIN** au serveur **tftp/SCP/FTP** sur votre système.

Étape 3. SSH au serveur avec l'adresse IP du CIMC. Exécutez ensuite les commandes partagées :

```
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
```

Étape 4. Vérifiez ensuite l'état de la mise à niveau à l'aide de la commande **#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
```

Étape 5. Exécutez à nouveau la commande **#show detail** une fois le téléchargement terminé.

```
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
```

Étape 6. Tapez ensuite **activate**.

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

Étape 7. Maintenant, le serveur doit redémarrer et la connectivité est restaurée dans 5 minutes. Vous pourrez vérifier la mise à niveau à l'aide de la même commande :

```
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 #
```

Étape 8. Vous pouvez vous connecter à CIMC et lancer la vKVM, puis mettre à jour le

micrologiciel à l'aide de l'utilitaire de mise à niveau de l'hôte.

> **Astuce** : Il n'est pas nécessaire de mettre à jour le BIOS à partir de l'interface de ligne de commande pour réaliser la mise à niveau CIMC pour les serveurs M4. Mais une fois le CIMC mis à jour et accessible à partir du navigateur. Veillez à exécuter le HUU et à mettre à jour tous les composants.

Pour plus d'informations, reportez-vous au guide de gestion des microprogrammes Cisco IMC : Guide de configuration CLI.

Informations connexes

- FN - 72012 - Versions spécifiques d'UCS Manager affectées par Adobe Flash en fin de vie - Logiciel
- FN - 72014 - (Cisco IMC) pour serveurs rack UCS M3 affectés par la fin de vie d'Adobe Flash
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.