Atualize o CIMC no APIC

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Antes de atualizar

Procedimento

Introdução

Este documento descreve como atualizar o Cisco Integrated Management Controller (CIMC) em servidores UCS C Series que executam o Cisco APIC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Servidores Unified Computing System (UCS)
- Application Policy Infrastructure Controller (APIC)

Componentes Utilizados

As informações neste documento são baseadas nos servidores APIC executados nos servidores UCS C Series.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de atualizar

A atualização da versão do software da estrutura da ACI pode definir novos requisitos para a versão do CIMC em execução na estrutura. Portanto, é sempre recomendável verificar as notas de versão da versão do software APIC para saber a lista de versões do software CIMC compatíveis para uma versão específica do APIC.

1. Verifique as notas de versão do APIC e confirme para qual imagem do software CIMC você precisa atualizar. Link para as notas de versão do APIC.

2. Obtenha a imagem do Software no site Cisco.com.

3. Confirme se a soma de verificação MD5 da imagem corresponde àquela publicada no site Cisco.com.

4. O tempo necessário para o processo de atualização de uma versão do CIMC varia de acordo com a velocidade do link entre a máquina local e o chassi do UCS-C e a imagem do software de origem/destino e outras versões de componentes internos.

5. A atualização do CIMC não afeta a rede de produção, pois os APICs não estão no caminho de dados do tráfego.

6. Quando você atualiza a versão do CIMC, também pode ser necessário alterar o navegador da Internet e a versão do software Java para executar a máquina virtual baseada em Kernal (vKVM).

Para atualizar o CIMC do APIC, você também pode usar o Cisco Host Upgrade Utility com base no guia.

Servidores APIC executados em servidores UCS C Series. Cisco UCS 220 M5, Cisco UCS 220 M4 (dispositivos de segunda geração APIC-SERVER-M2 e APIC-SERVER-L2) ou Cisco UCS 220 M3 (dispositivo de primeira geração APIC-SERVER-M1 e APIC-SERVER-L1), com uma pequena diferença que os servidores fabricados com uma imagem protegida por Trusted Platform Module (TPM), certificados e uma ID de produto (PID) do APIC.

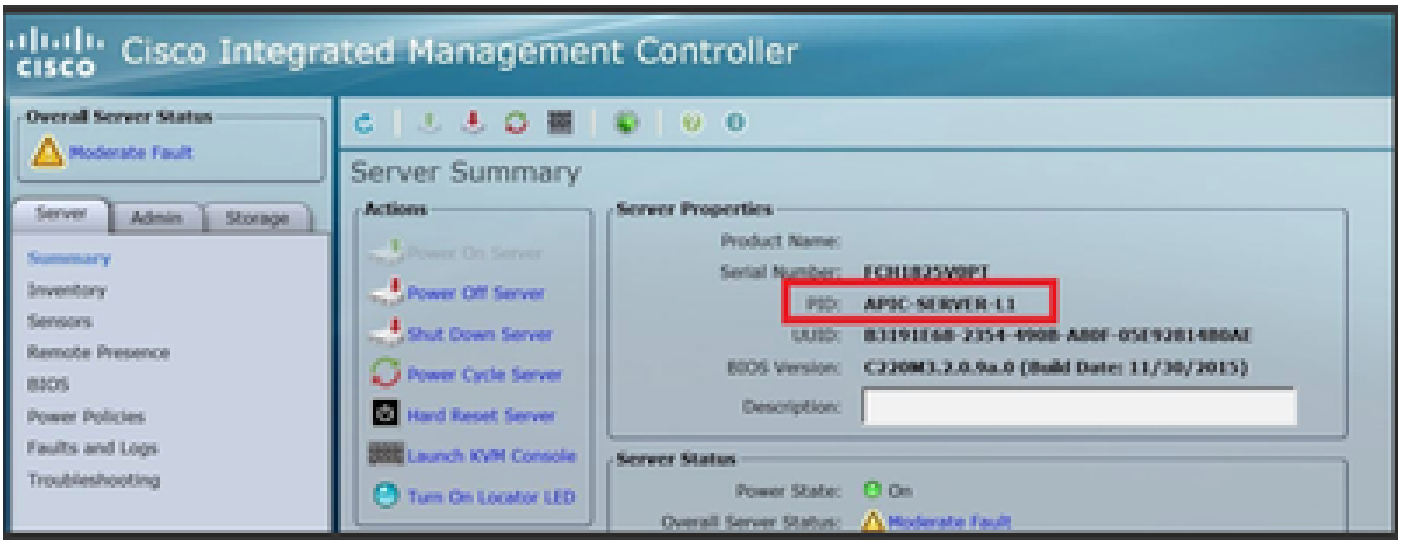
Plataforma APIC	Plataforma correspondente do UCS	Descrição
APIC-SERVER-M1	UCS-C220-M3	Cluster de três controladores Cisco APIC de primeira geração com configurações de CPU, disco rígido e memória de tamanho médio para até 1.000 portas de borda.
APIC-SERVER-M2	UCS-C220-M4	Cluster de três controladores Cisco APIC de segunda geração com CPU de tamanho médio, disco rígido e configurações de memória para até 1.000 portas de borda.
APIC-SERVER-M3	UCS C220 M5	Cluster de três controladores Cisco APIC de segunda geração com CPU de tamanho médio, disco rígido e configurações de memória para até 1.000 portas de borda.
APIC-SERVER-L1	UCS-C220-M3	Cluster de três controladores Cisco APIC de primeira geração com CPU de grande porte, disco rígido e configurações de memória para mais de 1.000 portas de borda.

APIC-SERVER-L2	UCS-C220-M4	Cluster de três controladores Cisco APIC de segunda geração com CPU de grande porte, disco rígido e configurações de memória para mais de 1.000 portas de borda.
APIC-SERVER-L3	UCS C220 M5	Cisco APIC com grandes configurações de CPU, disco rígido e memória (mais de 1.200 portas de borda).

Procedimento

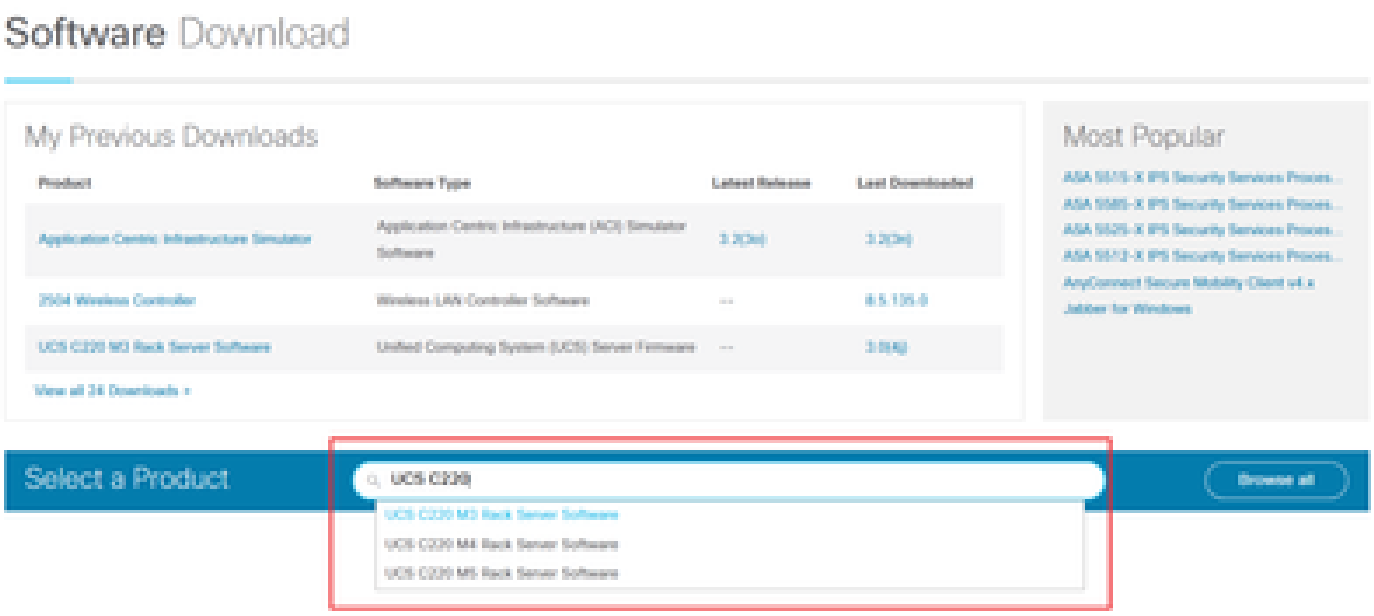
Etapa 1. Determine primeiro o modelo APIC.

Você pode verificar isso na GUI do CIMC para verificar o PID exibido em Server> Summary.



Etapa 2. Fazer Download do Software.

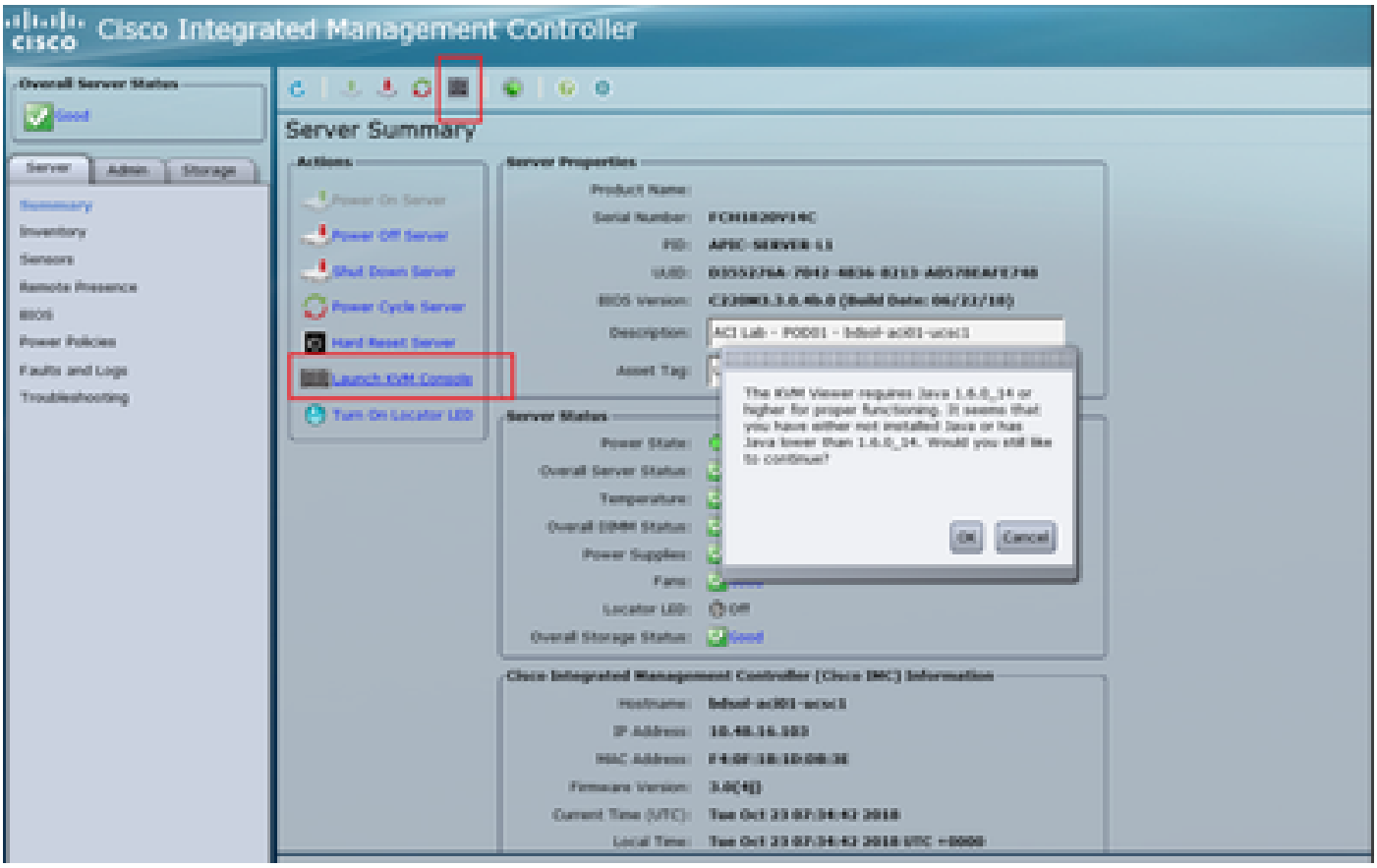
Na página Cisco Download Software, navegue para Select a Product > Downloads > Home Servers - Unified Computing > UCS C-Series Rack-Mount Standalone Server Software > Escolha UCS 220 M3/M4/M5 com base na geração do APIC > Unified Computing System (UCS) Server Firmware.

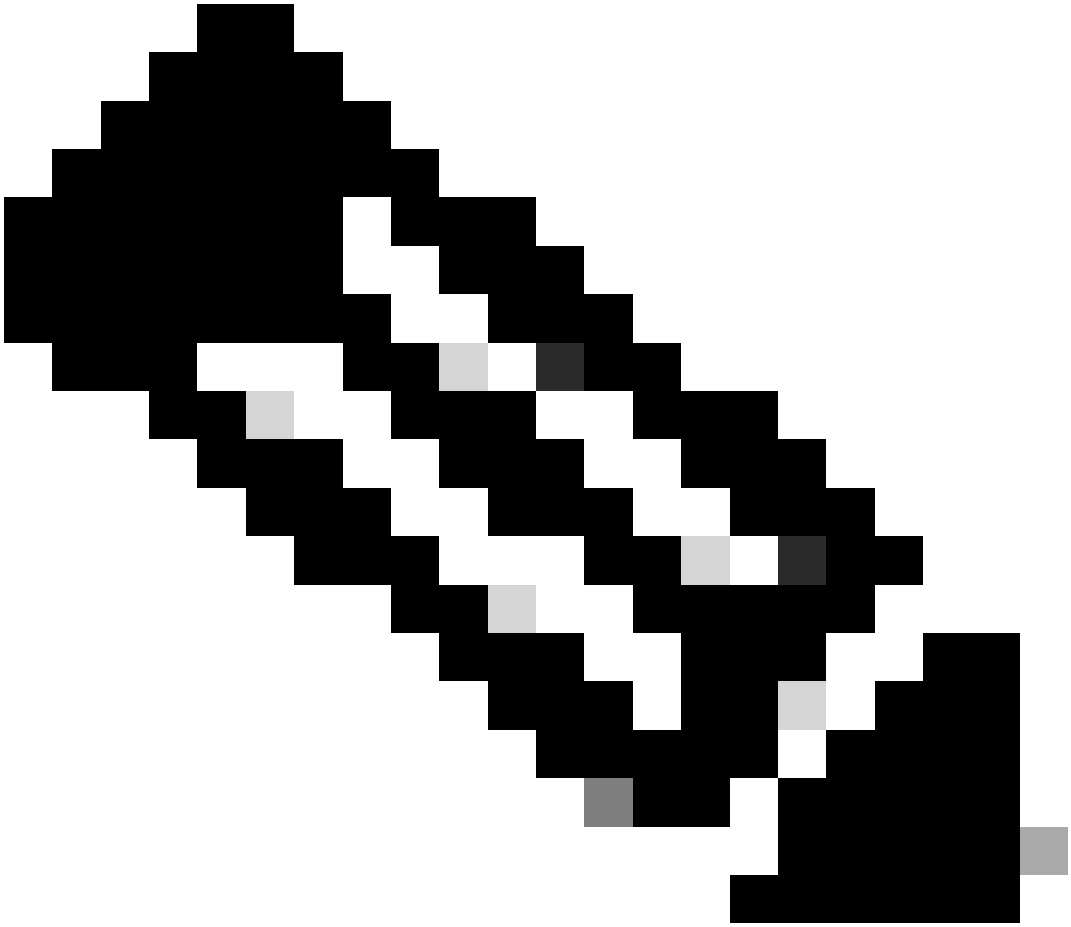


Note: Verifique a [versão CIMC e o guia de versão do software] recomendados para fazer download da versão do firmware CIMC recomendada para sua versão do software ACI atual.

Use apenas o firmware recomendado pelo APIC do CIMC em vez do mais recente ou recomendado para esse modelo do UCS.

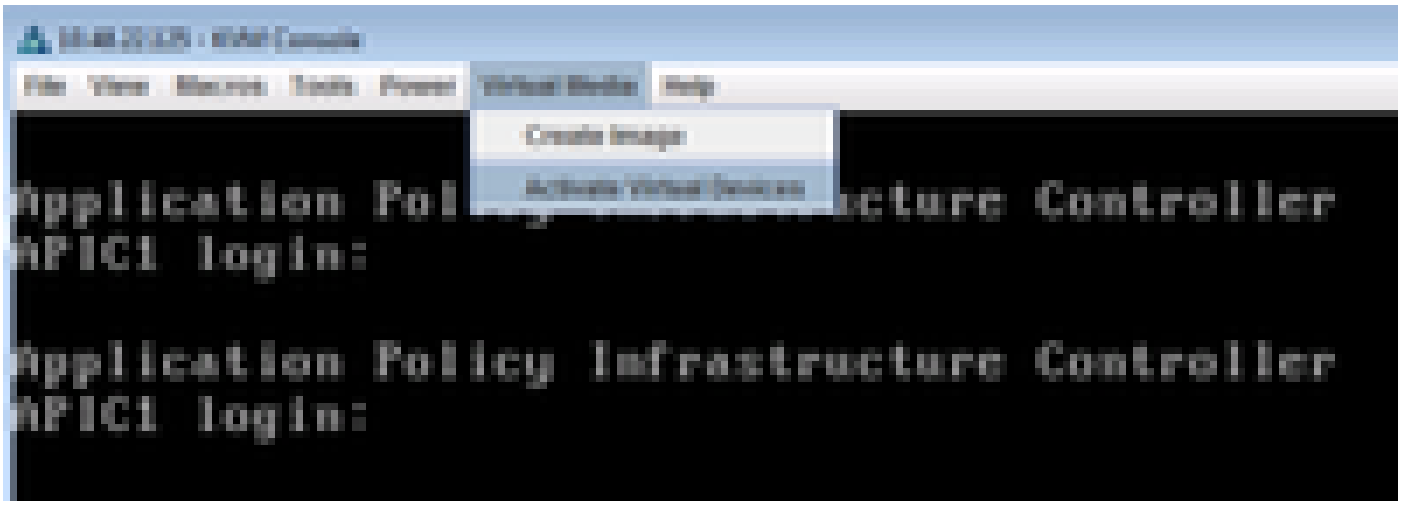
Etapa 3. Inicie o console KVM na GUI do CIMC.



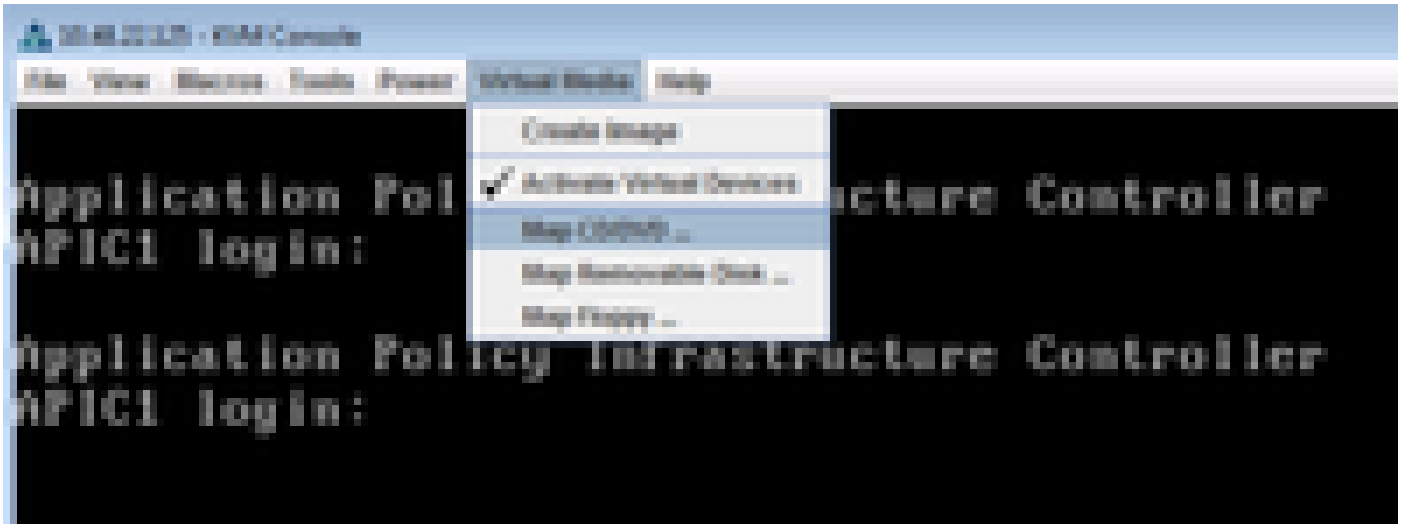


Note: Se você tiver problemas ao abrir o console KVM, isso geralmente é um problema com a versão JAVA. Leia as Notas de versão da sua versão do CIMC para conhecer as diferentes soluções disponíveis.

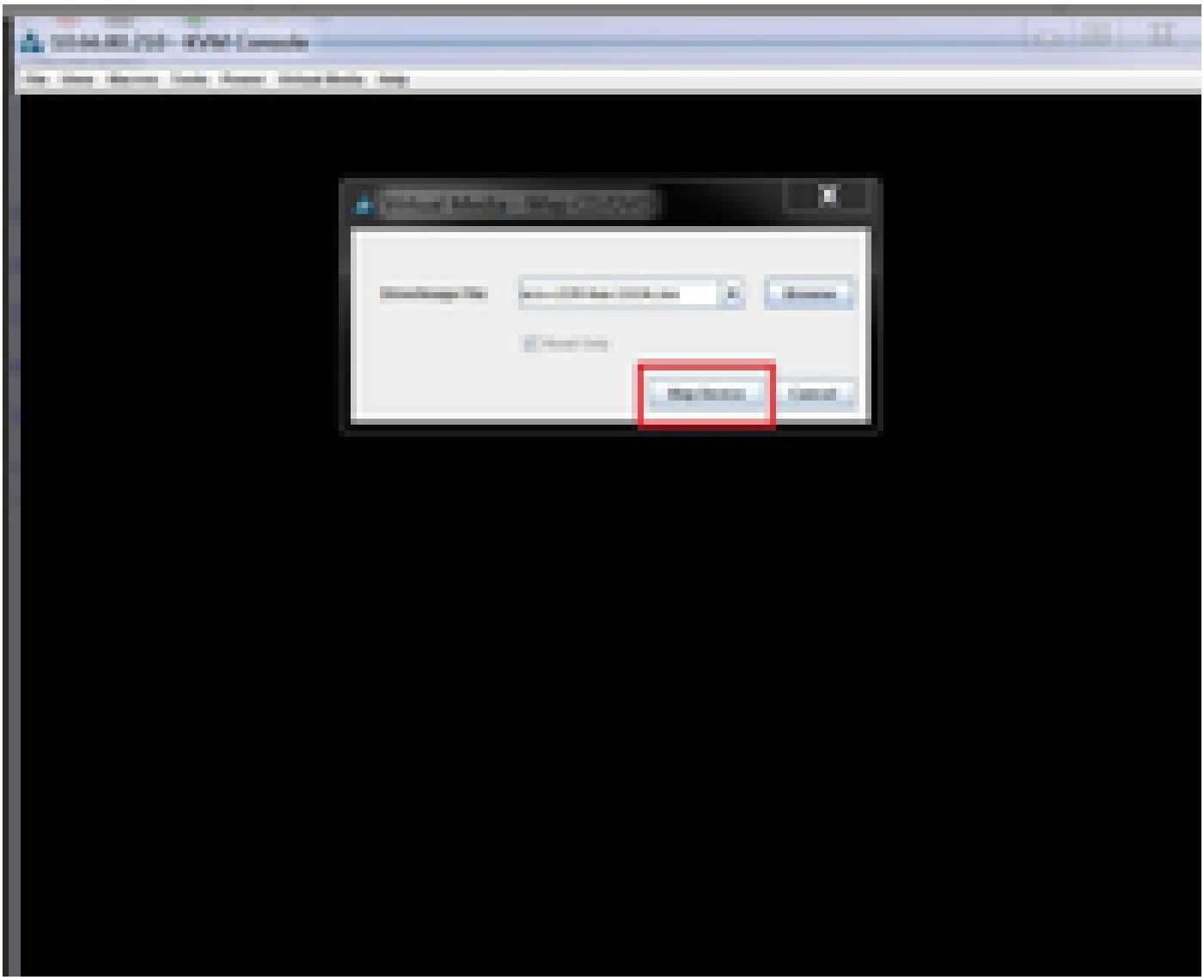
Etapa 4. Para ativar o dispositivo virtual, navegue até Virtual Media > Ativate Virtual Devices conforme mostrado na imagem.



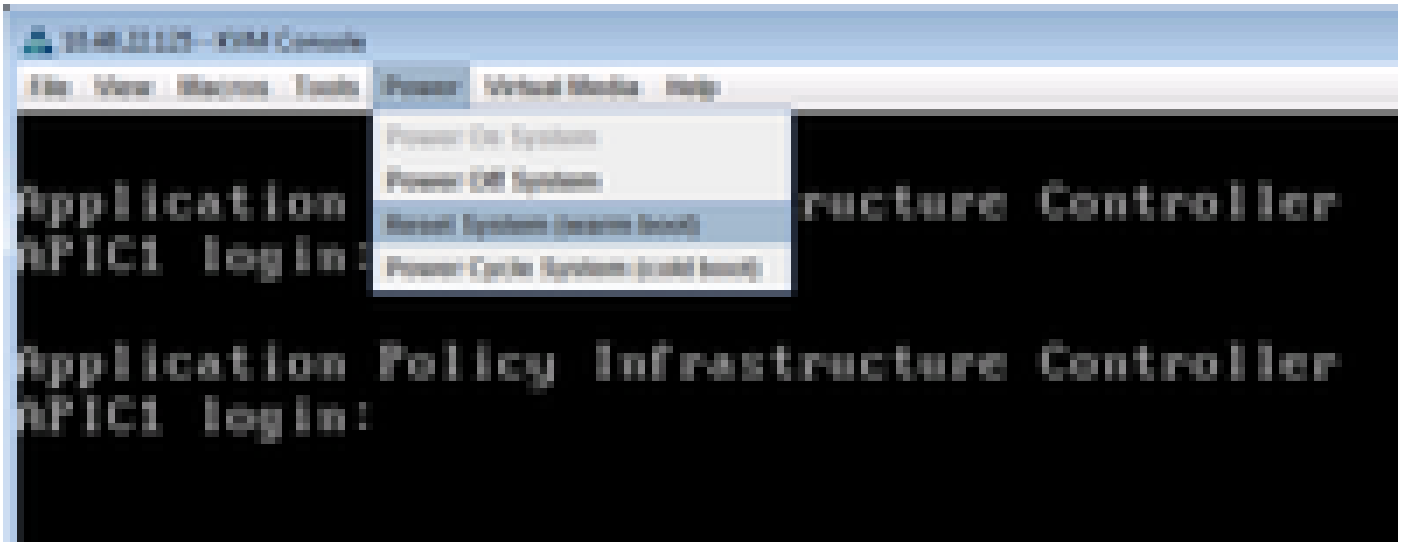
Etapa 5. Para mapear a imagem ISO descarregada como um CD/DVD, navegue para Virtual Media > Map CD/DVD como mostrado na imagem.



Etapa 6. Navegue pela imagem ISO da máquina local e clique em Mapear dispositivo conforme mostrado na imagem.

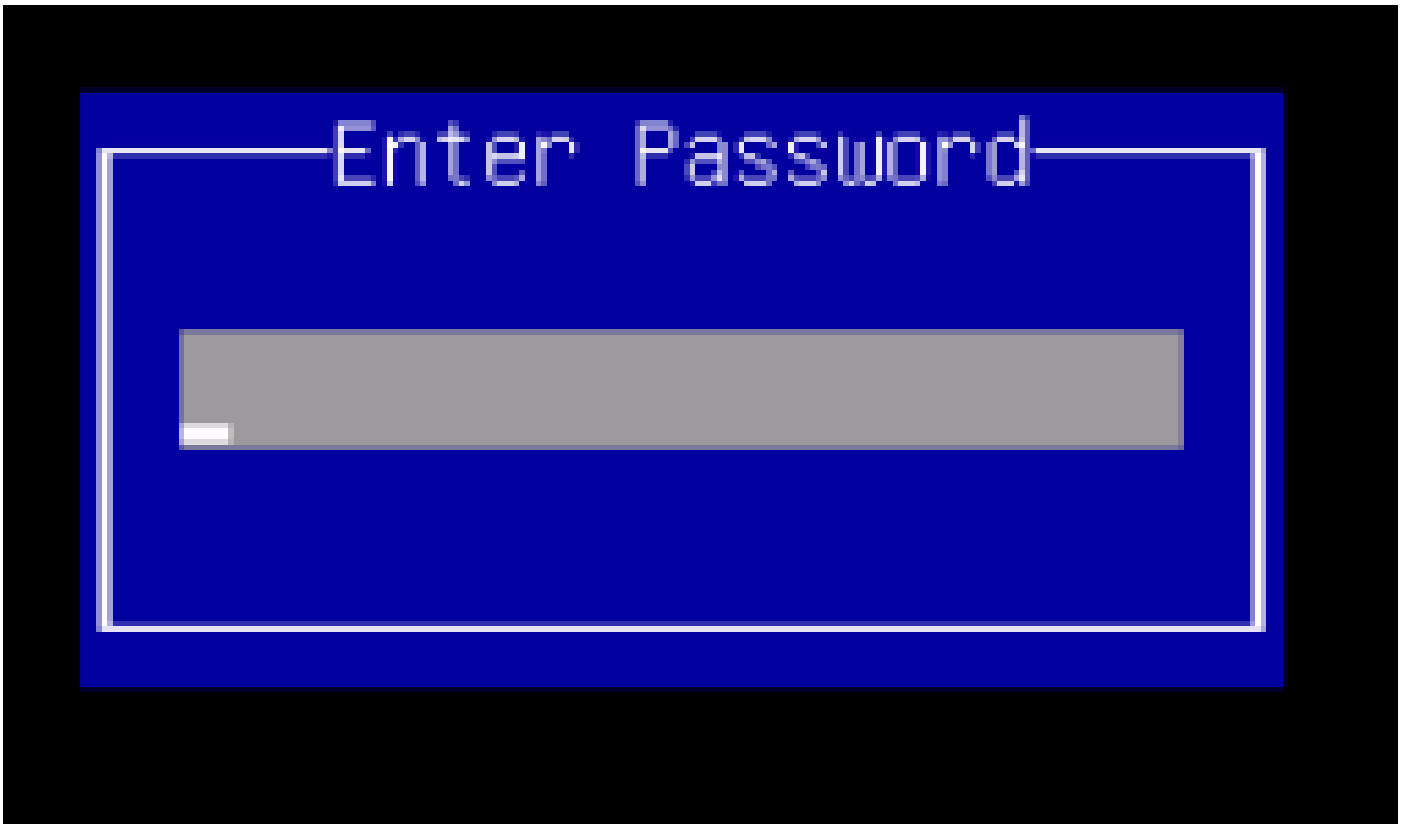


Etapa 7. Para reinicializar, navegue para Power > Reset System (warm boot) conforme mostrado na imagem.



Etapa 8. Para entrar no menu Boot, pressione F6 depois que o sistema reinicializar, como mostra a imagem.

Etapa 9. Insira a senha definida pelo usuário ou use a senha padrão, que é a senha.



Note: Você precisa definir uma senha de administrador do BIOS antes de executar este procedimento. Para definir essa senha, pressione a tecla F2 quando solicitado durante a inicialização do sistema para entrar no utilitário de configuração do BIOS. Em seguida,

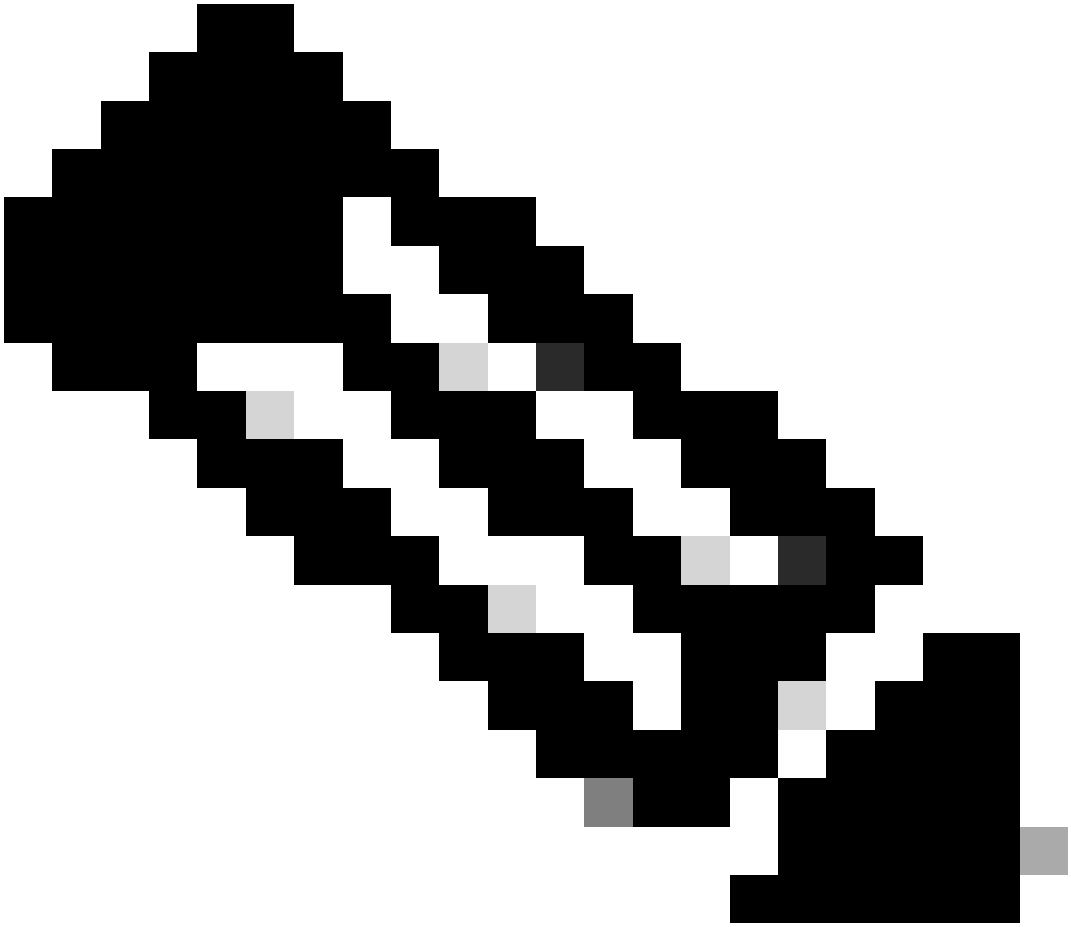
navegue até Security > Set Administrator Password e insira a nova senha duas vezes, conforme solicitado.

Etapa 10. Escolha o dispositivo de inicialização vKVM mapeado vDVD1.22 como mostrado na imagem.

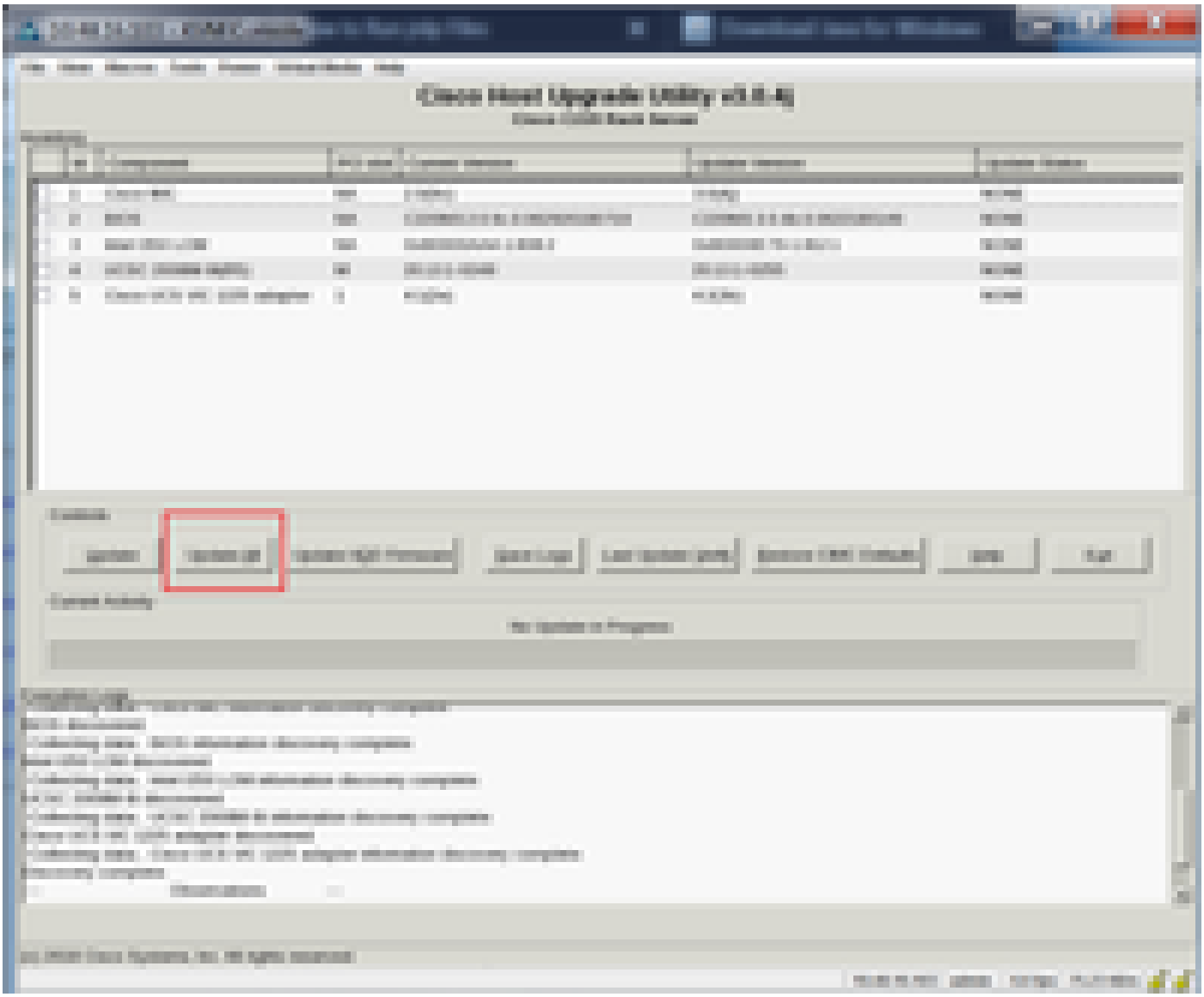
Etapa 11. Agora, o Cisco UCS Host Upgrade Utility é iniciado conforme mostrado na imagem.

Etapa 12. Leia o contrato de licençae clique em Concordo conforme mostrado na imagem.

Etapa 13. Para atualizar todos os componentes, clique em Atualizar tudo , que atualiza a versão atual para a versão atualizada.

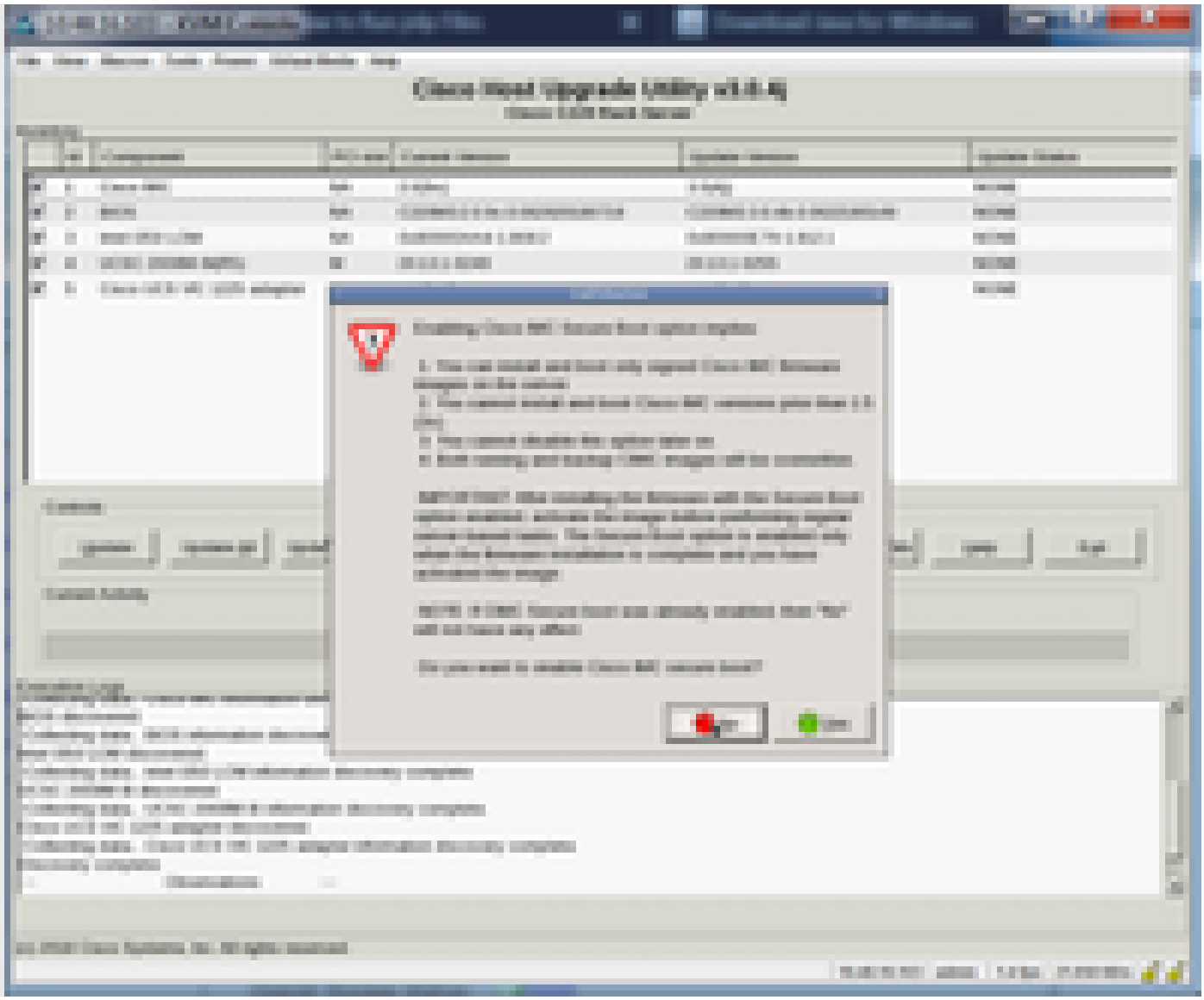


Note: Durante a atualização, o APIC pode mostrar desconexões.



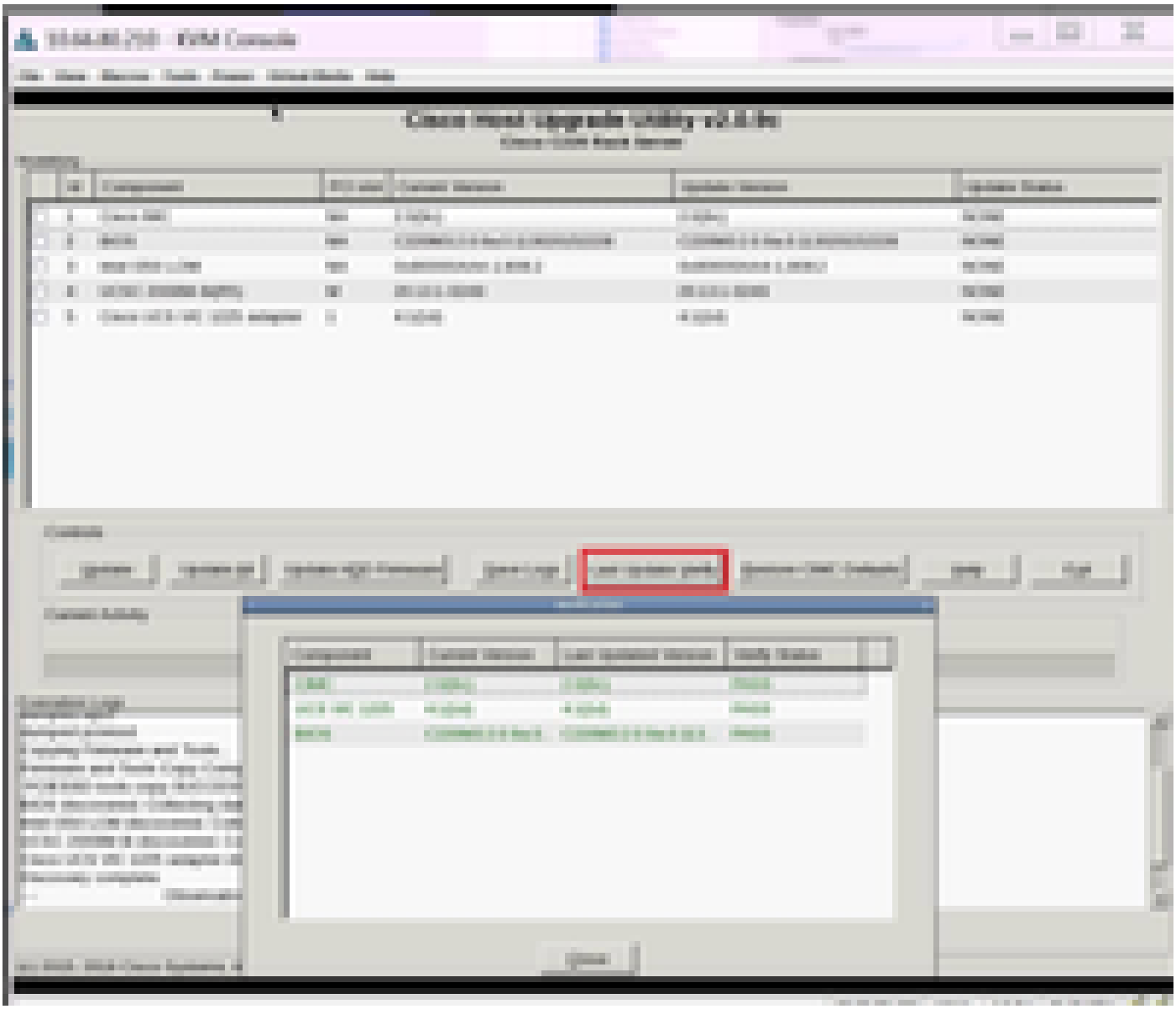
Etapa 14. Não habilitar a inicialização segura do Cisco IMC.

Uma janela pop-up é exibida para habilitar o Cisco IMC Secure Boot. Selecione NO, caso contrário, consulte a seção Introdução ao Cisco IMC Secure Boot no Guia de configuração da GUI do controlador de gerenciamento integrado dos servidores Cisco UCS C-Series, versão 4.0.

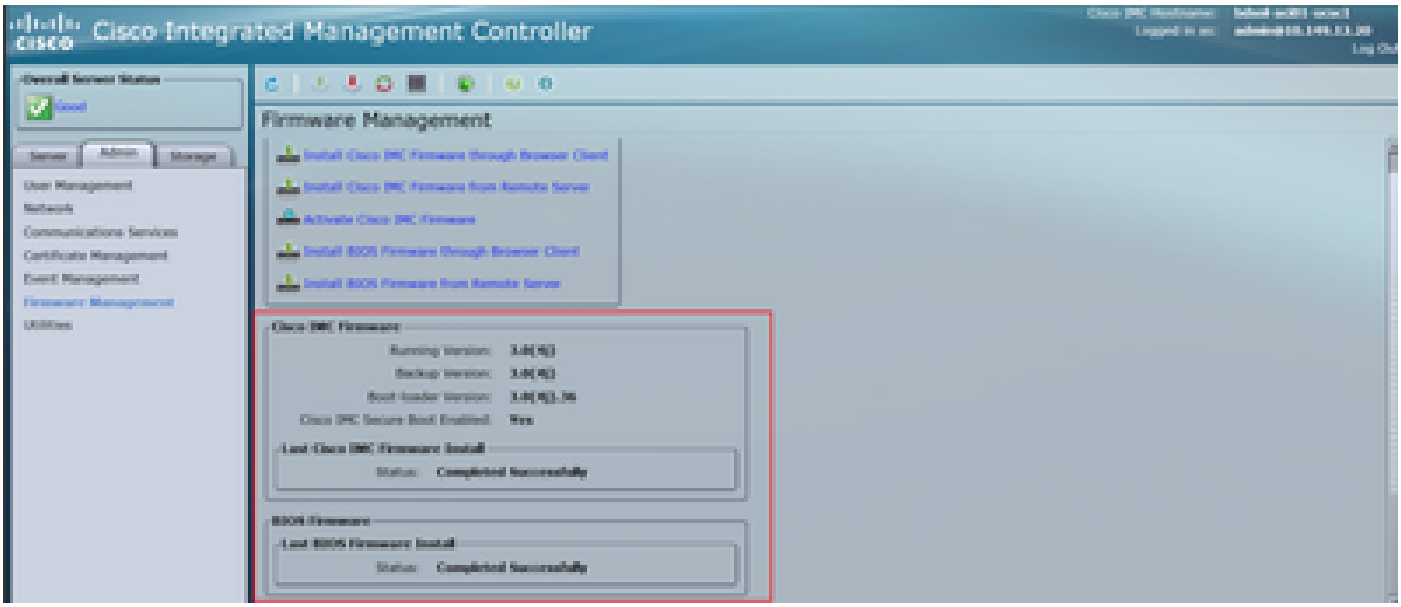


Etapa 15. O HUU atualiza cada componente individualmente. Depois de concluído, ele reinicializa a unidade e você pode acessar o chassi usando a GUI e a CLI.

Quando o servidor for reinicializado, você será removido da GUI do CIMC. Você precisa fazer login novamente no CIMC e verificar se a atualização foi concluída com êxito. Para fazer isso, você pode verificar através da GUI ou inicializar o Utilitário de atualização do host CIMC e selecionar Verificação da última atualização para garantir que todos os componentes passaram na atualização com êxito.



Etapa 16. Para verificar o upgrade bem-sucedido desta versão, inicie a sessão na GUI do CIMC e navegue até Admin > Firmware Management e verifique o Cisco IMC Firmware conforme mostrado na imagem.


Cisco Integrated Management Controller
Firmware Management
Install Cisco IMC Firmware Through Browser Client
Install Cisco IMC Firmware from Remote Server
Activate Cisco IMC Firmware
Install BIOS Firmware Through Browser Client
Install BIOS Firmware from Remote Server
Cisco IMC Firmware
Running Version:
Backup Version:
Boot-loader Version:
Cisco IMC Secure Boot Enabled:
Yes
Last Cisco IMC Firmware Install
Status:
Completed Successfully
BIOS Firmware
Last BIOS Firmware Install
Status:
Completed Successfully

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.