Guía de despliegue inalámbrico virtual del regulador de Cisco

Contenido

Introducción
prerrequisitos
Soporte virtual del regulador
Características no admitidas virtuales del controlador de WLAN
Solo requerimiento de recurso virtual del regulador
Recomendaciones sugeridas del hardware para recibir los reguladores virtuales de Cisco
Requisito AP
Componentes Utilizados
Topología
Convenciones
Release Notes
Instalación del controlador virtual
Interfaces virtuales virtuales del regulador
Configuración de la interfaz del switch conectada con el servidor UCS
Definición del modo promiscuo de VMware
Configuraciones virtuales del regulador
Puerto de la consola virtual del regulador
Comience para arriba el vWLC
Administración virtual del regulador con la prima 1.2 de Cisco
Actualice el regulador virtual
Resolución de problemas
Consideraciones AP
El tiempo es incorrecto
Hash de SSC
Información Relacionada

Introducción

Antes de la versión 7.3, el software del regulador del Wireless LAN (red inalámbrica (WLAN)) se ejecutó en el hardware dedicado que le se esperaba que comprara. El regulador virtual del Wireless LAN (vWLC) se ejecuta en el hardware general bajo infraestructura de la virtualización del estándar de la industria. El vWLC es ideal para las implementaciones pequeñas y de tamaño mediano con una infraestructura virtual y requiere un regulador de las en-premisas. Los entornos distribuidos de la bifurcación pueden también beneficiarse con un regulador virtual centralizado con menos bifurcaciones requeridas (hasta 200).

los vWLCs no son un reemplazo de los controladores de hardware del envío. La función y

características del vWLC ofrecen las ventajas del despliegue y las ventajas de los servicios de controlador donde existen o se plantean centros de datos con infraestructura de virtualización.

Ventajas del vWLC:

- Flexibilidad en la selección del hardware basada en sus requisitos.
- El coste reducido, los requisitos de memoria, y el otro overheads puesto que los cuadros múltiples se pueden substituir por las instancias múltiples corrientes del solo hardware de los reguladores, de los dispositivos de administración de red (NC) y de otros servidores (ISE, MSE, VSG/Firewall).
- Independiente y mutuamente - los casos exclusivos permiten que los administradores utilicen los reguladores virtuales múltiples para manejar diversos campus (o aún manejar los sitios de cliente múltiple) usando el mismo hardware.
- Características del permiso proporcionadas por el software de la virtualización, incluyendo la Alta disponibilidad, la protección contra fallas, y la facilidad de la migración.

Ventajas de VMware con el vWLC:

- **vSphere**: Un paquete de la infraestructura de la virtualización de VMware, que incluye el hipervisor ESX/ESXi, vMotion, los DR, HA, tolerancia de fallas, vSphere distribuyó el Switch, y más.
- **servidor del vCenter**: El servidor del vCenter de VMware (antes VMware VirtualCenter) proporciona una plataforma scalable y extensible que forme la fundación para la Administración de la virtualización:Control centralizado y visibilidad a todos los niveles de la infraestructura virtualAdministración dinámica con el vSpherePlataforma de administración scalable y extensible con un ecosistema amplio del partner

prerrequisitos

Soporte virtual del regulador

- Plataforma: AIR-CTVM-K9
- Hardware Cisco UCS, UCS expreso, HP y servidores de IBM
- VMware OS: ESX/ESXi 4.x/5.x
- Modo de FlexConnect: central y Local Switching
- Autorización: Licencias bloqueadas del nodo a UDI (60 días eval)
- Número máximo de (APS) de los Puntos de acceso: 200
- Número máximo de clientes: 3000
- Número máximo de sitios hasta 200
- Desempeño del rendimiento de procesamiento hasta el 500 Mbps por el regulador virtual
- Administración con la infraestructura 1.2 de la prima de Cisco y arriba

Características no admitidas virtuales del controlador de WLAN

Esta lista incluye las características no admitidas de la versión 7.3.112.0 del WLC y de la versión 7.4.100.60:

- Seguridad de la capa de transporte de datagrama de los datos (DTL)
- Punto de acceso de OfficeExtend (OEAP) (ningunos datos DTL)

- Limitación de la tarifa
- Limitación inalámbrica de la tarifa (contrato del ancho de banda)
- Servidor DHCP interno
- Movilidad/ancla del invitado
- Modo de multidifusión**Nota:** El tráfico Multicast conmutado local de FlexConnect se interliga transparente para atado con alambre y Tecnología inalámbrica en el mismo VLA N. Los Puntos de acceso de FlexConnect no limitan el tráfico que se basa en el Internet Group Management Protocol (IGMP) o el snooping de la detección del módulo de escucha del Multicast (MLD).
- Modo unidifusión
- PMIPv6
- IPv6
- Puntos de acceso en el modo local
- Puntos de acceso interiores de la malla
- Puntos de acceso al aire libre de la malla (un AP al aire libre con el modo de FlexConnect trabajará)**Nota:** Los AP al aire libre tales como AP1552 se soportan en el modo de FlexConnect si los AP no se utilizan en un despliegue de la malla.
- Cisco 600 Series OEAPs
- Exchange Protocol de TrustSec SGT (SXP)
- (WGB) del Work Group Bridge
- VideoStream
- Alta disponibilidad
- Movilidad jerárquica
- 802.11w
- Visibilidad y control (AVC) de la aplicación**Nota:** Vea el controlador de WLAN virtual liberar 7.5 características no admitidas en el Guía de despliegue inalámbrico virtual del regulador de Cisco, libere 7.5 para la lista actualizada.

Escoja el requerimiento de recurso virtual del regulador

- CPU: 1 CPU virtual
- Memoria: 2 GB
- Espacio en disco: 8 GB
- Interfaz de Red: el vWLC soporta un puerto para la comunicación de datos

Recomendaciones sugeridas del hardware para recibir los reguladores virtuales de Cisco

- Servidor del montaje en bastidor UCS R210-2121605W (2 RU):2 * Intel Xeon CPU X5670 @ 2.93 gigahertzMemoria de 16 G
- Servidor de IBM x3550 M3:2 * Los procesadores de las 5600 Series de Intel Xeon con 4 quitan el corazón a cada y cada base capaz de hacer roscar híper que le dé 16 CPU en gigahertz total @3.6memoria 12G
- Los servicios ISR G2 alistan el motor (SRE) usando el UCS expreso (meta del estiramiento):SRE 700: Sola base Intel Core Duo 1.86 gigahertz con la memoria 4 GBSRE 900: Dual Core Intel Core Duo 1.86 gigahertz con la memoria 4 GB (mejorable a 8 GB)

Requisito AP

- Todos los 802.11n AP con la versión 7.3 del software requerido se soportan.
- Los AP actuarán en el modo de FlexConnect solamente.
- El autoconvert AP a FlexConnect se soporta en el regulador.
- Los nuevos AP pedidos enviarán con el software 7.3 de la fabricación.
- Los AP existentes se deben actualizar al software 7.3 antes de unirse a un regulador virtual.**Nota:** El regulador virtual en la versión 7.3 utiliza los certificados firmados del uno mismo (SSC) en comparación con los Certificados instalados fabricación (MIC) en el regulador tradicional. El AP podrá validar el certificado de SSC proporcionado por el regulador virtual antes de unirse a. Vea las consideraciones AP en la sección de Troubleshooting para más detalles.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch del Cisco Catalyst
- Dispositivo virtual de los reguladores del Wireless LAN
- Software del regulador 7.3 del Wireless LAN
- Infraestructura 1.2 de la prima de Cisco
- Puntos de acceso 802.11n en el modo de FlexConnect
- Servidor DHCP
- Servidor DNS
- NTP
- Laptop, Smartphone, y tablillas del cliente de red inalámbrica (IOS de Apple, Android, Windows, y mac)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Topología

Para implementar y probar correctamente el vWLC de Cisco, una configuración de la red mínima se requiere, similar al diagrama mostrado en esta sección. Usted necesita simular una ubicación con un FlexConnect AP en un despliegue centralmente conmutado, y/o con la adición de los sitios local y remoto con el DHCP local (mejor si hay también un DNS y un Acceso local a Internet).

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Release Notes

La red del Cisco Unified Wireless (CUWN) 7.3 Release Note contiene la información importante

sobre esta versión. Inicie sesión al cisco.com para los últimos Release Note antes de cargar y de probar el software.

Instalación del controlador virtual

Para el despliegue y la Administración del vWLC, usted necesitará descargar ninguno de estos habitaciones de VMware al puesto de trabajo:

- Sola Administración del servidor de ESXi - Utilice al cliente del vSphere de VMware.
- Los servidores múltiples de ESXi requieren el vCenter - Las características anticipadas también se atan con el vCenter que necesita las licencias separadas (vMotion, y así sucesivamente).

Comience al **cliente del vSphere de VMware**, y inicie sesión al servidor de ESXi.

Interfaces virtuales virtuales del regulador

- Interfaz de administración
- Interfaz virtual
- Interfaz dinámica
- Interfaz del administrador AP

Configuración de la interfaz del switch conectada con el servidor UCS

Esta sección proporciona una configuración de muestra de la conexión de interfaz del Cisco Catalyst al servidor de ESXi para el switch virtual como interfaz de tronco. La interfaz de administración se puede conectar con un puerto de acceso en el Switch.

```
interface GigabitEthernet1/1/2
 description ESXi Management
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/1/3
 description ESXi Trunk
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

Complete estos pasos:

1. Cree dos switches virtuales separados para asociar al servicio virtual del regulador y los datos viran hacia el lado de babor. Van a **ESX** > la **configuración** > el **establecimiento de una red**, y el tecleo **agrega el establecimiento de una red**.
2. Seleccione la **máquina virtual**, y haga clic **después**.
3. Cree un vSwitch y asigne un NIC físico para conectar el puerto del servicio del vWLC. El puerto del servicio no tiene que ser conectado con cualquier parte de la red (desconectada típicamente/inusitada). Como consecuencia, cualquier NIC (incluso desconectado) se puede utilizar para este vSwitch.
4. Haga clic en Next (Siguiente).

5. Proporcione una escritura de la etiqueta (en este ejemplo, **puerto del servicio del vWLC**).
6. No seleccione **ninguno (0)** para el VLAN ID pues el puerto del servicio es típicamente un puerto de acceso.
7. Haga clic en Next (Siguiente).
8. Aquí, usted ve que vSwitch1 está creado para el puerto del servicio del vWLC. El tecleo **agrega el establecimiento de una red** para relanzar para el puerto de los datos.
9. Para el nuevo vSwitch, seleccione el NIC físico conectado en un puerto troncal si hay NIC múltiples/portgroup asignado a un EtherChannel en el Switch.
10. Agregue el NIC.
11. Haga clic en Next (Siguiente).
12. Proporcione una escritura de la etiqueta (en este ejemplo, **puerto de los datos del vWLC**).
13. Para el VLAN ID, seleccione **ALL(4095)** puesto que esto está conectada con un puerto troncal del Switch.
14. Haga clic **después** hasta que usted complete los pasos para agregar el vSwitch.

Definición del modo promiscuo de VMware

El modo promiscuo es una política de seguridad que se puede definir en el switch virtual o el portgroup llano en el vSphere ESX/ESXi. Una interfaz de la red de la máquina virtual, de la consola de servicio, o de VMkernel en un portgroup que permita el uso del modo promiscuo puede considerar todo el tráfico de la red el atravesar del switch virtual.

Por abandono, el adaptador de la red virtual de un sistema operativo del invitado recibe solamente las tramas que se significan para él. La colocación del adaptador de red del invitado en el modo promiscuo lo hace recibir todas las tramas pasajeras en el switch virtual que se permitan bajo política de VLAN para el portgroup asociado. Esto puede ser útil para la supervisión de la detección de intrusos o si un sniffer necesita analizar todo el tráfico en el segmento de red.

El puerto de los datos del vWLC requiere el vSwitch asignado validar al modo promiscuo para las operaciones correctas.

Complete estos pasos:

1. Localice vSwitch2 (asignado para el puerto de los datos del vWLC), y haga clic las **propiedades**.
2. Seleccione el VMNet asignado al puerto de los datos del vWLC (nota que fijan al modo promiscuo predeterminado de la Seguridad para rechazar), y el tecleo **edita**.
3. En la ventana de pPropiedades, seleccione la **ficha de seguridad**.
4. Marque el cuadro para el **modo promiscuo**, elija **validan de la** lista desplegable, y hacen clic la **AUTORIZACIÓN**. Es importante observar que la **dirección MAC cambia** y **forjó las transmisiones que los** campos se fijan **para validar** por abandono. Usted debe invertir estos valores **para validar** si usted los cambió de los valores predeterminados.
5. Confirme el cambio, y haga clic **cerca**.Se fija el software virtual del regulador como un paquete .ovf en el centro del software de Cisco. Usted puede descargar el paquete .ova/.ovf y instalarlo a cualquier otra aplicación virtual. El software viene con una licencia de evaluación libre del 60-día. Después de que se comience el VM, la licencia de evaluación puede ser activada y una licencia comprada se puede instalar y activar automáticamente más adelante.
6. Descargue la imagen virtual de los HUEVOS del regulador al disco local.

7. Van a **ESX >** el **archivo > despliegan la plantilla OVF** para comenzar la instalación.
8. Hojee a la ubicación de los HUEVOS clasifían (descargado del sitio de Cisco), y hacen clic **después**.
9. Haga clic en Next (Siguiente).
10. Proporcione un nombre para el vWLC o valide el valor por defecto, y haga clic **después**.
11. Valide la configuración **puesta a cero perezosa de la disposición gruesa** predeterminada, y haga clic **después**.
12. Valide el valor por defecto de la asignación de red, y haga clic **después**.
13. Confirme las configuraciones del despliegue, y el clic en Finalizar para comenzar la instalación.
14. Haga clic **cerca** cuando el despliegue es completo.

Dos asuntos importantes a observar con respecto actualizar a los reguladores virtuales:

- La imagen de los HUEVOS se necesita solamente para la instalación de la primera vez.
- La imagen .AES se puede utilizar posteriormente para actualizar/que retrocede.

Configuraciones virtuales del regulador

Después de crear el regulador virtual, configure las configuraciones de la máquina virtual para asociar el establecimiento de una red y para agregar una consola en serie virtual.

Complete estos pasos:

1. Seleccione el vWLC, y el tecleo **edita las configuraciones de la máquina virtual**.
2. **Adaptador de red** selecto **1 al puerto del servicio del vWLC** (vSwitch creado en el establecimiento de una red ESX).
3. **Adaptador de red 2 del** mapa al **puerto de los datos del vWLC**.
4. Confirme la asignación correcta.

Puerto de la consola virtual del regulador

El puerto de la consola da el acceso al prompt de consola del WLC. Como consecuencia, el VM puede ser aprovisionado con los puertos seriales para conectar con éstos. En ausencia de los puertos seriales, la consola del cliente del vSphere está conectada con la consola en el vWLC.

VMware ESXi soporta un puerto de consola en serie virtual que se pueda agregar al vWLC VM. El puerto serial se puede acceder en una de estas dos maneras:

- **Puerto de serial física en el host**: El puerto serial virtual de los vWLC se asocia al puerto serial del hardware en el servidor. Esta opción se limita al número de puertos de serial física en el host. Si en un escenario del vWLC del multi-arrendatario, esto puede no ser ideal.
- **Conecte vía la red**: El puerto serial virtual de los vWLC se puede acceder usando la sesión telnet de una máquina remota a un puerto específico afectado un aparato para el VM en el hipervisor. Por ejemplo, si la dirección IP del hipervisor es 10.10.10.10 y el puerto afectado un aparato para un vWLC VM es 9090, usando “telnet 10.10.10.10 el 9090", apenas como acceder la consola WLC físico usando un servidor terminal de Cisco, la consola en serie de los vWLC puede ser accedida.

Complete estos pasos:

1. En la lengueta del **hardware del** vWLC, haga click en Add
2. En la lengueta del **hardware del** vWLC, haga click en Add
3. En este ejemplo, elija **conectan vía la red**, y hacen clic **después**.
4. Vaya al **forro selecto de la red**:Para el forro de la red, elija el **servidor (el VM está atenta la conexión)**.Para el puerto URI, ingrese el **<host> de telnet://: <port>** (por ejemplo, telnet://10.10.10.10:9090).
5. Tecleo **después** para revisar las opciones, y clic en Finalizar.
6. Haga Click en OK para completar las configuraciones configuradas.Para habilitar para el serial vía la red, ESX se debe configurar para tener en cuenta tales peticiones.
7. Navegue al ESX, haga clic la **ficha de configuración**, vaya al **perfil del** > Security (Seguridad) del **software**, y haga clic en las **propiedades**.
8. En la **ventana de pPropiedades del Firewall**, el **puerto serial** selecto **VM conectado con el vSPC**, y la **AUTORIZACIÓN del** tecleo.

Comience para arriba el vWLC

Complete estos pasos:

1. Comience el vWLC, y seleccione la consola para observar la primera vez el proceso de instalación.
2. Monitoree el progreso hasta la consola VM muestra que el vWLC ha recomenzado (éste es automático).
3. Abra a una sesión telnet en el vWLC como se muestra aquí:
4. La sesión telnet ahora manejará la consola al vWLC.**Nota:** Solamente un modo de consola puede ser operativo en cualquier momento, por ejemplo una consola VM (por la clave-interrupción en el lanzamiento) o la consola en serie (comprobación/red). No es posible mantener ambos al mismo tiempo.
5. Continúe esperando hasta que el vWLC haya venido en línea completamente y le indique a que comience al Asisitente de la herramienta de configuración.
6. Configure el direccionamiento/la máscara/el gateway de la interfaz de administración. Configure la interfaz de administración VLAN ID si está marcado con etiqueta. Continúe con el resto.
7. Similar a todos los dispositivos de la red, configurar el NTP es crucial. El regulador virtual debe tener el reloj correcto como es posible tener un reloj incorrecto en el host ESX, o de la configuración manual, que puede dar lugar a los AP que no se unen a en el proceso.
8. Complete la configuración y permita que el vWLC reajuste.
9. Se sugiere que usted hace ping la interfaz de administración del vWLC para asegurarse de que ha venido en línea. Login al vWLC.
10. Usted puede publicar el **comando show interface summary** y hacer ping el gateway del vWLC.
11. Conecte con la Administración del vWLC usando un buscador Web
12. Inicialmente, hay 0 Puntos de acceso (cero) soportados. Permita a la licencia de evaluación para permitir que el AP se una a.
13. Vaya a la **Administración** > a la **activación de software** > a las **licencias**. Seleccione la base-ap-**cuenta**, y establezca la prioridad al **alto**.
14. El Haga Click en OK, y **valida el** EULA para continuar.
15. Haga Click en OK, y reajustado el vWLC para que la licencia de evaluación tome el efecto.
16. Reinicie el vWLC.

17. Registre detrás adentro al vWLC, y observe que los 200 AP ahora están soportados con la licencia de evaluación habilitada.
18. Conecte un AP, y monitoree para que el mensaje de incorporación ocurra.
19. Del navegador, vaya a la **TECNOLOGÍA INALÁMBRICA** y confirme que el AP se ha unido a.
20. Haga clic el AP, y cambie modo AP a **FlexConnect**. Solamente FlexConnect se soporta (central y Local Switching) en la versión 7.3.
21. Puede ser útil considerar usar la función del autoconvert del regulador (por ejemplo, cualquier modo AP que se une al vWLC será convertido automáticamente a FlexConnect). Publique este comando para implementar:`(Cisco Controller) >` **`config ap autoconvert flexconnect enable`**

Administración virtual del regulador con la prima 1.2 de Cisco

La versión 1.2 de la infraestructura de la prima de Cisco es la versión mínima requerida centralmente manejar uno o más reguladores virtuales de Cisco. La Administración para el regulador virtual de Cisco es no diferente que los Controladores físicos de la herencia con respecto a Cisco WCS o NC. Cisco prepara la infraestructura 1.2 proporciona la configuración, la administración del software, la supervisión, la información, y el troubleshooting de los reguladores virtuales. Refiera a la documentación primera de la infraestructura de Cisco como sea necesario para administrativo y el soporte de administración.

1. Inicie sesión al servidor de la infraestructura de la prima de Cisco como **raíz**. Por abandono, la selección de la opinión de la Administración es el tema del ciclo vital, que es nuevo empezando por la versión 1.2. El tema clásico (mostrado más adelante) será más familiar a los administradores que han estado trabajando en Cisco WCS y NC.
2. Va **a actuar >** el **centro de trabajo del dispositivo**.
3. En el centro de trabajo del dispositivo, el tecleo **agrega el dispositivo**.
4. Ingrese el IP Address y la cadena de comunidad SNMP (de lectura/grabación). Por abandono, el SNMP RW para el regulador es privado. Haga clic en Add (Agregar).
5. La infraestructura de la prima de Cisco descubrirá y sincronizará con el regulador virtual. El tecleo restaura para poner al día la pantalla.
6. Cuando se descubre el regulador virtual, se enumera como manejado y accesible (mostrado en el verde). Agregue cualquier otro regulador virtual en este momento, si está disponible.
7. El nuevo regulador será enumerado en el **regulador VIRTUAL del Wireless LAN del tipo de dispositivo >** de la **serie de Cisco**.
8. Navegue para dirigirse para una vista sumaria (en el tema del ciclo vital) de los dispositivos que son manejados.
9. Para el resto de esta guía, el tema clásico se utiliza para realizar la tarea similar de agregar el regulador virtual, así como de poner al día la imagen del sistema. Va a y el switch de selección al **tema clásico**.
10. Vaya a la **configuración >** a los **reguladores**.
11. Para agregar un nuevo regulador virtual, selecto **agregue los reguladores… del** selecto una lista desplegable del comando.
12. Ingrese el IP Address, la cadena de comunidad SNMP de lectura/grabación, y el haga click en Add
13. La infraestructura de la prima de Cisco visualizará esta notificación:
14. Vaya a la **configuración >** a los **reguladores**. El regulador virtual será enumerado como

accesible una vez que se ha descubierto y se ha agregado con éxito. Si no, y como se muestra arriba, el dispositivo aparecerá en la página del dispositivo desconocido si no fue descubierto con éxito.

Actualice el regulador virtual

En los pasos tempranos de la instalación, el regulador virtual de Cisco requirió inicialmente un archivo de los HUEVOS para la nueva creación virtual del dispositivo. Sin embargo, las características del regulador y las actualizaciones del software virtuales que mantienen requieren un archivo común AES transferible del sitio Web de Cisco.

Complete estos pasos:

1. Descargue el archivo AS*7_3*aes a un host de destino (por ejemplo, el servidor FTP TFTP/).
2. Apenas en cuanto a los controladores heredados, vaya a la red GUI del regulador > de los **COMANDOS** > del **archivo de la descarga**. Seleccione el tipo de archivo, el modo de la transferencia, la dirección IP, el trayecto del archivo, y el nombre del archivo (archivo .aes). Haga clic la **descarga** para comenzar el proceso.
3. Cuando el proceso ha completado con éxito, a le indican que reinicie para que la nueva imagen del software tome el efecto. Haga clic el link a la página de la reinicialización para continuar.
4. Haga clic la **salvaguardia y reinicie**.
5. Cisco prepara la infraestructura puede también ser útil para actualizar un regulador virtual o a muchos reguladores virtuales al mismo tiempo. Vaya a la **configuración** > a los **reguladores**. Seleccione (casilla de verificación) uno o más reguladores virtuales. Seleccione el **software de la descarga (TFTP) de la** lista desplegable del comando. Este ejemplo utiliza el modo TFTP para la actualización de la imagen.
6. Proporcione el tipo de la descarga, el servidor TFTP (nuevo si usa el externo), la dirección IP, el trayecto del archivo, y el nombre del archivo del servidor (que es el tipo de archivo .aes). Haga clic en **Descarga**.
7. Esta pantalla es un ejemplo de la imagen AES que es transferida a los reguladores virtuales:
8. Cisco prepara la infraestructura pondrá al día el estatus hasta que el software haya transferido con éxito.
9. Similar a la experiencia directamente del regulador, se requiere una reinicialización cuando la transferencia es completa. En la infraestructura de la prima de Cisco, vaya a la **configuración** > a los **reguladores**, y seleccione los reguladores virtuales. Seleccione los **reguladores de la reinicialización del** selecto una lista desplegable del comando….
10. Cisco prepara la infraestructura indicará para los parámetros de la reinicialización tales como configuración de la salvaguardia, y así sucesivamente. Haga clic en OK.
11. La infraestructura de la prima de Cisco notificará al administrador que se están reiniciando los reguladores virtuales.
12. Cuando es completa, la infraestructura primera de Cisco proporcionará los resultados del proceso.

Resolución de problemas

Consideraciones AP

Problema conocido AP que no se une al vWLC - El AP debe conseguir la entrada del hash de un controlador heredado antes de que se una a un vWLC.

- Un AP debe estar en la versión de software 7.3.1.35 y arriba unirse a con éxito un regulador virtual. Los reguladores virtuales utilizan SSC para validar un AP antes de unirse a.
- Un AP en la versión 7.3 puede validar el certificado de SSC proporcionado por el regulador virtual.
- Después de la validación de certificado acertada, un AP marcará la clave del hash del regulador virtual en la lista de claves salvadas en el flash. Si hace juego el hash salvado, la validación se pasa y los movimientos AP al estado de FUNCIONAMIENTO. Si la validación del hash falla, desconectará del regulador y recomenzará el proceso de detección.
- La validación del hash, que es un paso adicional de la autorización, será realizada solamente si el AP se está uniendo a un regulador virtual. Habrá un botón para dar vuelta a la validación con./desc. de la clave del hash.
- Por abandono, se habilita la validación del hash, así que significa que el AP necesita tener la clave virtual del hash del regulador en su flash antes de que pueda completar con éxito la asociación con el regulador virtual. Si se apaga el botón, el AP desviará la validación y el movimiento del hash directamente al estado de FUNCIONAMIENTO.
- La clave del hash se puede configurar en las configuraciones de la movilidad del regulador, que consigue avanzada a todos los AP se unen a que. El AP salvará esta configuración hasta que se asocie con éxito a otro regulador. Después de lo cual, hereda la configuración de la clave del hash del nuevo regulador.
- Típicamente, los AP pueden unirse a un regulador tradicional, descargan las claves del hash, y después se unen a un regulador virtual. Sin embargo, si se une a un regulador tradicional, el botón de la validación del hash puede ser apagado y puede unirse a cualquier regulador virtual. El administrador puede decidir mantener el botón con./desc.

Esta información se captura en el Id. de bug Cisco CSCua55382.

Exceptions:

- Si el AP no tiene ninguna clave del hash en su flash, desviará la validación del hash, si se asume que es una instalación de la primera vez.En este caso, la validación del hash se desvía con independencia de si el botón de la validación del hash es con./desc.Una vez que se une a con éxito el regulador, heredará la configuración del hash del miembro de grupo de movilidad (si está configurado en el regulador). Después de lo cual, puede unirse a un regulador virtual solamente si tiene una entrada dominante del hash en su base de datos.
- Borrar la configuración AP del regulador o en la consola AP dará lugar a la borradura de todas las claves del hash. Después de lo cual, el AP se une al regulador virtual como si sea una instalación de la primera vez.`Borrado del capwap de la prueba AP>Reinicio del capwap de la prueba AP>`

El tiempo es incorrecto

- En la inicial instale, es posible que el tiempo puede ser sesgado o sincronizó no correctamente. Como consecuencia, el AP puede no poder unirse a correctamente. El en este caso, marca el sello de fecha/hora de la validez de SSC para asegurarse de que está correcto. El NTP es siempre el ir recomendado adelante.`(Cisco Controller) >`**`show certificate ssc`** `SSC Hash validation..... Enabled. SSC Device Certificate details: Subject Name : C=US, ST=California, L=San Jose, O=Cisco Virtual Wireless LAN`

Controller, CN=DEVICE-vWLC-AIR-CTVM-K9-000C29085BB8, MAILTO=support@vwlc.com Validity : **Start : 2012 Jun 8th, 17:52:46 GMT End : 2022 Apr 17th, 17:52:46 GMT** Hash key : **bd7bb60436202e830802be1e8931d539b67b2537**

Hash de SSC

- El AP es un nuevo AP con 7.3 y no tiene hash puede unirse al WLC virtual fácilmente:ap#**show capwap client config**
- El AP puede tener un hash más viejo de SSC, de una vieja instalación o de unirse a otros reguladores. Es posible configurar el WLC para no validar SSC, permite que los AP se unan al vWLC, entonces volviendo a permitir la validación otra vez.(Cisco Controller) >**configure certificate ssc hash validation disable**
- Realice el comando del **capwap** *<erase/restart> de la* **prueba** para borrar las configuraciones del capwap AP y el iniciado se une al proceso.APf866.f267.67af#**test capwap erase** APf866.f267.67af#**test capwap restart** restart capwap APf866.f267.67af# *Jun 9 12:27:22.469: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 10.10.11.20:5246 *Jun 9 12:27:22.525: %WIDS-6-DISABLED: IDS Signature is removed and disabled. *Jun 9 12:27:22.529: %LWAPP-3-CLIENTERRORLOG: LWAPP LED Init: incorrect led state 255 *Jun 9 12:27:22.897: Starting Ethernet promiscuous mode *Jun 9 12:27:32.903: %CAPWAP-3-ERRORLOG: Go join a capwap controller *Jun 9 12:27:23.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 10.10.11.20 peer_port: 5246 *Jun 9 12:27:23.276: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: 10.10.11.20 peer_port: 5246 *Jun 9 12:27:23.276: %CAPWAP-5-SENDJOIN: sending Join Request to 10.10.11.20
- Como parte de la configuración de la movilidad, si hay regulador virtual en la red, el administrador necesita agregar una clave del hash del regulador virtual en todos los reguladores del par. Si agrega otro regulador del par, la consideración es agregar el hash (mostrado en SSC hecho salir arriba) al miembro de grupo de movilidad.(Cisco Controller) >**config mobility group member add 10.10.11.30** (Cisco Controller) >**config mobility group member hash 10.10.11.30 bd7bb60436202e830802be1e8931d539b67b2537**

Información Relacionada

- Matriz de la función de FlexConnect
- Documentación del REVESTIMIENTO de Cisco
- Guía de despliegue del regulador de bifurcación de la Tecnología inalámbrica de la flexión 7500
- Soporte Técnico y Documentación - Cisco Systems