Postura de la versión 1.4 de la configuración ISE con Microsoft WSUS

Contenido

Introducción

Este documento describe cómo configurar las funciones de la postura del Cisco Identity Services Engine (ISE) cuando se integra con los servicios de la actualización del Microsoft Windows server (WSUS).

Nota: Cuando usted accede la red, le reorientan al ISE para el aprovisionamiento de la versión 4.1 del Cliente de movilidad Cisco AnyConnect Secure con un módulo de la postura, que marca el Estado de cumplimiento en el WSUS y instala las actualizaciones necesarias para que la estación sea obediente. Una vez que la estación está señalada como obediente, el ISE permite el acceso a la red completo.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementaciones, autenticación, y autorización de Cisco ISE
- El conocimiento básico sobre la manera de la cual el ISE y Cisco AnyConnect posture el agente actúa
- Configuración del dispositivo de seguridad adaptante de Cisco (ASA)
- Conocimiento básico VPN y del 802.1x
- Configuración de Microsoft WSUS

Componentes Utilizados

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

- Versión 7 de Microsoft Windows
- Versión 2012 de Microsoft Windows con la versión 6.3 WSUS
- Versiones de ASA 9.3.1 de Cisco y posterior
- Versiones de software 1.3 de Cisco ISE y posterior

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.

Configurar

Esta sección describe cómo configurar el ISE y los elementos de redes relacionados.

Diagrama de la red

Ésta es la topología que se utiliza para los ejemplos en este documento:

Aquí está el flujo de tráfico, como se ilustra en el diagrama de la red:

1. El usuario remoto conecta con Cisco AnyConnect para el acceso VPN al ASA. Éste puede ser cualquier tipo de acceso unificado, tal como una sesión atada con alambre de puente de la autenticación 802.1x/MAC (MAB) que se termine en el Switch o una sesión inalámbrica que se termine en el regulador del Wireless LAN (WLC).

2. Como parte del proceso de autenticación, el ISE confirma que el estatus de la postura de la estación terminal no es igual a obediente (regla de la autorización de *ASA-VPN_quarantine*) y que los atributos del cambio de dirección están vueltos en el mensaje del *access-accept del radio*. Como consecuencia, el ASA reorienta todo el tráfico HTTP al ISE.

3. El usuario abre a un buscador Web y ingresa cualquier direccionamiento. Después del cambio de dirección al ISE, el módulo de la postura de Cisco AnyConnect 4 está instalado en la estación. El módulo de la postura entonces descarga las directivas del ISE (requisito para WSUS).

4. El módulo de la postura busca para Microsoft WSUS, y realiza la corrección.

5. Después de la corrección acertada, el módulo de la postura envía un informe al ISE.

6. El ISE publica un cambio del radio de la autorización (CoA) que proporciona el acceso a la red completo a un usuario de VPN obediente (regla de la autorización de *ASA-VPN_compliant*).

   Nota: Para que la corrección trabaje (la capacidad de instalar las actualizaciones de Microsoft Windows en un PC), el usuario debe tener derechos administrativos locales.

Microsoft WSUS

> Nota: Una configuración detallada del WSUS está fuera del ámbito de este documento. Para los detalles, refiera a los servicios de la actualización del Servidor Windows del desplegar en su documentación de Microsoft de la organización.

El servicio WSUS se despliega a través del puerto TCP estándar 8530. Es importante recordar que para la corrección, otros puertos también están utilizados. Esta es la razón por la cual es seguro agregar la dirección IP de WSUS a la lista de control de acceso (ACL) del cambio de dirección en el ASA (descrito más adelante en este documento).

La directiva del grupo para el dominio se configura para las actualizaciones y las puntas de Microsoft Windows al servidor local WSUS:

Éstas son las actualizaciones recomendadas que se habilitan para las directivas granulares que se basan en diversos niveles de gravedad:

El alcance del client cara permite la flexibilidad lejos mayor. El ISE puede utilizar las directivas de la postura que se basan en los diversos envases del ordenador del Microsoft Active Directory (AD). El WSUS puede aprobar las actualizaciones que se basan en esta calidad de miembro.

ASA

El acceso simple de Secure Sockets Layer (SSL) VPN para el usuario remoto se emplea (los detalles cuyo esté fuera del ámbito de este documento).

Aquí está un ejemplo de configuración:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 10
 ip address 172.16.32.100 255.255.255.0

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.31.100 255.255.255.0

aaa-server ISE protocol radius
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (inside) host 172.16.31.202
 key cisco

webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 error-recovery disable

group-policy POLICY internal
group-policy POLICY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group SSLVPN type remote-access
tunnel-group SSLVPN general-attributes
 address-pool POOL-VPN
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy POLICY

ip local pool POOL-VPN 172.16.50.50-172.16.50.60 mask 255.255.255.0
```

Es importante configurar una lista de acceso en el ASA, que se utiliza para determinar el tráfico que se debe reorientar al ISE (para los usuarios que no son todavía obedientes):

```
access-list Posture-redirect extended deny udp any any eq domain
access-list Posture-redirect extended deny ip any host 172.16.31.103
access-list Posture-redirect extended deny ip any host 172.16.31.202
access-list Posture-redirect extended deny icmp any any
access-list Posture-redirect extended permit tcp any any eq www
```

Solamente el Domain Name System (DNS), el ISE, WSUS, y el tráfico del Internet Control Message Protocol (ICMP) se permite para los usuarios no obedientes. Todo el otro tráfico (HTTP) se reorienta al ISE para el aprovisionamiento de AnyConnect 4, que es responsable de la postura

y de la corrección.

ISE

> Nota: El aprovisionamiento y la postura de AnyConnect 4 está fuera del ámbito de este documento. Refiera a la integración de AnyConnect 4.0 con el ejemplo de configuración de la versión 1.3 ISE para más detalles, tales como cómo configurar el ASA como dispositivo de red y instalar la aplicación de Cisco AnyConnect 7.

Posture la corrección para WSUS

Complete estos pasos para configurar la corrección de la postura para WSUS:

1. Navegue a la **directiva > a las condiciones > a la corrección de las acciones de la postura > de la corrección > de los servicios de la actualización del Servidor Windows** para crear una nueva regla.

2. Verifique que la determinación de las *actualizaciones de Microsoft Windows* esté fijada al **nivel de gravedad**. Esta parte es responsable de la detección si se inicia el proceso de la corrección.

El agente de la actualización de Microsoft Windows después conecta con el WSUS y marca si hay algunas actualizaciones *críticas* para ese PC que aguarden la instalación:

Requisito de la postura para WSUS

Navegue a la **directiva > a las condiciones > a la postura > a los requisitos** para crear una nueva regla. La regla utiliza una condición simulada llamada *pr_WSUSRule*, así que significa que el WSUS está entrado en contacto para marcar para saber si hay la condición cuando la corrección es necesaria (las actualizaciones *críticas*).

Una vez que se cumple esta condición, el WSUS instala las actualizaciones que se han configurado para ese PC. Éstos pueden incluir cualquier tipo de actualizaciones, y también ésos con la gravedad inferior nivelan:

Perfil de AnyConnect

Configure el perfil del módulo de la postura, junto con el perfil de AnyConnect 4 (según lo descrito en la integración de AnyConnect 4.0 con el ejemplo de configuración de la versión 1.3 ISE):

Reglas del aprovisionamiento del cliente

Una vez que el perfil de AnyConnect está listo, puede ser referido de la directiva de *aprovisionamiento del cliente*:

La aplicación entera, junto con la configuración, está instalada en el punto final, que se reorienta al cliente Provisioning la página porta. AnyConnect 4 pudo ser actualizado y un módulo adicional (postura) ser instalado.

Perfiles de la autorización

Cree un perfil de la autorización para el cambio de dirección al perfil del aprovisionamiento del cliente:

Reglas de la autorización

Esta imagen muestra las reglas de la autorización:

Por primera vez, se utiliza la regla de *ASA-VPN_quarantine*. Como consecuencia, se vuelve el perfil de la autorización de la *postura*, y el punto final se reorienta al portal de disposición del cliente para el aprovisionamiento de AnyConnect 4 (con el módulo de la postura).

Una vez que es obediente, se utiliza la regla de *ASA-VPN_compliant* y se permite el acceso a la red completo.

Verificación

Esta sección proporciona la información que usted puede utilizar para verificar que usted configuración trabaja correctamente.

PC con las directivas actualizadas GPO

Las políticas de dominio con la configuración WSUS se deben avanzar después de los registros PC en el dominio. Esto puede ocurrir antes de que establezcan a la sesión de VPN (fuera de la banda) o después si el *comienzo antes de que* se utilicen las funciones del *inicio* (él se puede también utilizar para el 802.1x atado con alambre/acceso de red inalámbrica).

Una vez que el cliente de Microsoft Windows tiene la configuración correcta, esto se puede reflejar de las configuraciones de Windows Update:

Si es necesario, un objeto de la directiva del grupo (GPO) restaura y servidor del agente de la actualización de Microsoft Windows que la detección puede ser utilizada:

```
C:\Users\Administrator>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.


C:\Users\Administrator>wuauclt.exe /detectnow

C:\Users\Administrator>
```

Apruebe una actualización crítica en el WSUS

El proceso de aprobación puede beneficiarse del alcance del sitio del cliente:

Vuelva a enviar el informe con el *wuauclt* si es necesario.

Marque el estatus PC en el WSUS

Esta imagen muestra cómo marcar el estatus PC en el WSUS:

Una actualización se debe instalar para el siguiente restaura con el WSUS.

Sesión de VPN establecida

Después de que establezcan a la sesión de VPN, se utiliza la regla de la autorización de *ASA-VPN_quarantine* ISE, que vuelve el perfil de la autorización de la *postura*. Como consecuencia, el tráfico HTTP del punto final se reorienta para los 4 aprovisionamientos del módulo de la actualización y de la postura de AnyConnect:

En este momento, el estatus de la sesión en el ASA indica el acceso limitado con el cambio de dirección del tráfico HTTP al ISE:

```
asav# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 69
Assigned IP  : 172.16.50.50           Public IP    : 192.168.10.21

<...some output omitted for clarity...>

ISE Posture:
  Redirect URL : https://ise14.example.com:8443/portal/gateway?sessionId=ac101f64000
45000556b6a3b&portal=283258a0-e96e-...
  Redirect ACL : Posture-redirec
```

El módulo de la postura recibe las directivas del ISE y realiza la corrección

El módulo de la postura recibe las directivas del ISE. Los debugs de **ise-psc.log** muestran el requisito que se envía al módulo de la postura:

```
2015-06-05 07:33:40,493 DEBUG  [portal-http-service12][] cisco.cpm.posture.runtime.
PostureHandlerImpl -:cisco:ac101f6400037000556b40c1:::- NAC agent xml
<?xml version="1.0" encoding="UTF-8"?><cleanmachines>
 <version>2</version>
 <encryption>0</encryption>
 <package>
   <id>10</id>
   <name>WSUS</name>
   <version/>
   <description>This endpoint has failed check for any AS installation</description>
   <type>10</type>
   <optional>0</optional>
    <path>42#1</path>
```

```
   <remediation_type>1</remediation_type>
   <remediation_retry>0</remediation_retry>
   <remediation_delay>0</remediation_delay>
   <action>10</action>
   <check>
      <id>pr_WSUSCheck</id>
   </check>
   <criteria/>
 </package>
</cleanmachines>
```

El módulo de la postura acciona automáticamente el agente de la actualización de Microsoft Windows para conectar con el WSUS y para descargar las actualizaciones como está configurado en las directivas WSUS (todas automáticamente sin cualquier intervención del usuario):

Nota: Algunas de las actualizaciones pudieron requerir un reinicio de sistema.

Acceso a la red completo

Usted verá esto después de que la estación sea señalada como obediente por el módulo de la postura de AnyConnect:

El informe se envía al ISE, que evalúa de nuevo la directiva y golpea la regla de la autorización de *ASA-VPN_compliant*. Esto proporciona el acceso a la red completo (vía el CoA del radio). Navegue a las **operaciones > a las autenticaciones** para confirmar esto:

Los debugs (**ise-psc.log**) también confirman el Estado de cumplimiento, el activador CoA, y las configuraciones finales para la postura:

```
DEBUG  [portal-http-service17][] cisco.cpm.posture.runtime.PostureManager -:cisco:
ac101f6400039000556b4200:::- Posture report token for endpoint mac
08-00-27-DA-EF-AD is Healthy
DEBUG  [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:
ac101f6400039000556b4200:::- entering triggerPostureCoA for session
ac101f6400039000556b4200
DEBUG  [portal-http-service17][] cisco.cpm.posture.runtime.PostureCoA -:cisco:ac
101f6400039000556b4200:::- Posture CoA is scheduled for session id
[ac101f6400039000556b4200]

DEBUG  [portal-http-service17][] cisco.cpm.posture.runtime.PostureHandlerImpl -:cisco:
ac101f6400039000556b4200:::- DM_PKG report non-AUP:html = <!--X-Perfigo-DM-Error=0-->
<!--error=0--><!--X-Perfigo-DmLogoff-Exit=0--><!--X-Perfigo-Gp-Update=0-->
<!--X-Perfigo-Auto-Close-Login-Scr=0--><!--X-Perfigo-Auto-Close-Login-Scr-Time=0-->
<!--user role=--><!--X-Perfigo-OrigRole=--><!--X-Perfigo-UserKey=dummykey-->
<!--X-Perfigo-RedirectUrl=--><!--X-Perfigo-ShowInfo=--><!--X-Perfigo-Session=-->
<!--X-Perfigo-SSO-Done=1--><!--X-Perfigo-Provider=Device Filter-->
<!--X-Perfigo-UserName=cisco--><!--X-Perfigo-DHCP-Release-Delay=4-->
<!--X-Perfigo-DHCP-Renew-Delay=1--><!--X-Perfigo-Client-MAC=08:00:27:DA:EF:AD-->

DEBUG  [pool-183-thread-1][]cisco.cpm.posture.runtime.PostureCoA -:cisco:
ac101f6400036000556b3f52:::- Posture CoA is triggered for endpoint [08-00-27-da-ef-ad]
with session [ac101f6400039000556b4200]
```

También, el informe de evaluación detallado ISE de la postura confirma que la estación es obediente:

Nota: El Media Access Control (MAC) Address exacto de la interfaz de red física en

Microsoft Windows PC se sabe debido a las Extensiones de ACIDEX.

Troubleshooting

No hay actualmente información de Troubleshooting disponible para esta configuración.

Notas importantes

Esta sección proporciona una cierta información importante sobre la configuración que se describe en este documento.

Detalles de la opción para la corrección WSUS

Es importante distinguir la condición del requisito de la corrección. AnyConnect acciona el agente de la actualización de Microsoft Windows para marcar la conformidad, dependiente sobre las *actualizaciones de Windows del validar usando la* configuración de la corrección.

Por este ejemplo, se utiliza el *nivel de gravedad*. Con la configuración *crítica*, el agente de Microsoft Windows marca si hay () actualizaciones críticas no instaladas pendientes. Si hay, después la corrección comienza.

El proceso de la corrección pudo entonces instalar todas las actualizaciones críticas y menos importantes basadas en la configuración WSUS (actualizaciones aprobadas para la máquina específica).

Con *Windows del validar las actualizaciones usando el* conjunto como **Cisco gobiernan**, las condiciones que se detallan en el requisito deciden a si la estación es obediente.

Servicio de Windows Update

Para las implementaciones sin un servidor WSUS, hay otro tipo de la corrección que puede ser utilizado llamó la *corrección de Windows Update*:

Este tipo de la corrección permite el control sobre las configuraciones de la actualización de Microsoft Windows y le permite para realizar las actualizaciones inmediatas. Una condición típica que se utiliza con este tipo de la corrección es *pc_AutoUpdateCheck*. Esto permite que usted marque si la configuración de la actualización de Microsoft Windows esté habilitada en el punto final. Si no, usted puede habilitarlo y realizar la actualización.

Integración SCCM

Una nueva función para la versión 1.4 ISE llamada *Administración de la corrección* permite la integración con muchos proveedores externos. El dependiente sobre el vendedor, las opciones múltiples está disponible para las condiciones y las correcciones.

Para Microsoft, soportan el servidor de la administración del sistema (SMS) y al administrador de configuración de System Center (SCCM).

Información Relacionada

- Servicios de la postura en la guía de configuración de Cisco ISE
- Guía del administrador del Cisco Identity Services Engine, versión 1.4
- Guía del administrador del Cisco Identity Services Engine, versión 1.3
- Despliegue los servicios de la actualización del Servidor Windows en su organización
- Soporte Técnico y Documentación - Cisco Systems