Configure el portal del invitado del 2.1 ISE con PingFederate SAML SSO

Contenido

Introducción

Este documento describe cómo configurar la versión 2.1 del Cisco Identity Services Engine (ISE) para proporcionar las solas capacidades de On(SSO) de la muestra para los usuarios porta del invitado con el lenguaje de marcado de la aserción de la Seguridad (SAML).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios del invitado del Cisco Identity Services Engine.
- Conocimiento básico sobre SAML SSO.

Componentes Utilizados

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

- Versión 2.1 del Cisco Identity Services Engine
- Servidor de PingFederate 8.1.3.0 de la identidad del ping como identidad Provider(IdP) de SAML

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 su red está viva, aseegurese que usted entiende el impacto potencial de cualquier configuración aplicada.

Descripción del flujo

SAML es un estándar XML basado para intercambiar los datos de la autenticación y autorización entre los dominios de seguridad.

SAML la especificación define tres papeles: el director (Usuario invitado), el [IdP] del proveedor de la identidad (servidor federado de IPing), y el proveedor de servicio [SP] (ISE).

En un flujo típico de SAML SSO, el SP pide y obtiene una aserción de la identidad del IdP. De acuerdo con este resultado, el ISE puede realizar las decisiones de políticas mientras que el IdP puede incluir los atributos configurables que el ISE puede utilizar (es decir grupo y dirección de correo electrónico asociados al objeto AD).

Flujo previsto para este caso del uso

1. El regulador del Wireless LAN (WLC) o el switch de acceso se configura para un flujo central típico de la autenticación Web (CWA).

   Consejo: Encuentre los ejemplos de configuración para los flujos CWA en la sección de información relacionada en la parte inferior del artículo.

2. El cliente conecta y la sesión consigue autenticada contra el ISE. El acceso a la red Device(NAD) aplica los pares del valor de atributos de la reorientación (AVP) vueltos por el ISE (el URL-reorientar-ACL y URL-reorienta).

3. El cliente abre al navegador, genera el tráfico HTTP o HTTPS, y consigue reorientado al portal del invitado ISE.

4. Una vez en el portal el cliente podrá ingresar las credenciales previamente asignadas del invitado (**patrocinador creado**) y la uno mismo-disposición una nueva cuenta del invitado o utilizar sus credenciales AD para iniciar sesión (**login del empleado**) que proporcionen la sola muestra en las capacidades a través SAML.

5. Una vez que el usuario selecciona la opción del “login del empleado”, el ISE verifica si hay una aserción activa asociada a la sesión del buscador de este cliente contra el IdP. Si no hay sesiones activas, el IdP aplicará el ingreso del usuario al sistema. En este paso se indicará al usuario que ingrese las credenciales AD en el portal de IdP directamente.

6. El IdP autentica al usuario vía el LDAP y crea una nueva aserción que permanezca viva por un tiempo configurable.

   Nota: El ping federado por abandono aplica un **tiempo de espera de la sesión de** 60 minutos (éste significa que si no hay pedidos de registro SSO del ISE en 60 minutos después de autenticación inicial la sesión está borrada) y un **descanso máximo de la sesión de** 480 minutos (incluso si el IdP ha recibido los pedidos de registro constantes SSO del ISE para

este usuario que la sesión expirará en 8 horas).

Mientras la sesión de la aserción sea todavía activa, el empleado experimentará el SSO cuando él utiliza el portal del invitado. Una vez los tiempos de la sesión hacia fuera, una autenticación de usuario nuevo será aplicada por el IdP.

Configurar

Esta sección discute los pasos para la configuración para integrar el ISE con el ping federado y cómo habilitar al navegador SSO para el portal del invitado.

> Nota: Aunque existan las diversas opciones y posibilidades cuando usted autentica a los Usuarios invitados, no todas las combinaciones se describen en este documento. Sin embargo, este ejemplo provee de usted la información necesaria entender cómo modificar el ejemplo a la configuración exacta que usted quiere alcanzar.

Paso 1. Prepare el ISE para utilizar un proveedor externo de la identidad de SAML

1. En Cisco ISE, elija la **administración > la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores identificación**.
2. Haga clic en Add (Agregar).
3. Bajo lengueta de **Genaral**, ingrese un **nombre del proveedor identificación**. Haga clic en Save (Guardar). El resto de la configuración en esta sección depende de los meta datos que necesite ser importada del IdP en pasos posteriores.

Paso 2. Configure el portal del invitado para utilizar un proveedor externo de la identidad

1. Elija los **centros de trabajo > el acceso de invitado > la configuración > los portales del invitado.**
2. Cree un nuevo porta y elija el **portal Uno mismo-registrado del invitado**.

> Nota: Éste no será el portal principal que la experiencia del usuario pero un subportal que obrará recíprocamente con el IdP para verificar el estatus de la sesión. Este portal se llama SSOSubPortal.

3. Amplíe las **configuraciones porta** y elija **PingFederate** para el **método de autentificación**.

4. **De la secuencia de la fuente de la identidad,** elija el defined(PingFederate) externo de SAML IdP previamente.

5. Amplíe las secciones de las **paginaciones del banner de Acceptable Use Policy(AUP)** y del Poste-**login** y inhabilite ambos.

El flujo porta es:

6. Guarde los cambios.

7. Vuelva a los portales del invitado y cree un nuevo usando la opción Uno mismo-**registradoa del portal del invitado.**

> Nota: Éste será el visible porta primario al cliente. El portal primario utilizará el SSOSubportal como interfaz entre el ISE y el IdP. Este portal se llama PrimaryPortal.

8. Amplíe las **paginaciones del login** y elija el **SSOSubPortal** creado previamente bajo "**permiten que el portal siguiente del invitado del identidad-proveedor sea utilizado para el login**".

9. Amplíe las **paginaciones del banner AUP y del Poste-login del Acceptable Use Policy** y desmarquelas.

En este momento el flujo porta debe parecer esto:

10. Elija el **arreglo para requisitos particulares > las páginas > el login porta**. Usted debe ahora tener la opción para personalizar las **opciones alternativas del login** (icono, texto, y así sucesivamente).

> Nota: Note eso en el lado derecho, bajo avance porta, la opción adicional del login es visible.

11. Haga clic en Save (Guardar).

Ahora ambos portales aparecen conforme a la lista del portal del invitado.

Paso 3. Configure PingFederate para actuar como proveedor de la identidad para el portal del invitado ISE

1. En el ISE, elija la **administración > la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores > PingFederate identificación** y haga clic la **información del proveedor de servicio.**
2. Conforme a la **información del proveedor de servicio de la exportación,** haga clic la **exportación.**

3. Salve y extraiga archivo zip generado. El archivo XML contenido aquí se utiliza para crear el perfil en PingFederate en pasos posteriores.

> Nota: Desde aquí, este documentos abarca la configuración de PingFederate. Esta configuración es lo mismo para las soluciones múltiples como el portal del patrocinador, MyDevices, y los portales BYOD. (Esas soluciones no se cubren en este artículo).

4. Abra el portal de PingFederate admin (típicamente https://ip:9999/pingfederate/app).

5. Bajo la **ficha de configuración de IdP > conexiones SP que la** sección elige **cree nuevo**.

6. Bajo el **Tipo de conexión,** haga clic **después.**

7. Bajo **opciones de conexión,** haga clic **después.**

8. Bajo **meta datos de la importación**, haga clic el botón de radio del **archivo**, el tecleo **eligió el archivo** y elige el archivo XML exportado previamente del ISE.

el resumen de los meta datos 9.Under, hace clic **después**.

10.On la página de la información general, bajo nombre de la conexión, ingresan un nombre (tal como ISEGuestWebAuth) y hacen clic **después**.

11. Bajo **navegador SSO,** haga clic al **navegador SSO de la configuración** y bajo control de los **perfiles de SAML las** opciones y haga clic **después**.

tecleo del **curso de la vida de la aserción** 12.On **después.**

creación de la aserción de la configuración del tecleo de la **creación de la aserción** 13.On**.**

la asignación de la identidad 14.Under elige el **estándar** y hace clic **después.**

15. En el **contrato del atributo > extienda el contrato** ingresan el **correo de los** atributos y el **memberOf** y el tecleo **agregan**. Haga clic en Next (Siguiente).

La configuración de esta opción permite que el proveedor de la identidad pase el **MemberOf** y **envíe por correo electrónico los** atributos proporcionados por el Active Directory al ISE, que el ISE puede utilizar más adelante como condición durante la decisión de políticas.

caso del adaptador del mapa del tecleo de la **asignación de la fuente de la autenticación** 16.Under **nuevo**.

el caso del adaptador 17.On elige el **adaptador de la forma HTML**. Tecleo **después**

18. Bajo **métodos de la asignación** elija la segunda opción abajo y haga clic **después.**

19. En las **fuentes del atributo y el** tecleo de las **operaciones de búsqueda del usuario agregue el cuadro de la fuente del atributo.**

20. Bajo el **almacén de los datos** ingrese una descripción, y elija el caso de la conexión LDAP del **almacén activo de los datos** y defina qué tipo de servicio de directorio es éste. Si no hay **almacenes de datos** configurados con todo el tecleo **maneja los almacenes de datos** para agregar la nueva instancia.

21. Bajo la **búsqueda del directorio LDAP** defina la **base DN** para las operaciones de búsqueda del usuario LDAP en el dominio y haga clic **después**.

> Nota: Esto es importante pues definirá la base DN durante las operaciones de búsqueda del usuario LDAP. Una base incorrectamente definida DN dará lugar al objeto no encontrado en el esquema LDAP.

el filtro 22.Under **LDAP** agrega la cadena **sAMAccountName=$ {nombre de usuario}** y hace clic **después**.

23. Bajo **cumplimiento del contrato del atributo** elija las opciones dadas y haga clic **después**.

24. Verifique la configuración en la sección de resumen y haga clic **hecho**.

25. Apoye en tecleo de las **operaciones de búsqueda de las fuentes y del usuario del atributo después**.

26. Bajo **fuente a prueba de averías del atributo** haga clic **después**.

27. Bajo **cumplimiento del contrato del atributo** elija estas opciones y haga clic **después.**

28. Verifique la sección y el tecleo de la configuración en resumen **hechos**.

29. Apoye en el tecleo de la **asignación de la fuente de la autenticación después**.

30. Una vez que la configuración se ha verificado bajo el tecleo de la **página de resumen hecho**.

31. Apoye en el tecleo de la **creación de la aserción después**.

32. Bajo **configuraciones del protocolo**, haga clic las **configuraciones del protocolo de la configuración**. En este momento debe haber dos entradas pobladas ya. Haga clic en Next (Siguiente).

33. Bajo SLO mantenga el tecleo URL **después.**

34. En los atascamientos permisibles de SAML, desmarque las opciones ARTEFACTO y JABÓN y haga clic **después.**

35. Bajo directiva de la firma haga clic **después**.

36. Bajo política de encripción haga clic **después**.

37. Revise la configuración en la página de resumen y haga clic **hecho**.

38. Apoye en el navegador SSO > tecleo de las configuraciones del protocolo **después**, valide la configuración, y haga clic **hecho**.

39. La lengueta del navegador SSO aparece. Haga clic en Next (Siguiente).

40. Bajo las **credenciales de la configuración del** tecleo de las **credenciales** y elija el certificado de firma que se utilizará durante IdP a la comunicación ISE y marque la opción **incluyen el certificado en la firma**. Luego haga clic en Next (Siguiente).

> Nota: Si no hay tecleo configurado los Certificados **maneje los Certificados** y siga los prompts para generar un **certificado autofirmado** que se utilizará para firmar IdP a las comunicaciones ISE.

41. Valide la configuración conforme a la página de resumen y haga clic **hecho**.

42. Apoye en el tecleo de la lengueta de las **credenciales después**.

43. Conforme a la **activación y al resumen** elija el **ACTIVE del estado de la conexión**, valide el resto de la configuración, y haga clic **hecho**.

Paso 4. Importe los meta datos de IdP en el perfil externo del proveedor ISE SAML IdP

1. Bajo la consola de administración de PingFederate, elija la **Configuración del servidor > las funciones administrativas > la exportación de los meta datos.** Si el servidor se ha configurado para los papeles múltiples (IdP y SP), elija la opción que **soy la identidad Provider(IdP).** Haga clic en Next (Siguiente).
2. Bajo modo de los **meta datos** selecto **"seleccione la información para incluir en los meta datos manualmente".** Haga clic en Next (Siguiente).

3. Bajo **protocolo** haga clic **después**.

4. En el **contrato del atributo** haga clic **después**.

5. Bajo **clave de firma** elija el certificado configurado previamente en el perfil de la conexión. Haga clic en Next (Siguiente).

6. Bajo **firma de los meta datos** elija el certificado de firma y el control **incluye la clave pública de este certificado en el elemento de información fundamental.** Haga clic en Next (Siguiente).

7. Bajo tecleo del **certificado del cifrado XML después**.

Nota: La opción para aplicar el cifrado aquí está hasta la red Admin.

8. Bajo la **exportación del** tecleo de la **sección de resumen**. Salve el archivo de metadatos generado y después haga clic **hecho**.

9. Bajo el ISE, elija a la **administración > a la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores > PingFederate identificación**.

10. **Los Config del proveedor de la identidad del** tecleo **> hojean** y proceden a importar los meta datos guardados de la operación de la exportación de los meta datos de PingFederate.

11. Elija la lengueta de los **grupos**, bajo **atributo de la membresía del grupo** agregue el **memberOf** y después haga clic **agregan**

Bajo el nombre **en la aserción** agregue el nombre distintivo que el **IdP** debe volver cuando el atributo del **memberOf** es autenticación extraída de la forma LADP. En este caso conectan al grupo configurado al grupo del patrocinador de TOR y el DN para este grupo es como sigue:

Una vez que usted agrega el DN y el "nombre en **AUTORIZACIÓN del** tecleo de la descripción ISE".

12. Elija la lengueta y el haga click en Add de los **atributos**

En este paso, agregue el atributo "correo" que está contenido en el token de SAML pasajero del IdP que basó en la interrogación del ping sobre el LDAP, él debe contener el atributo del correo electrónico para ese objeto.

Nota: Los pasos 11 y 12 se aseguran de que el ISE reciba el correo electrónico del objeto AD y los atributos de MemberOf a través del IdP inicia sesión la acción.

Verificación

1. Inicie el portal del invitado usando la prueba porta URL o siguiendo el CWA fluya. El usuario tendrá las opciones para ingresar las credenciales del invitado, crea su propia cuenta, y el login del empleado.

2. **Login del empleado del** tecleo. Puesto que no hay sesiones activas reorientarán al usuario al portal del login de IdP.

3. Ingrese las credenciales AD y haga clic la **muestra encendido**.

4. La pantalla de inicio de IdP reorientará al usuario a la página porta del éxito del invitado.

5. En este momento, cada vez que el usuario vuelve al invitado porta y elige el "**login del empleado**" serán permitidos en la red mientras la sesión sea todavía activa en el IdP.

Troubleshooting

Cualquier problema de la autenticación de SAML será registrado bajo ise-psc.log. Hay un componente dedicado (SAML) bajo **configuración del registro de la administración > del registro > del debug > selecciona el nodo en la pregunta >** fijó SAML el componente al **nivel de debug**.

Usted puede acceder el ISE con el CLI y ingresar la **cola de ise-psc.log de la aplicación del** comando show logging y monitorear SAML los eventos, o usted puede descargar ise-psc.log para el análisis adicional bajo las **operaciones > los registros del Troubleshooting > de la descarga > selecciona la lengueta de los registros del nodo > del debug ISE > el tecleo ise-psc.log** para descargar los registros.

```
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- ResponseValidationContext:
        IdP URI: PingFederate
        SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
        Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action
        Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210
        Client Address: 14.0.25.62
        Load Balancer: null
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Validate signature to SAML standard
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
```

```
cpm.saml.framework.validators.SAMLSignatureValidator -::::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating response
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -::::- Validating assertion
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -::::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- SAML Response: validation succeeded for guest
IDPResponse
:
        IdP ID: PingFederate
        Subject: guest
        SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
        SAML Success:true
        SAML Status Message:null
        SAML email:guest@rtpaaa.net
        SAML Exception:null
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- Authenticate SAML User - result:PASSED
```

Información Relacionada

- Autenticación Web central con el ejemplo de configuración del WLC y ISE de Cisco.
- Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine.
- Release Note para el Cisco Identity Services Engine, 2.1 de la versión
- Guía del administrador del Cisco Identity Services Engine, 2.1 de la versión