Portal del patrocinador del 2.1 de la configuración ISE con PingFederate SAML SSO

Contenido

Introducción

Este documento describe cómo configurar un servidor de PingFederate SAML con el 2.1 de Engine(ISE) de los servicios de la identidad de Cisco para proporcionar las solas capacidades de On(SSO) de la muestra para patrocinar a los usuarios.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios del invitado del Cisco Identity Services Engine.
- Conocimiento básico sobre las implementaciones de 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.
- R2 del Servidor Windows 2012 con los servicios de Active Directory.

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 los comandos any.

Convenciones

Refiera a los convenios de los consejos técnicos de Cisco para más información sobre las convenciones sobre documentos

Descripción del flujo

El lenguaje de marcado de la aserción de la Seguridad (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 del patrocinador), el proveedor de la identidad (IdP) (servidor federado del ping), 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 durante las decisiones de políticas. Una vez que ocurre la autenticación inicial, indicase al usuario no debe para las credenciales otra vez que acceda el servicio mientras la sesión de la aserción sea todavía activa en el IdP.

Éste es el flujo previsto para este caso del uso:

1. Las tentativas del usuario de iniciar sesión al portal del patrocinador iniciando el nombre de dominio completo (FQDN) de encargo del portal configurado del patrocinador.
2. El ISE verifica si hay una aserción activa asociada a la sesión del buscador de este cliente publicando un rápido reorienta al IdP. Si no hay sesiones activas, el IdP aplicará el ingreso del usuario al sistema.
3. El IdP autentica al usuario vía el LDAP y pasa los atributos del memberOf y del correo electrónico a ISE(SP).
4. El ISE procesa la respuesta de IdP XML y basado en el atributo del memberOf y en la configuración de los grupos del patrocinador permitirán o serán rechazado al usuario (control de condición de la membresía del grupo para hacer juego a un grupo configurado del patrocinador).
5. El Time to Live de la sesión variará en cada solución. En este caso del uso, el ping Federate será configurado con un **tiempo de espera de la sesión de** 60 minutos (si no hay pedidos de registro SSO del ISE en 60 minutos después de la autenticación inicial, se borra la sesión) y un **descanso máximo de la sesión de** 480 minutos (incluso si el IdP ha estado recibiendo los pedidos de registro constantes SSO del ISE para este usuario que la sesión expirará en 8 horas). Una vez los tiempos de la sesión hacia fuera, una autenticación de usuario nuevo es aplicada por el IdP.
6. Mientras que la sesión es todavía activa, el usuario del patrocinador debe poder cerrar el hojeador y la reaparición al portal sin ingresar las credenciales.

Configurar

La sección siguiente discutirá los pasos para la configuración para integrar el ISE con el ping federado y cómo habilitar al navegador SSO para el portal del patrocinador.

Nota: Aunque existan las diversas opciones y posibilidades cuando usted autentica a los usuarios del patrocinador, 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, navegue a la **administración > a la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores identificación**.
2. El tecleo agrega
3. Conforme a la ficha general, ingrese un nombre del proveedor identificación y haga clic la **salvaguardia**. El resto de la configuración en esta sección dependerá de los meta datos que necesite ser importada del IdP.

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

1. Navegue a los **centros de trabajo > al acceso de invitado > a la configuración > a los portales del patrocinador**
2. Haga clic en al **patrocinador porta (valor por defecto)** o cree un nuevo portal.
3. Bajo **configuraciones porta** ingrese un Nombre de dominio totalmente calificado (FQDN) de encargo (FQDN) conectado a este portal del patrocinador.
4. Seleccione de la **secuencia de la fuente de la identidad que** SAML externo IdP definió previamente.

5. Verifique que el diagrama de flujo represente la **salvaguardia** siguiente y del tecleo:

Paso 3. Configuración PingFederate como IdP para manejar los pedidos de autenticación ISE

1. Navegue a la **administración > a la Administración de la identidad** ISE **> las fuentes externas de la identidad > SAML los proveedores >** PingFederate **identificación**
2. Haga clic la lengueta de la **información del proveedor de servicio** y haga clic la **exportación**

3. Salve y extraiga archivo zip generado. El archivo XML contenido aquí será utilizado mientras que crea el perfil en PingFederate.

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

5. Bajo sección de la **ficha de configuración IDP > de las conexiones SP** selecta 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**, el **archivo** selecto, eligió el archivo y selecciona el archivo XML exportado previamente del ISE.

9. Conforme al **resumen de los meta datos**, haga clic en **después**.

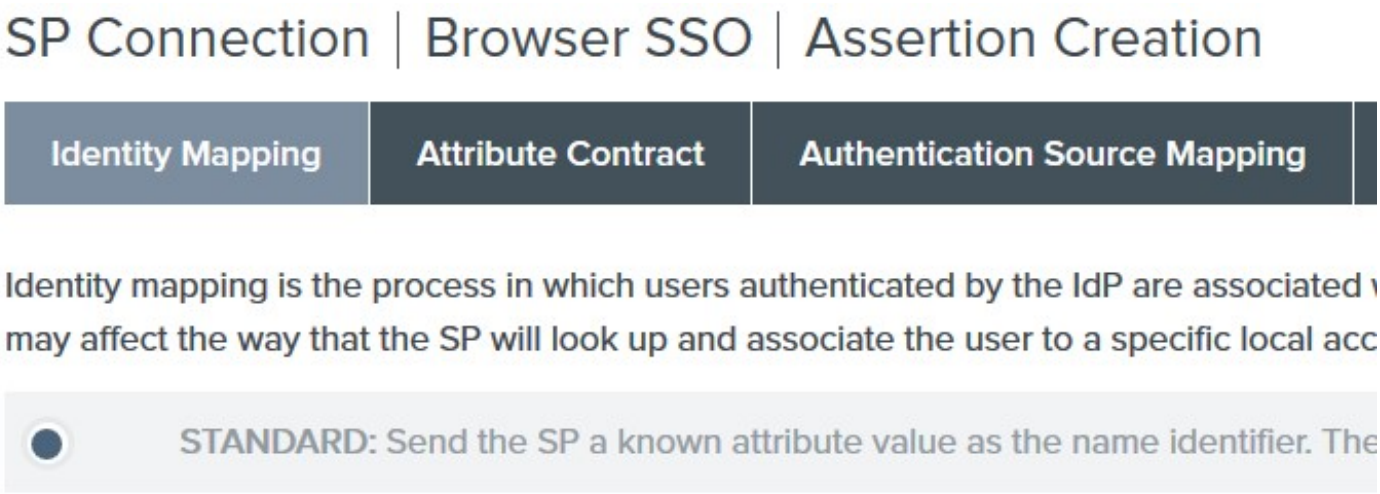
10. En la página de la información general, bajo **nombre de la conexión** ingrese un nombre (IE. ISEsponsorPortal) y hace clic **después**.

11. Bajo **navegador SSO de la configuración del** tecleo del **navegador SSO** y bajo **perfiles de SAML** marque estas opciones y haga clic después:

12. En el **curso de la vida de la aserción** haga clic **después**

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

14. Bajo **estándar** selecto y tecleo de la **asignación de la identidad después**



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

> Nota: Esto es un Paso crítico como el ISE confía en estos atributos para la asignación correcta del grupo del patrocinador y también envía por correo electrónico es necesario para las funciones correctas de la notificación.

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

17. En el **caso del adaptador** seleccione el **adaptador de la forma HTML**. Haga clic en Next (Siguiente).

18. Bajo **método de la asignación** seleccione la segunda opción y haga clic **después**

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

20. Bajo el **almacén de los datos** ingrese una descripción, después selecciónela de los **datos activos salvan** su caso de la conexión LDAP y definen qué tipo de servicio de directorio es éste. Si no hay almacenes de los datos configurados con todo haga clic en **manejan los almacenes de los datos** para agregar el nuevo citan como ejemplo.

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. La base incorrectamente definida DN dará lugar a un error “objeto no encontrado en el esquema LDAP”.

22. Bajo el **filtro LDAP** agregue la cadena **sAMAccountName=$ {nombre de usuario}** y haga clic **después**.

23. Bajo **cumplimiento del contrato del atributo** seleccione estas opciones 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** seleccione estas opciones y haga clic **después**:

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

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

29. Una vez que la configuración se ha verificado bajo tecleo de la **sección de resumen hecho**.

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

31. Bajo **configuraciones del protocolo** haga clic las **configuraciones del protocolo de la configuración**.

En este momento debe haber 3 entradas pobladas ya. Tecleo **después**

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

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

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

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

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

37. Apoye en el **navegador SSO** > tecleo de las **configuraciones del protocolo después**, valide la configuración y haga clic **hecho**. Esto traerá detrás el tecleo del **navegador SSO** cuadro **después**.

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

Nota: Si no hay Certificados configurados, el tecleo **maneja los Certificados** y sigue los

prompts para generar un certificado autofirmado que se utilizará para firmar IdP a las comunicaciones ISE.

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

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

41. Conforme a la **activación y al resumen** selectos en el **ACTIVE del estado de la conexión**, valide el resto de la configuración y haga clic la **salvaguardia**.

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, navegue a la **Configuración del servidor > a las funciones administrativas > a la exportación de los meta datos** si el servidor se ha configurado para los papeles múltiples (IdP y SP) selecciona la opción que **soy la identidad Provider(IdP).** Haga clic **después**

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** seleccione el certificado configurado previamente en el perfil de la conexión. Haga clic en Next (Siguiente).

6. Bajo **firma de los meta datos** seleccione 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**. La opción para aplicar el cifrado aquí está hasta la red Admin.

8. Bajo la salvaguardia de la **exportación del** tecleo de la **sección de resumen el** archivo de metadatos generado y entonces hace clic **hecho**.

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

10. Haga clic en el **proveedor de la identidad que el >**Click de los **Config hojea** y proceda a importar los meta datos guardados de la operación de la exportación de los meta datos de Pingfederate.

11. La lengueta selecta de los **grupos** y bajo **atributo de la membresía del grupo** agrega el **memberOf** y después hace clic **agrega**

12. Bajo el nombre **en la aserción** agregue el **nombre distintivo** que el IdP debe volver detrás cuando el atributo del **memberOf** es autenticación ldap extraída de la forma. Conectarán a este grupo al grupo del patrocinador.

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

ISE".

13. Lengueta selecta y haga click en Add de los **atributos** En este paso agregaremos el atributo **"correo"**. Esto se contiene en la autenticación de SAML; resultado pasajero del IdP (basado en el atributo del correo electrónico para ese objeto de usuario en el Active Directory).

> Nota: Este paso es tan importante que el ISE debe poder procesar el correo electrónico conectado a la sesión del patrocinador para poder asociar cualquier cuenta en el estado pendiente de los flujos uno mismo-registradoes. Si no seguirá habiendo las cuentas en un estado del limbo pues no asociarán a la "persona que es" correo electrónico visitado a una sesión válida del patrocinador. Es también importante para la notificación por correo electrónico propone.

14. Bajo **ficha Avanzadas** seleccione las configuraciones siguientes:

> Nota: Esta sección dará instrucciones el ISE para incluir el atributo del correo electrónico en las peticiones del logout al servidor del IdP. Esto es importante cuando el usuario del patrocinador termina una sesión manualmente del portal.

15. Haga clic en Save (Guardar).

16. En este paso el administrador asociará el grupo del Active Directory extraído por el IdP a un grupo del patrocinador. Navegue a los **centros >** al **acceso de invitado >** a la **configuración >** al **patrocinador de trabajo agrupa > ALL_ACCOUNTS** (o seleccione al grupo apropiado). Haga clic a los **miembros** y seleccione el **PingFederate**: **Agrúpenos** asoció en los pasos anteriores y lo agregan a la columna de los grupos de usuario seleccionado. Luego haga clic en OK (Aceptar).

17. Cuando se configura el flujo registrado uno mismo, las cuentas estarán hasta que finalice la aprobación. En este caso, selecto **"apruebe y vea las peticiones de los invitados uno mismo-registradoes"** y selecciónelas **"solamente hasta que finalicen las cuentas asignadas a este patrocinador"** como una forma sencilla de verificar la dirección de correo electrónico del objeto es AD y transferidas a la identidad del patrocinador en el ISE a través del servidor de IdP usando el atributo del **correo**.

18. Haga clic en Save (Guardar). Esto acaba la configuración en el ISE.

Verificación

1. Inicie el portal del patrocinador usando la aduana configurada FQDN. El ISE debe reorientar al usuario al portal de la autenticación de usuario de PingFederate.

2. Ingrese las credenciales del Active Directory y la muestra del golpe encendido. La pantalla de inicio de IdP reorientará al usuario al AUP inicial en el portal del patrocinador ISE.

En este momento el usuario del patrocinador debe tener acceso total al portal.

3. Verifique la sola muestra encendido. Cuando de la "se utiliza la característica **prueba URL porta**" el ISE debe preguntar las credenciales del patrocinador cada vez si el SSO no se configura.

Inicie el portal del patrocinador con el link porta de la prueba URL. El patrocinador URL ISE

conmutará rápidamente al IdP URL para verificar el estatus de la sesión y una vez que se confirma el token de la sesión reorientan al cliente de nuevo al portal del patrocinador sin la necesidad de ingresar las credenciales.

4. Verifique que el atributo del correo electrónico esté pasado correctamente del objeto del Active Directory a IdP al ISE. La manera más fácil de probar está creando una nueva cuenta en el patrocinador porta y seleccionando la opción de la **notificación**. Si el correo electrónico se extrae correctamente aparecerá bajo campo de la **dirección de correo electrónico del** patrocinador.

5. Verifique la función del **logout**. Esto es crucial en la integración de verificar que el logout del patrocinador acciona la sesión simbólica que se terminará en el lado del servidor de la identidad. Firme hacia fuera del patrocinador porta y aseegurese que la próxima vez que el usuario intenta acceder el portal del patrocinador, será reorientado de nuevo a la pantalla de la autenticación de IdP.

Troubleshooting

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

Podemos acceder el ISE con el CLI y publicar “una cola de ise-psc.log de la aplicación del registro de la demostración” y monitorear los eventos de SAML viva, o podemos descargar **ise-psc.log** para el análisis adicional bajo las **operaciones >** los **registros del Troubleshooting >** de la **descarga >** seleccionamos la lengueta de los **registros del** nodo **>** del **debug** ISE **>** el tecleo **ise-psc.log** para descargar los registros.

El registro inicial de la autenticación parecerá típicamente esto:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>


2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Después del evento de la conexión con el sistema inicial, cada vez que los accesos del usuario el portal del patrocinador nosotros considerarán el ISE el extraer de la información de la aserción

para verificar que el token es todavía activo. El resultado debe parecer esto:

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>


2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Información Relacionada

[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]