Integre el gadget de terceros con Finesse en el modo SSO

Contenido

Introducción

Este documento describe lo que se necesita para la integración de un dispositivo de terceros con Finesse mientras el sistema está en modo de inicio de sesión único (SSO). También se da un ejemplo para el modo NON SSO.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Finesse
- SSO
- Dispositivos de terceros Finesse

Componentes Utilizados

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

- Cisco Finesse versión 11.6
- SSO
- gadget de terceros
- Servicio REST de terceros.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos son los pasos iniciales mientras el agente intenta iniciar sesión y autenticarse con SSO o NONSSO.

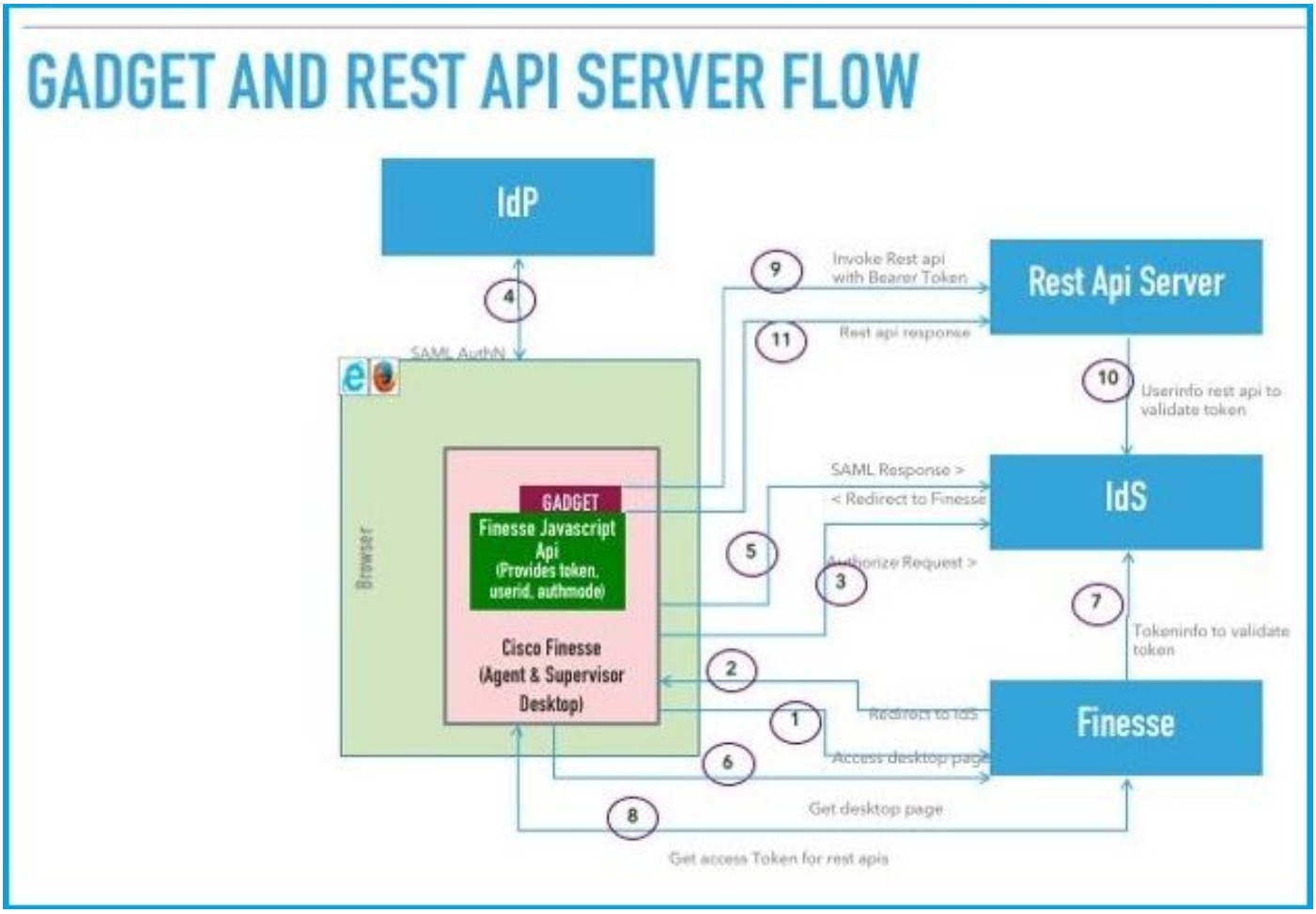
el segundo paso describe lo que se debe considerar después de una autenticación exitosa en el caso de SSO y NONSSO.

1. Cuando se inicia sesión en el escritorio, Finesse detecta el modo de autenticación del sistema (SSO/NONSSO) y, en función del modo de autenticación, se muestra la página de inicio de sesión adecuada. Los usuarios ven la página de inicio de sesión IDP en caso de modo SSO y la página de inicio de sesión Finesse en caso de modo NONSSO.

2. Después de una autenticación exitosa, todas las solicitudes se autentican según el modo de autenticación del sistema. Para implementaciones de SSO, todas las solicitudes a Finesse llevan un token de acceso como parte del encabezado de solicitud. El token se valida contra el servidor IDP para una autenticación exitosa. Sin embargo, para las solicitudes a servicios web de terceros, el encabezado Auth debe configurarse en función del esquema de autenticación implementado por el servicio web de terceros. En caso de implementación de NONSSO, todas las solicitudes llevan el encabezado **Basic** Auth con nombre de usuario y contraseña codificados base64. Todas las solicitudes en este caso se validan con la base de datos local de Finesse.

Explicación del modelo básico de interacción para el modo SSO

Esta *imagen* muestra el modelo básico de interacción entre un gadget de terceros, Finesse, IDS y un servicio REST de terceros, cuando el sistema está en modo SSO.



Imagen

Esta es la descripción de cada paso que se muestra en la imagen.

1. Agent/Supervisor accede a la URL del escritorio Finesse. (Ejemplo: *https://finesse.com:8445/desktop*)
2. Finesse detecta que el modo de autenticación es SSO y redirige el explorador a IDS.
3. El explorador envía la solicitud de autorización de redirección a IDS. En este punto, el IDS detecta si *el usuario* tiene un token de acceso válido o no. Si *el usuario* no tiene un token de acceso válido, IDS redirige al proveedor de identidad (IdP).
4. Si la solicitud se redirige a IdP, IdP proporciona la página *Login* para autenticar *al usuario.*
5. La afirmación SAML de IdP se envía al IDS, que redirige al escritorio Finesse.
6. El explorador realiza una operación GET de la página de escritorio de Finesse.
7. Finesse obtiene el token de acceso de IDS con el código de autenticación SAML.
8. Desktop obtiene el token de acceso que se utilizará para autenticar las API REST posteriores.
9. El gadget de terceros se carga en el escritorio e invoca una API REST de terceros con el token de acceso (portador) en el auth-header.
10. El servicio REST de terceros valida el token con IDS.
11. La respuesta REST de terceros se devuelve al gadget.

Configuración de gadgets.io.makerequest para el modo SSO y NONSSO

Paso 1. Para las llamadas de la API REST de Finesse realizadas a través de Shindig , los gadgets deben agregar el encabezado de autorización "Bearer" en los encabezados gadgets.io.makeRequest.

Paso 2. Los gadgets deben realizar llamadas gadgets.io.makeRequest nativas para todas las solicitudes REST, el encabezado de autorización debe configurarse dentro de los parámetros de solicitud.

Para las implementaciones no SSO, este es el encabezado de autenticación.

```
"Basic " + base64.encode(username : password)
```

Para implementaciones de SSO, éste es el encabezado de autenticación.

```
"Bearer "  + access_token
```

El token de acceso se puede recuperar del objeto **finesse.gadget.Config**.

```
 access_token = finesse.gadget.Config.authToken
```

El nuevo encabezado de autorización se debe agregar a los parámetros de solicitud.

```
 params[gadgets.io.RequestParameters.HEADERS].Authorization = "Basic " + base64.encode(username
: password);
```

```
params[gadgets.io.RequestParameters.HEADERS].Authorization = "Bearer " + access_token;
```

Paso 3. Se ha agregado un método de utilidad **getAuthHeaderString** dentro de **utilidades.Utilidades**. Este método de utilidad toma el objeto config como argumento y devuelve la cadena de encabezado de autorización. Los gadgets pueden utilizar este método de utilidad para establecer el encabezado de autorización en los parámetros de solicitud.

```
params[gadgets.io.RequestParameters.HEADERS].Authorization=
finesse.utilities.Utilities.getAuthHeaderString(finesse.gadget.config);
```

> **Nota:** Para las solicitudes de API a servicios web de terceros, el encabezado de autenticación debe configurarse en función del esquema de autenticación implementado por el servicio web de terceros. Los desarrolladores de Gadget tienen la libertad de utilizar autenticación básica o basada en token portador, o cualquier otro mecanismo de autenticación de su elección.