Integre o dispositivo da terceira parte com fineza no modo SSO

Índice

Introdução

Este documento descreve o que está precisado para a integração de dispositivos de uma 3ª parte com fineza quando o sistema estiver em único Sinal-no modo (SSO). Um exemplo é dado igualmente para o modo NON SSO.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fineza de Cisco
- SSO
- Dispositivos da 3ª parte da fineza

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 11.6 da fineza de Cisco
- SSO
- Dispositivo da 3ª parte
- Serviço do RESTO da 3ª parte.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estas são as etapas inicial quando o agente tentar entrar e autenticar com SSO ou NONSSO.

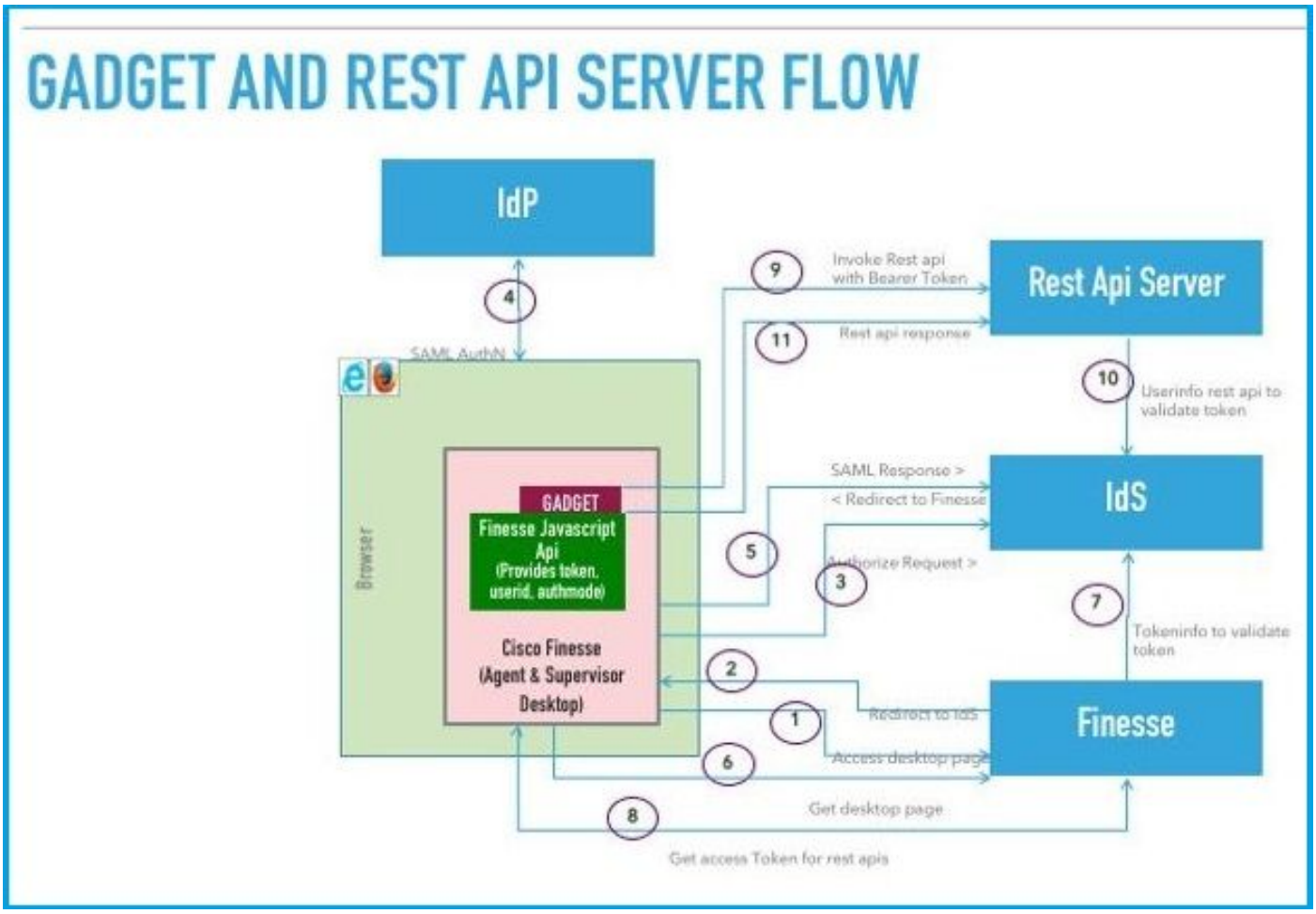
o segundo passo descreve que necessidades de ser considerado após a autenticação bem sucedida em caso do SSO e do NONSSO.

1. Na altura do início de uma sessão do desktop, a fineza detecta o modo do AUTH do sistema (SSO/NONSSO) e baseado no modo do AUTH, Loginpage apropriado é indicado. Os usuários veem a página de login IDP em caso do modo SSO e a página de login da fineza em caso do modo NONSSO.

2. Após a autenticação bem sucedida, todos os pedidos são autenticados com base no modo do AUTH do sistema. Para disposições SSO, todos os pedidos à fineza levam o access token como parte do encabeçamento de pedido. O token é validado contra o server IDP para a autenticação bem sucedida. Contudo, para pedidos aos serviços de Web da 3ª parte, o encabeçamento do AUTH tem que ser ajustado baseado no método de autenticação executado pelo serviço de Web da 3ª parte. Em caso do desenvolvimento NONSSO, todos os pedidos levam o encabeçamento básico do AUTH com nome de usuário e senha codificado base64. Todos os pedidos são validados neste caso contra o base de dados local da fineza.

Explicação do modelo básico da interação para o modo SSO

Esta *imagem* mostra o modelo básico da interação entre um dispositivo da 3ª parte, a fineza, o IDS, e um serviço do RESTO da 3ª parte, quando o sistema reage do modo SSO.



Imagem

Está aqui a descrição para cada etapa mostrada na imagem.

1. O agente/supervisor alcança o desktop URL da fineza.
   (Exemplo: *https://finesse.com:8445/desktop)*
2. A fineza detecta que o modo de autenticação é SSO e reorienta o navegador ao IDS.
3. O navegador envia a reorientação autoriza o pedido ao IDS. Neste momento, o IDS detecta se o *usuário* tem um access token válido ou não. Se o *usuário* não tem um access token válido, o IDS reorienta ao fornecedor da identidade (IdP).
4. Se o pedido é reorientado a IdP, IdP fornece a página de login autenticando o *usuário.*
5. A afirmação de SAML de IdP é enviada ao IDS, que reorienta de volta ao desktop da fineza.
6. O navegador faz um GET da página do desktop da fineza.
7. A fineza obtém o access token do IDS com o código do AUTH de SAML.
8. O Desktop consegue o access token ser usado para autenticar o RESTO subsequente API.
9. O dispositivo da 3ª parte carrega no desktop e invoca um RESTO API da 3ª parte com o access token (portador) no autêntico-encabeçamento.
10. O serviço do RESTO da 3ª parte valida o token com IDS.
11. A resposta do RESTO da 3ª parte é retornada ao dispositivo.

Configuração de gadgets.io.makerequest para o modo SSO e NONSSO

Etapa1. Para os atendimentos do RESTO API da fineza feitos através do baile, os dispositivos precisam de adicionar o encabeçamento da autorização do “portador” em encabeçamentos gadgets.io.makeRequest.

Etapa 2. Os dispositivos precisam de fazer atendimentos nativos gadgets.io.makeRequest para todos os pedidos do RESTO, o encabeçamento da autorização têm que ser ajustados dentro dos params do pedido.

Para disposições NON SSO, este é o encabeçamento do AUTH.

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

Para disposições SSO, este é o encabeçamento do AUTH.

```
"Bearer "  + access_token
```

O access token pode ser recuperado do **objeto finesse.gadget.Config.**

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

O mustl novo do encabeçamento da autorização seja adicionado aos params do pedido.

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

Etapa 3. Um método de serviço público que **getAuthHeaderString** foi **utilidades** internas adicionadas**. Utilidades**. Este método de serviço público toma o objeto da configuração

como o argumento e retorna a corda do encabeçamento da autorização. Os dispositivos podem utilizar este método de serviço público para ajustar o encabeçamento da autorização em params do pedido.

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

> Nota: Para pedidos API aos serviços de Web da 3ª parte, o encabeçamento do AUTH tem que ser ajustado baseado no método de autenticação executado pelo serviço de Web da 3ª parte. Os colaboradores do dispositivo têm a liberdade para usar o AUTH básico ou a autenticação baseada token do portador, ou todo o outro mecanismo da autenticação de sua escolha.