Integre o gadget de terceiros com o Finesse no modo SSO

Contents

Introduction

Este documento descreve o que é necessário para a integração de um gadgets de terceiros com o Finesse enquanto o sistema está no modo de Logon Único (SSO). Um exemplo também é dado para o modo NON SSO.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Finesse
- SSO
- Gadgets de terceiros do Finesse

Componentes Utilizados

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

- Cisco Finesse versão 11.6
- SSO
- gadget de terceiros
- Serviço REST de terceiros.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estas são as etapas iniciais enquanto o agente tenta fazer logon e autenticar com SSO ou

NONSSO.

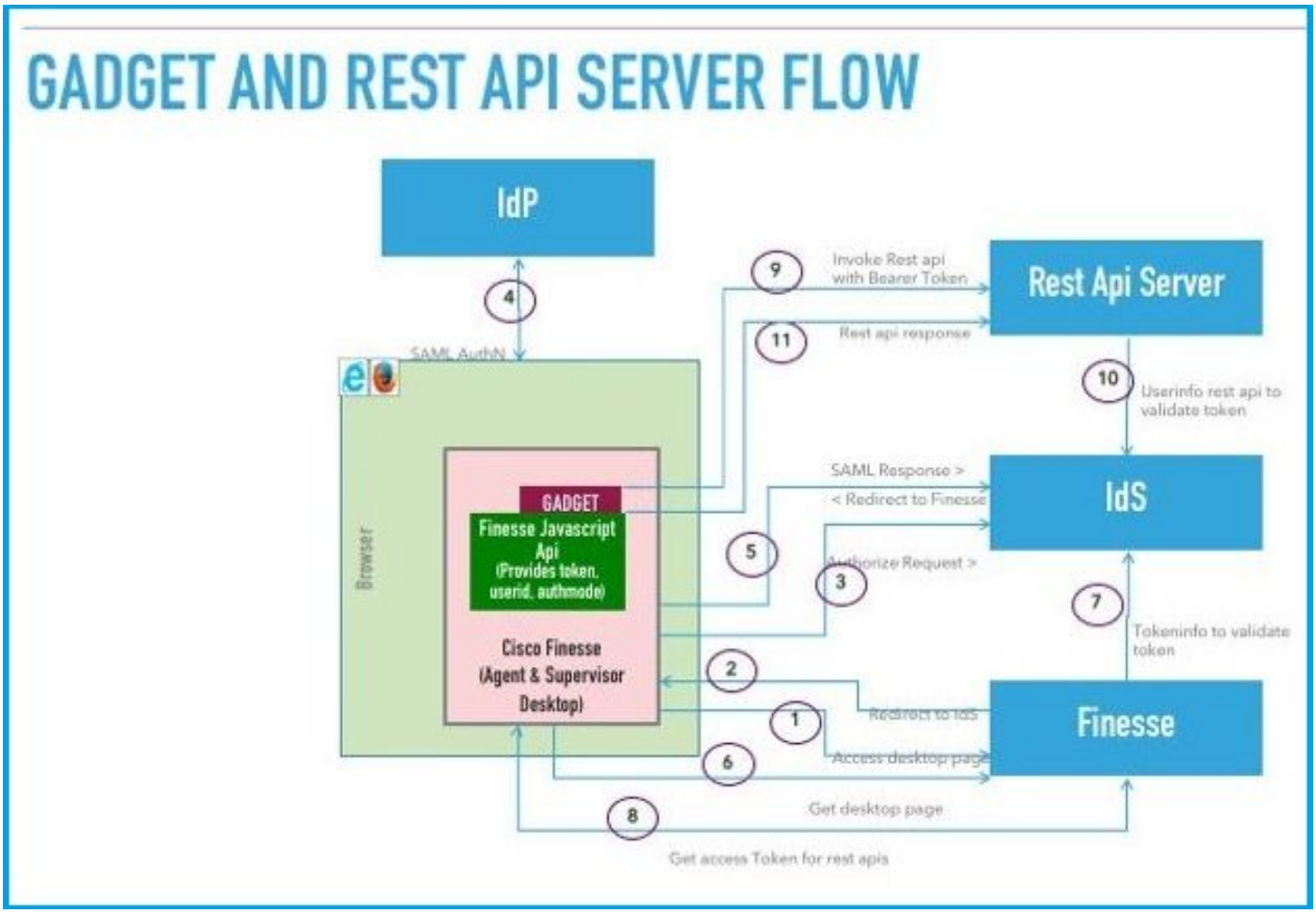
a segunda etapa descreve o que precisa ser considerado após a autenticação bem-sucedida no caso de SSO e NONSSO.

1. No momento do login na área de trabalho, o Finesse detecta o modo de autenticação do sistema (SSO/NONSSO) e, com base no modo de autenticação, a página de login apropriada é exibida. Os usuários veem a página Login do IDP no caso do modo SSO e a página Login do Finesse no caso do modo NONSSO.

2. Após a autenticação bem-sucedida, todas as solicitações são autenticadas com base no modo Auth do sistema. Para implantações SSO, todas as solicitações ao Finesse transportam o token de acesso como parte do cabeçalho da solicitação. O token é validado no servidor IDP para autenticação bem-sucedida. No entanto, para solicitações a serviços Web de terceiros, o cabeçalho Auth deve ser definido com base no esquema de autenticação implementado pelo serviço Web de terceiros. No caso da implantação do NONSSO, todas as solicitações carregam o cabeçalho **Basic** Auth com nome de usuário e senha codificados em base64. Todas as solicitações nesse caso são validadas no banco de dados local do Finesse.

Explicação do modelo básico de interação para o modo SSO

Esta *imagem* mostra o modelo básico de interação entre um gadget de terceiros, Finesse, IDS e um serviço REST de terceiros, quando o sistema está no modo SSO.



Imagem

Aqui está a descrição de cada etapa mostrada na imagem.

1. O agente/supervisor acessa o URL da área de trabalho do Finesse. (Exemplo: *https://finesse.com:8445/desktop*)
2. O Finesse detecta que o modo de autenticação é SSO e redireciona o navegador para o IDS.
3. O navegador envia a solicitação de autorização de redirecionamento para o IDS. Neste ponto, o IDS detecta se *o usuário* tem um token de acesso válido ou não. Se *o usuário* não tiver um token de acesso válido, o IDS redirecionará para o Provedor de identidade (IdP).
4. Se a solicitação for redirecionada para IdP, IdP fornece a página *Login* para autenticação *do usuário.*
5. A asserção SAML do IdP é enviada ao IDS, que redireciona de volta para o desktop Finesse.
6. O navegador faz GET da página de desktop do Finesse.
7. O Finesse obtém o token de acesso do IDS com o código de autenticação SAML.
8. A área de trabalho obtém o token de acesso a ser usado para autenticar APIs REST subsequentes.
9. O gadget de terceiros é carregado na área de trabalho e chama uma API REST de terceiros com o token de acesso (portador) no cabeçalho de áudio.
10. O serviço REST de terceiros valida o token com IDS.
11. A resposta REST de terceiros é retornada ao gadget.

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

Etapa 1. Para chamadas de API REST do Finesse feitas via Shindig , os gadgets precisam adicionar o cabeçalho de autorização "Portador" nos cabeçalhos gadgets.io.makeRequest.

Etapa 2. Os gadgets precisam fazer chamadas nativas gadgets.io.makeRequest para todas as solicitações REST, o cabeçalho de autorização deve ser definido dentro dos parâmetros de solicitação.

Para implantações de NON SSO, este é o cabeçalho de autenticação.

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

Para implantações SSO, este é o cabeçalho Auth.

```
"Bearer "  + access_token
```

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

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

O novo cabeçalho de autorização deve ser adicionado aos parâmetros de solicitação.

```
 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 utilitário **getAuthHeaderString** foi adicionado em **utilities.Utilities**. Este método de utilitário pega o objeto config como argumento e retorna a string do cabeçalho de autorização. Os gadgets podem usar esse método de utilitário para definir o cabeçalho de autorização em parâmetros de solicitação.

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

> **Note**: Para solicitações de API para serviços Web de terceiros, o cabeçalho de autenticação deve ser definido com base no esquema de autenticação implementado pelo serviço Web de terceiros. Os desenvolvedores de gadgets têm a liberdade de usar autenticação básica baseada em token de autenticação ou portador ou qualquer outro mecanismo de autenticação de sua escolha.