Integrazione di gadget di terze parti con Finesse in modalità SSO

Sommario

Introduzione

In questo documento viene descritto ciò che è necessario per l'integrazione di gadget di terze parti con Finesse quando il sistema è in modalità Single Sign-On (SSO). Viene fornito un esempio anche per la modalità NON SSO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Finesse
- SSO
- Gadget di terze parti Finesse

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Finesse versione 11.6
- SSO
- Gadget di terze parti
- Servizio REST di terze parti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questi sono i passi iniziali durante i quali l'agente tenta di eseguire l'accesso e l'autenticazione con SSO o NONSSO.

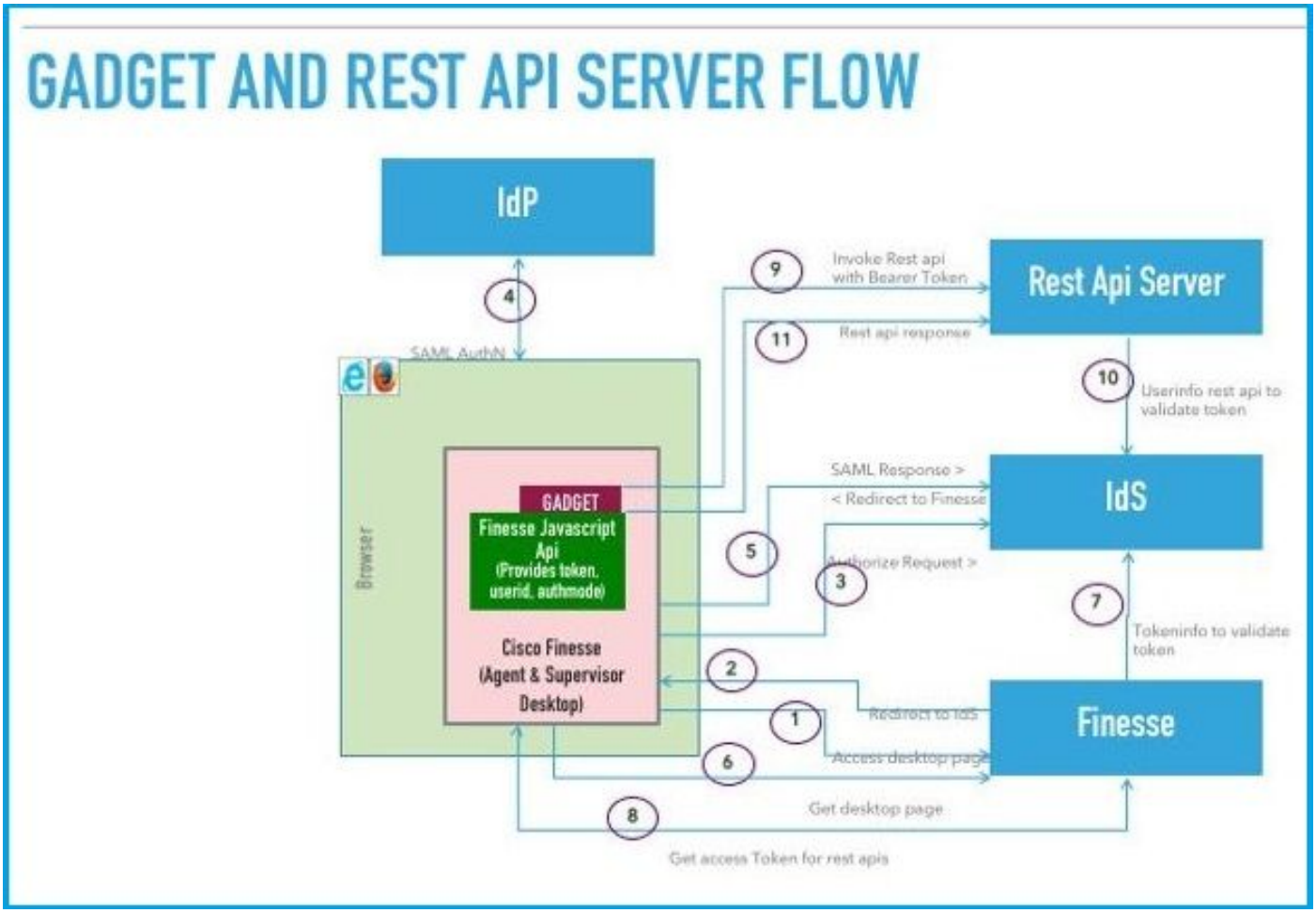
la seconda fase descrive cosa deve essere considerato dopo aver completato l'autenticazione in caso di SSO e NONSSO.

1. Al momento dell'accesso al desktop, Finesse rileva la modalità di autenticazione del sistema (SSO/NONSSO) e, in base alla modalità di autenticazione, viene visualizzata la pagina Login appropriata. Gli utenti visualizzano la pagina Accesso IDP in caso di modalità SSO e la pagina Accesso Finesse in caso di modalità NONSSO.

2. Dopo l'autenticazione, tutte le richieste vengono autenticate in base alla modalità di autenticazione del sistema. Per le distribuzioni SSO, tutte le richieste a Finesse hanno il token di accesso come parte dell'intestazione della richiesta. Il token viene convalidato sul server IDP per la corretta autenticazione. Tuttavia, per le richieste ai servizi Web di terze parti, l'intestazione Auth deve essere impostata in base allo schema di autenticazione implementato dal servizio Web di terze parti. In caso di distribuzione NONSSO, tutte le richieste hanno l'intestazione **Basic** Auth con nome utente e password codificati in base64. Tutte le richieste in questo caso vengono convalidate rispetto al database locale Finesse.

Spiegazione del modello base di interazione per la modalità SSO

Questa *immagine* mostra il modello di base dell'interazione tra un gadget di terze parti, Finesse, IDS e un servizio REST di terze parti, quando il sistema è in modalità SSO.



Immagine

Di seguito è riportata la descrizione di ogni passo mostrato nell'immagine.

1. L'agente/supervisore accede all'URL del desktop Finesse (esempio: *https://finesse.com:8445/desktop).*
2. Finesse rileva che la modalità di autenticazione è SSO e reindirizza il browser a IDS.
3. Il browser invia la richiesta di autorizzazione di reindirizzamento a IDS. A questo punto, IDS rileva se *l'utente* ha un token di accesso valido o meno. Se *l'utente* non dispone di un token di accesso valido, IDS viene reindirizzato al provider di identità (IdP).
4. Se la richiesta viene reindirizzata a IdP, IdP visualizza la pagina *Accesso* per l'autenticazione *dell'utente.*
5. L'asserzione SAML di IdP viene inviata a IDS, che reindirizza al desktop Finesse.
6. Il browser esegue un GET della pagina desktop Finesse.
7. Finesse ottiene il token di accesso da IDS con il codice di autenticazione SAML.
8. Desktop ottiene il token di accesso da utilizzare per autenticare le API REST successive.
9. I gadget di terze parti vengono caricati nel desktop e richiamano un'API REST di terze parti con il token di accesso (supporto) nell'intestazione auth.
10. Il servizio REST di terze parti convalida il token con IDS.
11. La risposta REST di terze parti viene restituita al gadget.

Configurazione di gadgets.io.makerequest per la modalità SSO e NONSSO

Passaggio 1. Per le chiamate all'API REST Finesse effettuate tramite Shindig, i gadget devono aggiungere l'intestazione di autorizzazione "Bearer" nelle intestazioni gadgets.io.makeRequest.

Passaggio 2. I gadget devono eseguire chiamate gadgets.io.makeRequest native per tutte le richieste REST. È necessario impostare l'intestazione dell'autorizzazione nei parametri della richiesta.

Per le distribuzioni NON SSO, questa è l'intestazione Auth.

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

Per le distribuzioni SSO, questa è l'intestazione Auth.

```
"Bearer "  + access_token
```

Il token di accesso può essere recuperato dall'oggetto **finesse.gadget.Config**.

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

La nuova intestazione dell'autorizzazione deve essere aggiunta ai parametri della richiesta.

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

Passaggio 3. Un metodo di utilità **getAuthHeaderString** è stato aggiunto in **utilities.Utilities**. Questo metodo di utilità utilizza l'oggetto config come argomento e restituisce la stringa dell'intestazione

dell'autorizzazione. I gadget possono utilizzare questo metodo di utilità per impostare l'intestazione di autorizzazione nei parametri di richiesta.

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

> **Nota:** Per le richieste API a servizi Web di terze parti, l'intestazione di autenticazione deve essere impostata in base allo schema di autenticazione implementato dal servizio Web di terze parti. Gli sviluppatori di gadget hanno la libertà di utilizzare l'autenticazione di base o l'autenticazione basata su token di connessione o qualsiasi altro meccanismo di autenticazione di loro scelta.