

닉스테크

서울시 성동구 왕십리로 58 포휴빌딩 10 층

전화 02-3497-8900 팩스 02-578-6621



## KUKUDocs DOCUMENT SERVER INTERGRATION

VERSION	0.0.2
DATE	2016-10-18
WRITER	장욱

---

## DOCUMENT HISTORY (문서정보/수정내역)

수정날짜	수정자	버전	추가/수정항목	내용
2016-10-18	장욱	0.0.1	초안 작성	초안 작성
2016-10-18	송천중	0.0.2	SSO 연동부	SAML 관련 내용 추가

## 1. CONTENTS (목차)

1. CONTENTS (목차).....	3
2. INTRODUCTION (개요).....	4
■ Purpose (목표).....	4
■ Overall System Configuration (전체 시스템 구성).....	4
● Nicstech Security Broker (NSB) 구성 요소 .....	4
● AWS Lambda 사용 .....	4
● SSO (Single Sign On) 사용 .....	5

## 2. INTRODUCTION (개요)

### ■ Purpose (목표)

- ✓ 본 문서는 닉스텍 Security Broker 에 KuKuDocs HTML5 기반 DocumentsViewer 인터그레이션을 위한 사전 환경 및 구성 방안에 대해 서술한다.

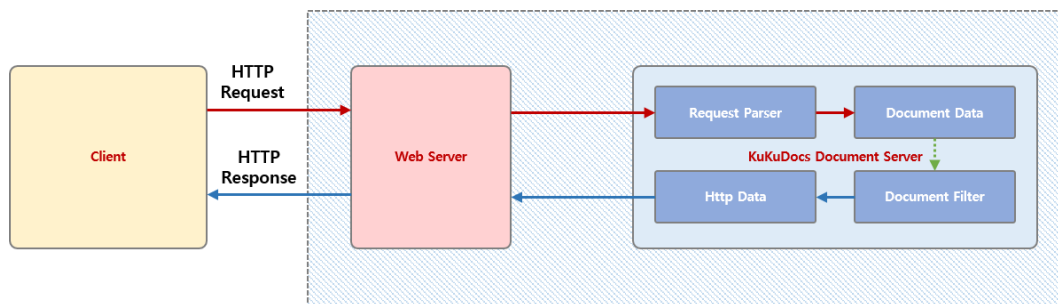
### ■ Overall System Configuration (전체 시스템 구성)

#### ● Nicstech Security Broker (NSB) 구성 요소

- ✓ AWS EC2 : VM 상에 KuKuDocs 서버 구성
- ✓ DataBase : Paas 형태로 제공되는 DataBase 사용
- ✓ Serverless Architecture : AWS API GW + AWS Lambda 를 통해 Non-WAS 형태의 웹서비스 구성
- ✓ RESTful API : Client 와 Sever 간 통신은 RESTful API 로만 동작한다.

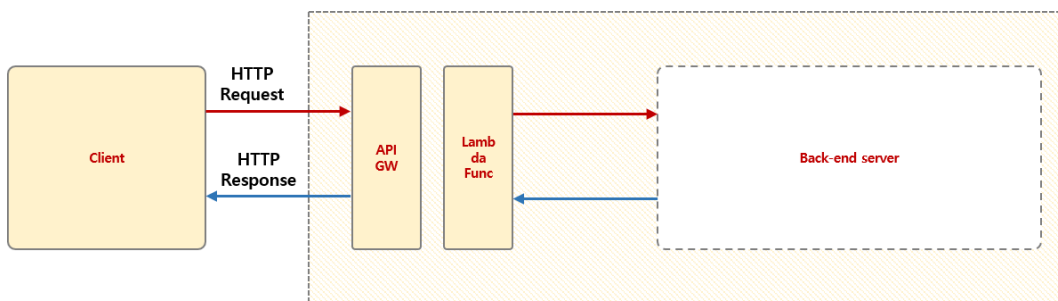
#### ● AWS Lambda 사용

- ✓ 기존 KuKuDocs Document Server 구성도 ( 예상 )

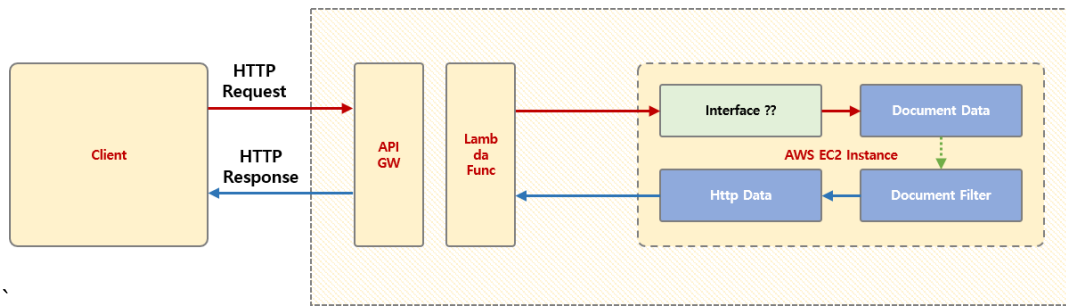


[그림 2-1 KuKuDocs]

- ✓ AWS API Gateway + Lambda 를 통한 서비스 구성도 ( 예상 )



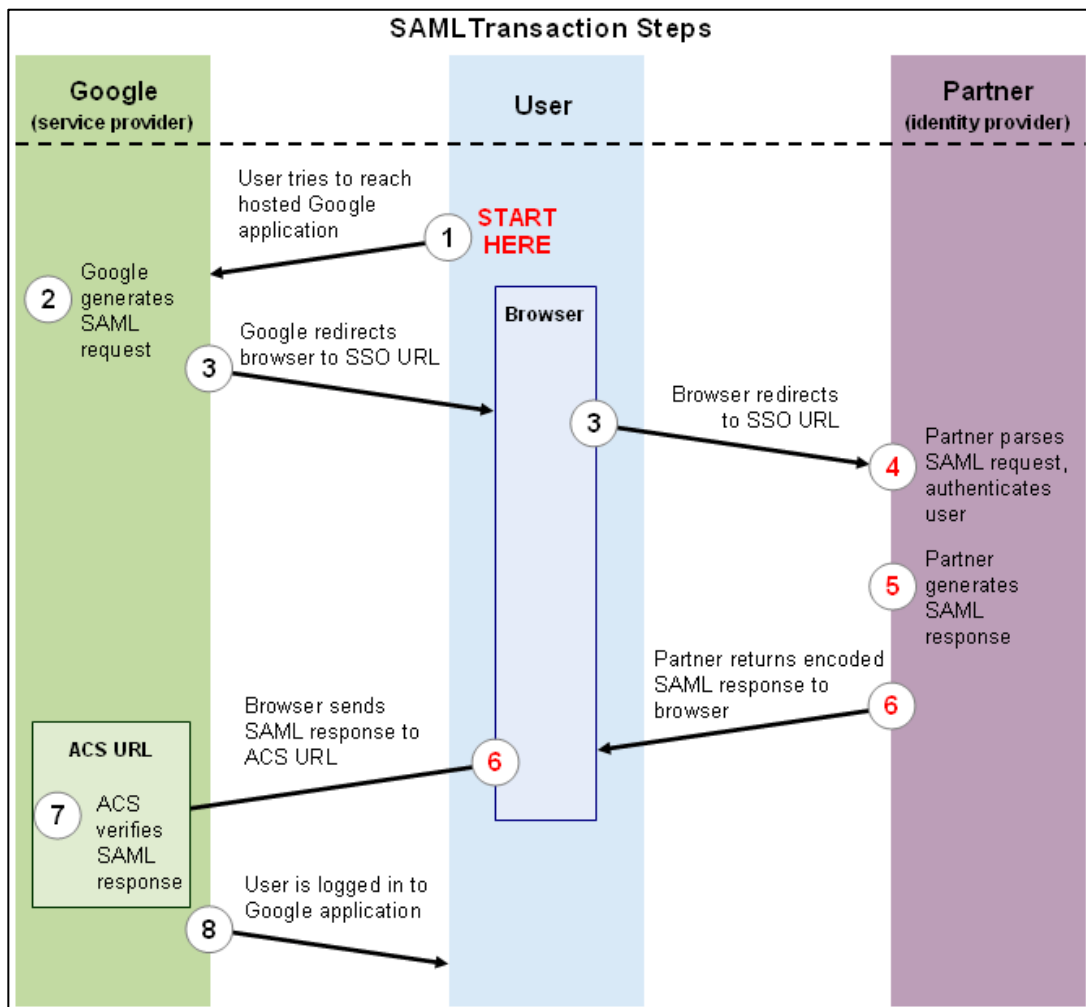
✓ **KuKuDocs Intergration 방안 (예상,, 구성 가능한지 검토 필요)**



[그림 4-4 응답형 DLP 구성]

● **SSO (Single Sign On) 사용**

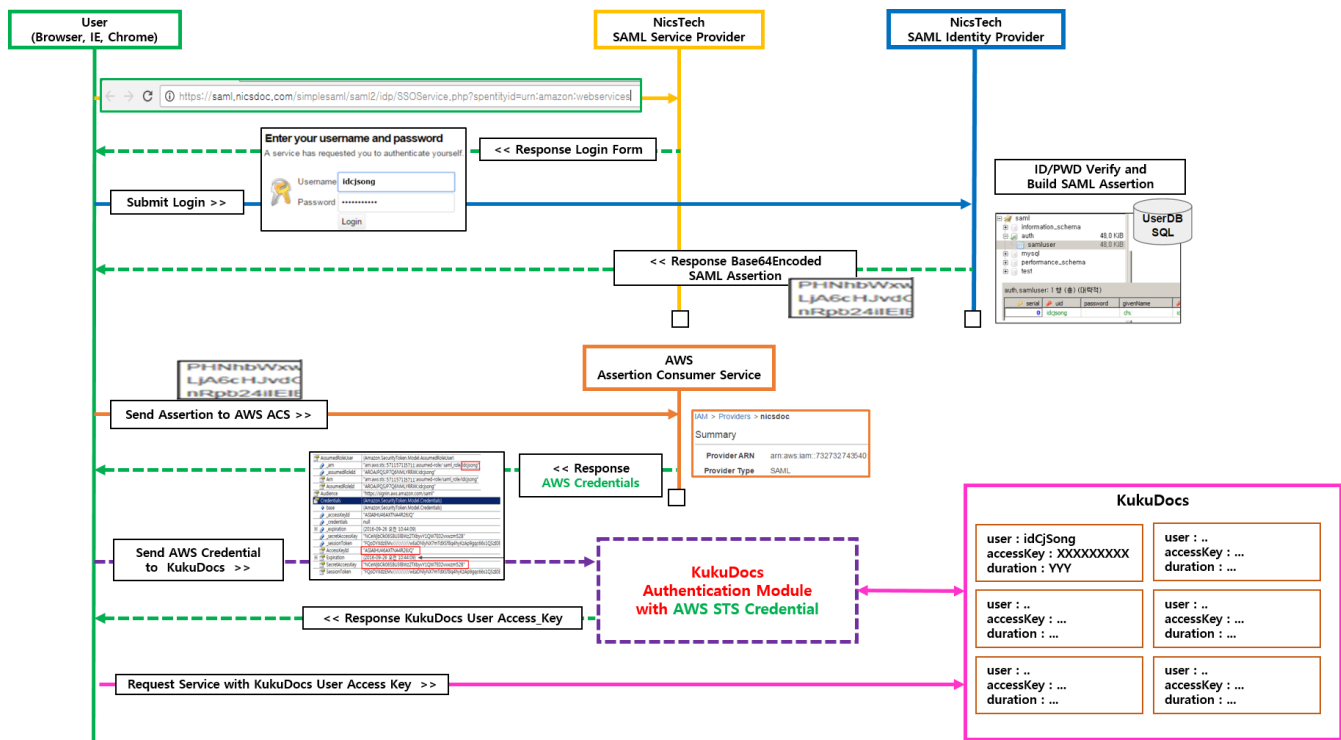
- ✓ SAML 사용 ( AWS 에서 제공하는 Service Provider, ID Provder 사용 )
- ✓ SAML 개요



✓ SAML 동작 시퀀스

- 1) 유저는 서비스 제공자 (SP)에 접근
- 2) 서비스 제공자는 SAML Request 를 생성 ( XHTML 로 생성되어 유저에게 응답 )
- 3) 유저의 브라우저는 SP 에서 응답받은 SSO URL 로 (인증제공자, Identity Provider)로 Redirect 한다.  
- 보통 SSO Login 폼 페이지로 Redirect 되고, 유저는 Login 정보를 입력하고 Submit 한다. (SAMLRequest 전달)
- 4) 인증제공자(IdP, Identity Provider)는 유저로부터 받은 SAMLRequest 를 파싱한후 유저인증 진행
- 5) IdP 는 인증정보에대한 SAMLResponse 를 생성한다.  
- SAMLResponse 는 IdP 의 전자서명이 포함( Base64 Encoding )
- 6) IdP 는 유저에게 SAMLResponse 를 전달
- 7) 유저의 브라우저는 ACS URL 로 SAMLResponse 를 전달  
- ACS URL ( Assertion Consumer Service URL)  
- ACS 는 서비스 제공자가 운영  
- 유저로부터 전달받은 SAMLResponse 를 확인 (ACS 는 SAMLResponse 의 전자서명을 검증 한다)  
- 실제 서비스 사이트로 유저를 Forward
- 8) 유저는 로그인에 성공하고 서비스를 제공받음

✓ SAML Intergration flow



✓ 구성요소

- 1) Service Provider : 닉스테크가 AWS 상에 구성
- 2) ID Provider : 닉스테크가 AWS 상에 구성

3) User : KuKuDocs 에 해당

✓ KuKuDocs 이슈

- 1) Nicstech 로부터 Redirection URL 을 제공 받아 Service Provider 로 Redirect 해야 함 (시퀀스 1 에 해당)
- 2) Service Provider 로 붙은 받은 SSO URL 및 HTML Form 을 통해 IP 프로바이더로 Redirect (시퀀스 3 에 해당)
- 3) ID Provider 로 부터 전달받은 Response 를 Service Provider 로 전달 (시퀀스 6 에 해당)
- 4) Service Provider 로 부터 전달받은 Credential 을 파싱 후 토큰으로 사용 (시퀀스 8 에 해당)  
(가장 중요한 부분)