# Seguridad de la red de la nube: Configuración ADFS para incluir a los grupos específicos a la hora de la autenticación

## Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Antecedentes](#)
[Configurar](#)
[Verificación](#)
[Troubleshooting](#)

## Introducción

Este documento describe cómo configurar los servicios federados Microsoft Active Directory (ADFS) como proveedor de la identidad (IdP), que envía a los detalles específicos del grupo al servicio de la Seguridad de la red de la nube de Cisco (CWS), bastante que una lista completa de membresías del grupo.

## Prerequisites

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de seguridad de la red de la nube con el portal de ScanCenter
- Autenticación del lenguaje de marcado de la aserción de la Seguridad (SAML)
- La administración del servidor de Microsoft ADFS

### Componentes Utilizados

La información en este documento se basa en la versión 2.0 de Microsoft ADFS, esos funcionamientos en el r2 2008 del Servidor Windows.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Antecedentes

Cuando ocurre el proceso de autenticación entre un buscador del cliente, el servidor ADFS (el IdP) y CWS (el proveedor de servicio (el SP)), toda la información se cifra y se agrega a la cadena URL en el buscador del cliente. Esto significa que la cadena URL es más larga cuando más información se envía al CWS.

Cuando usted configura SAML la autenticación (con Microsoft ADFS) para el uso con el servicio del CWS, usted debe configurar una confianza de confianza del partido para proporcionar la información del nombre de usuario y del grupo. Seguridad de la red de la nube: Configure el usuario/los atributos del grupo con PingFederate y ADFS mientras que el usar SAML describe este paso más detalladamente.

El número de grupos que agregan a un usuario a aumenta el tamaño URL. Si un usuario pertenece a un gran número de grupos del Active Directory (AD), el URL viene un tamaño por el que el límite impuesto navegador URL esté alcanzado, y el proceso de autenticación falla.

Cada navegador pudo definir su propia longitud permitida máximo URL. El RFC 2616 no especifica un Largo máximo, pero los límites prácticos son impuestos por los vendedores del navegador.

> **Note**: No es posible definir explícitamente a un número máximo de grupos porque un grupo no tiene un número fijo de caracteres. Por ejemplo, GroupA tiene menos caracteres que Test_Group_A. Para definir a varios grupos que permanece debajo del límite URL depende de la cuenta de carácter del Domain Name + del nombre del grupo.

# Configurar

Usted puede configurar el servidor de Microsoft ADFS para incluir a los grupos específicos en el proceso de autenticación. Usted seleccionaría típicamente solamente a los grupos usados en las reglas para filtros de la red del CWS. Cuando usted funciona con una auditoría de las directivas que existen, ayudan a determinar a los grupos que son ya funcionando.

Nuevo y las implementaciones que existen ya debe seguir la configuración de la mejor práctica que proporciona estas ventajas:

- Guarda el tamaño URL a un mínimo
- Acelera el proceso de autenticación entre el IdP (ADFS) y el SP (el CWS)
- Guarda el ancho de banda en cada pedido de autenticación

Configuración de la mejor práctica

Las confianzas del proveedor de las demandas abiertas y crean dos que la aceptación transforma las reglas:

La plantilla de la regla de la demanda del uso envía los atributos LDAP como demandas

**Almacén del atributo:** AD;

**Atributo LDAP:** Token-grupos - Nombres incompetentes;

**Tipo saliente de la demanda:** Grupo

La plantilla de la regla de la demanda del uso envía los atributos LDAP como demandas

**Almacén del atributo:** AD;

**Atributo LDAP:** SAM-Cuenta-nombre;

**Tipo saliente de la demanda:** Nombre

Cree la emisión transforman las reglas abriendo las confianzas de confianza de la parte y creando dos transforme las reglas:

El uso transforma una plantilla entrante de la demanda

**Tipo entrante de la demanda:** Nombre

**Formato:** sin especificar

**Tipo saliente de la demanda:** Nombre ID

**Formato:** Sin especificar

Seleccione el paso con todos los valores de la demanda

Utilice el passthrough o filtre una demanda entrante

**Tipo entrante de la demanda:** Grupo

Paso selecto con solamente los valores de la demanda que comienzan con un valor específico:

Especifique sus nombres del grupo AD

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- Mientras que está abierto una sesión como el usuario final, hojee a http://whoami.scansafe.net.
- La salida debe enumerar solamente a los grupos especificados en el procedimiento previamente mencionado, bastante que una lista completa de membresías del grupo.

# Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.