Fallos de inscripción en ZTNA para usuarios invitados con cuentas personales de Google en Cisco Secure Access

Contenido

Problema

Durante la implementación del acceso privado con ZTNA (acceso a la red de confianza cero), la inscripción de un usuario invitado con una cuenta personal de Google falla después del registro exitoso en el ID de Entra y el aprovisionamiento en el acceso seguro. Los síntomas específicos encontrados incluyen:

- Inscripción basada en el cliente: El proceso de inscripción alcanza la autenticación SSO, se proporcionan credenciales, pero ZTNA muestra un "error de E/S" y el proceso de inscripción se atasca
- Acceso sin cliente: Devuelve el mensaje de error "Cisco Secure Access Login failure. Check IDP Configuration" junto con un ID de transacción

Estos fallos impiden el acceso a los recursos privados y afectan a las pruebas de la funcionalidad de ZTNA para el acceso de tipo contratista mediante identidades no corporativas.

Entorno

- Cisco Secure Access con implementación de ZTNA
- ID de Microsoft Entry (anteriormente Azure AD) como proveedor de identidad
- Cuenta personal de Google (@gmail.com) registrada como usuario invitado en la ID de Entra
- Cuenta de invitado aprovisionada y visible en Secure Access
- Autenticación SAML configurada entre Entra ID y Cisco Secure Access

Resolución

El error de inscripción se resolvió modificando la configuración de asignación de atributos SAML en Microsoft Entra ID. Se adoptaron las siguientes medidas para resolver el problema:

Paso 1: Análisis del comportamiento del cliente y el paquete DART

Revise el paquete DART para confirmar que los componentes de Cisco Secure Client y ZTA funcionan correctamente. El análisis debe verificar que el flujo de inscripción llega correctamente a Cisco Secure Access y que el fallo se produce durante la autenticación SAML con el proveedor de identidad.

Paso 2: Examinar registros de autenticación de ID de entrada

Compruebe los registros de autenticación de ID de entrada para confirmar que el proceso de autenticación se completa correctamente desde la perspectiva del proveedor de identidad. Los registros deben mostrar una autenticación exitosa, pero Secure Access rechaza el inicio de sesión debido a la discordancia de atributos.

Paso 3: Identificar problema de asignación de atributos SAML

Determine que la ID de entrada está emitiendo el UPN (nombre principal de usuario) como la reclamación SAML, que no coincide con la identidad personal de la cuenta de Gmail esperada por Secure Access. El atributo IdP declarado no corresponde al identificador de usuario esperado.

Paso 4: Modificar asignación de atributos SAML

Cambie la asignación del atributo SAML en Microsoft Entry ID de UPN a Email Address. Esto garantiza que la reclamación de la dirección de correo electrónico coincida con la identidad personal de la cuenta de Google.

Paso 5: Verificar el éxito de inscripción

Después de implementar el cambio de asignación de atributos, vuelva a intentar el proceso de inscripción ZTNA. Cisco Secure Access ZTA debe reconocer ahora la dirección de Gmail y permitir que la inscripción se complete correctamente.

Causa

La falla de inscripción fue causada por una discordancia entre el atributo SAML que afirma Microsoft Entra ID y el identificador de usuario esperado en Cisco Secure Access. La ID de entrada se configuró para enviar el UPN (nombre principal de usuario) como la reclamación SAML, pero para las cuentas personales de Google (@gmail.com), este UPN no se correspondía con la identidad de la dirección de correo electrónico real. Cisco Secure Access esperaba recibir la dirección de correo electrónico como el atributo de identificación para comparar con la cuenta de usuario invitado aprovisionada, lo que resultaría en un rechazo de autenticación a pesar de una autenticación de IdP exitosa.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).