Sincronización de identidad de Cisco Secure Access con Active Directory y Microsoft EntraID

Contenido

Problema

Los usuarios experimentaron dificultades al intentar aprovisionar usuarios y grupos de dos orígenes de identidad con el mismo nombre de dominio en Cisco Secure Access. El escenario específico implicaba la sincronización de identidades de Active Directory local y Microsoft EntraID (anteriormente Azure AD), donde ambos orígenes utilizaban el mismo nombre de dominio (por ejemplo, domain.com).

Las principales preocupaciones fueron:

- Comprender cómo se comportan la propiedad de identidad y la asignación de pertenencia a grupos cuando existen los mismos usuarios y grupos en ambos orígenes de identidad
- Garantizar la aplicación uniforme de políticas de acceso seguro para los usuarios híbridos que acceden a los recursos tanto en las instalaciones como en la nube
- Mantener la visibilidad de IP interna para los usuarios en esta configuración de identidad híbrida
- Determinar si la sincronización simultánea de ambos orígenes causaría problemas en un entorno de producción

La documentación indicaba que "la sincronización simultánea de los mismos usuarios y grupos desde Cisco AD Connector y la aplicación Cisco User Management for Secure Access no es compatible y conduce a una aplicación de reglas de acceso incoherente".

Entorno

- Cisco Secure Access con integración de AD Connector y EntraID

- Active Directory local con nombre de dominio que coincide con el dominio EntraID
- Microsoft EntraID (Azure AD) con el mismo nombre de dominio que AD local
- Configuración de SSO de SAML para federación de identidades
- Módulo de gateway web seguro (SWG) para la aplicación de políticas
- Entorno híbrido que requiere acceso a recursos in situ y en la nube

Resolución

Se confirmó el siguiente comportamiento para la sincronización simultánea de los orígenes de Active Directory y EntraID:

Comportamiento de sincronización de grupo

Al sincronizar grupos con el mismo nombre de ambos orígenes:

- En Cisco Secure Access se crean dos objetos de grupo independientes, uno de cada origen
- Los grupos se pueden distinguir por su prefijo de origen en las directivas de acceso
- Los grupos de AD en las instalaciones se muestran como: AD-Domain/GroupName
- Los grupos EntraID aparecen como: GroupName

La verificación del laboratorio mostró una sincronización correcta con el mensaje "Correcto. <<<< Sincronizado" para grupos de varios dominios EntraID.

Comportamiento de sincronización de usuario

Al sincronizar usuarios con el mismo ID de usuario de ambos orígenes:

- La identidad del usuario se sobrescribe durante la sincronización

- Solo queda visible una ID de usuario única en Secure Access
- El origen de sincronización final determina los atributos y las pertenencias a grupos del usuario
- La sincronización de EntraID suele tener prioridad sobre AD en las instalaciones cuando ambos están configurados

Configuración de política de acceso

Ambos tipos de grupos se pueden utilizar en las políticas de acceso:

- Haga referencia a los grupos de AD en las instalaciones mediante la ruta completa: AD-Domain/GroupName
- Haga referencia a los grupos EntraID utilizando el nombre simple: GroupName
- Las políticas pueden diferenciar entre usuarios en función de su origen de pertenencia a grupos

La configuración siguiente funciona bien para muchos clientes.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

Causa

Durante las pruebas, confirmamos que siempre que un usuario se sincroniza desde el conector de AD en las instalaciones, "reclama" esa identidad en el panel de Umbrella. Si ese mismo usuario ya existe a través de la sincronización de Azure AD, la sincronización local sobrescribirá los datos de usuario de EntraID existentes.

Este comportamiento es una limitación documentada. Según la documentación técnica oficial de Cisco: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"No se admite la sincronización simultánea de las mismas identidades de usuario y grupo desde

Umbrella AD Connector y la aplicación Cisco Umbrella Azure AD, lo que provoca una aplicación de políticas incoherente".

Conclusión: Se confirma que la configuración deseada (visibilidad de VA para los usuarios existentes tanto en Azure como en las instalaciones) es una configuración no compatible.La ruta de acceso requiere el uso de clientes de roaming para garantizar la aplicación coherente de la identidad.

Contenido relacionado

- Aprovisionar identidades de Azure AD: documentación de Cisco Umbrella
- 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).