

Solucionar problemas de sincronização de identidade de usuário/grupo no Cisco Secure Access com IDP diferente

Contents

Problema

Este documento descreve como solucionar problemas de sincronização de identidade de usuário e grupo no Cisco Secure Access com diferentes Provedores de Identidade (IdPs), como Okta, Microsoft Entra ID e IBM Cloud.

Ambiente

- Cisco Secure Access — Integração de provisionamento SCIM
- Aplica-se ao conector SCIM 2.0 IdP (Okta, Azure AD)

Resolução

Overview

O Cisco Secure Access oferece suporte ao provisionamento de identidades de usuários e grupos diretamente do Okta e do Microsoft Entra ID (antigo Azure AD) usando o padrão SCIM 2.0, que elimina a necessidade de implantar um conector local do Active Directory (AD) para origens de identidade somente em nuvem. Este artigo consolida as suposições de arquitetura, os modos de falha comuns e a orientação para solução de problemas que engenheiros de campo e administradores encontram com mais frequência quando implantam ou mantêm essa integração.

Este documento está organizado em quatro seções:

- Configuração — onde obter instruções oficiais de configuração
- Suposições de arquitetura que, se violadas, causam falhas silenciosas ou difíceis de diagnosticar
- Problemas específicos do provedor (Okta versus Entra ID)
- Problemas genéricos do protocolo SCIM que se aplicam independentemente do IdP

Configuração

Este artigo se concentra na solução de problemas, não na configuração inicial. Use as Notas técnicas oficiais da Cisco neste documento para a configuração passo a passo:

- Para configurar o Cisco Secure Access com o Microsoft Entra ID (Azure AD), consulte este link: [Provisionar usuários e grupos para acesso seguro via Entra ID](#)
- Para configurar o Cisco Secure Access com o Okta, consulte este link: [Provisionar usuários e grupos para acesso seguro via OKTA](#)

Ambos os documentos abordam a geração do token SCIM e a URL de provisionamento no Secure Access, a configuração do aplicativo correspondente no IdP e a execução da sincronização de provisionamento inicial.

Introdução à arquitetura

Antes de solucionar o problema, confirme se a implantação corresponde a essas principais suposições. A maioria das falhas de sincronização retornam a uma dessas suposições.

Uma origem de identidade por vez

O provisionamento simultâneo dos mesmos usuários ou grupos a partir de um conector AD local e um IdP de nuvem (ID Okta ou Entra) não é suportado e leva à aplicação inconsistente de políticas. Se você migrar do Conector AD para um IdP de nuvem:

- Interrompa o serviço do Conector AD local.
- Confirme se nenhum trabalho de sincronização residual está em execução antes de habilitar o provisionamento de IdP de nuvem.

Os dispositivos virtuais são a exceção

O Entra ID ou Okta não pode fornecer integração de identidade para Virtual Appliances (VAs), porque o IdP não tem visibilidade nos mapeamentos de IP para usuário privados, que os VAs exigem. As implantações de VA ainda precisam do conector AD local, independentemente do que for usado para outros componentes.

Atribuir versus Enviar por push

- Ação: Atribuindo usuários ou grupos ao aplicativo
 - O que ele realmente faz: Provisiona os usuários membros desse grupo para Acesso Seguro
- Ação: Enviando um grupo (Okta)
 - O que ele realmente faz: Provisiona o próprio objeto de grupo (para direcionamento de política). Ele não sincroniza nenhum usuário.



Note: Não envie um grupo que também esteja atribuído ao aplicativo para provisionamento de usuários. Isso pode criar um estado de grupo duplicado ou conflitante.

Limites de grupo e usuário

Não há limite rígido para o número de usuários provisionados de qualquer IdP.

Os grupos são limitados. Historicamente, eram 200 grupos por organização da Okta ou da Entra ID; algumas documentações atuais mostram um teto maior (até 1.000) especificamente para Okta. Trate o número exato como dependente do ambiente e confirme com o Cisco Technical Assistance Center (TAC) ou a documentação atual da Cisco. Grupos além do limite não são provisionados silenciosamente, e nenhum erro é detectado.

Se precisar de uma cobertura mais ampla, use um grupo dinâmico "Todos os usuários" (Entra ID) ou "Todos" (Okta) em vez de uma tentativa de enviar cada grupo individualmente.

Ciclo de vida do token SCIM

No Cisco Secure Access, os tokens são gerados quando você escolhe Connect > Users, Groups and Endpoint Devices > Configuration Management > Integrate Directory. O token é mostrado apenas uma vez na criação.

Quando você regenera o token, ele imediatamente interrompe o provisionamento no lado do IdP até que o novo token seja inserido na configuração de provisionamento do Microsoft Entra ID ou Okta. Não há período de cortesia e o erro do lado do IdP é geralmente genérico (falha de autenticação) em vez de uma mensagem de token expirado.

Atualize o token periodicamente para garantir a segurança e teste a conexão no lado do IdP imediatamente após a rotação.

Questões Específicas do Okta

- Sintoma: Os grupos não aparecem no acesso seguro
 - Causa raiz: O envio de um grupo apenas provisiona o objeto do grupo; ele não sincroniza membros.
 - Resolução: Certifique-se de que os membros relevantes do grupo sejam atribuídos separadamente ao aplicativo em Atribuições.
- Sintoma: Usuários provisionados, mas atributos ausentes ou incorretos
 - Causa raiz: Acesso Seguro somente superfícies Nome de Exibição e Nome de Usuário; Os nomes fornecidos e de família não estão listados.
 - Resolução: Confirmar se os atributos necessários estão explicitamente selecionados para sincronização; não suponha que todos os campos de perfil do Okta sejam propagados.
- Sintoma: O provisionamento silencioso não faz nada
 - Causa raiz: As opções Criar usuários, Atualizar atributos do usuário ou Desativar usuários não estão habilitadas.

- Resolução: Verifique se todas as três estão marcadas em Provisionamento > Para aplicativo no console do administrador do Okta.
- Sintoma: objectGUID ou atributo personalizado não está sincronizando
 - Causa raiz: O atributo não é adicionado e mapeado por meio do Mapeamento de Perfil de Usuário.
 - Resolução: Adicione o atributo objectGUID e crie o mapeamento de perfil correspondente se esse identificador for necessário.
- Sintoma: Sincronização interrompida após a rotação de token
 - Causa raiz: Token SCIM ou API gerado novamente no Secure Access, mas não atualizado no Okta.
 - Resolução: Insira o novo token em Provisionamento > Configurar integração de API e execute Testar credenciais de API novamente.
- Sintoma: Não é possível determinar por que um usuário ou grupo específico falhou
 - Causa raiz: Os logs não foram verificados primeiro.
 - Resolução: Marque Reports > System Log no Okta, filtrado para o aplicativo Cisco User Management Connector, antes de escalar.
- Sintoma: Contagem de grupos excede limite, alguns ausentes sem erro
 - Causa raiz: A organização tem mais grupos com escopo do que o acesso seguro oferece.
 - Resolução: Reduza o escopo somente para grupos relevantes à política ou envolva o Cisco TAC para obter suporte de grupo de nível superior.

Problemas Específicos do Microsoft Entra ID

- Sintoma: A associação de grupo dinâmico não reflete no Secure Access
 - Causa raiz: A regra de grupo dinâmico está configurada incorretamente ou o grupo não está no escopo provisionado.
 - Resolução: Valide a regra de associação dinâmica diretamente no Entra ID antes de assumir um bug de sincronização do Secure Access.
- Sintoma: Esperava-se que o SAML SSO conduzisse a identidade SWG
 - Causa raiz: O AnyConnect Secure Web Gateway (SWG) não oferece suporte à

autenticação Security Assertion Markup Language (SAML) contra Entra ID; ele usa o mesmo mecanismo de autenticação passiva que o AD local.

- Resolução: Não criar identidades SWG orientadas por SAML para Entra ID; use autenticação passiva conforme documentado.
- Sintoma: O usuário mostra incorretamente o
 - Causa raiz: ID da Entra enviada ativa: falso porque o usuário saiu de um escopo de grupo atribuído ou um mapeamento de atributo ativo está configurado incorretamente.
 - Resolução: Verificar se o usuário foi removido de um grupo com escopo; verifique o mapeamento ativo (geralmente deve ser avaliado como Not([isSoftDeleted])).
- Sintoma: Aplicativo em quarentena, todo o provisionamento foi interrompido
 - Causa raiz: O aplicativo de destino retornou respostas repetidas não compatíveis com SCIM.
 - Resolução: Verifique o status de provisionamento do aplicativo empresarial para um sinalizador de quarentena antes de supor falhas individuais do usuário.
- Sintoma: O ciclo inicial de provisionamento falha completamente
 - Causa raiz: Falha de sincronização transitória na primeira execução.
 - Resolução: Clique em Reiniciar Provisionamento na página Visão Geral para forçar o Entra ID a tentar novamente a sincronização inicial.
- Sintoma: Mesclagem inesperada de usuários duplicados
 - Causa raiz: Duas identidades de origem compartilham o mesmo e-mail ou nome UPN.
 - Resolução: Garantir a exclusividade do e-mail e do UPN no diretório de origem; verifique se o atributo mail vem de um domínio verificado.
- Sintoma: O atributo pára de ser atualizado após uma alteração de esquema
 - Causa raiz: O tipo de atributo foi alterado no lado de destino (por exemplo, string para booleano), mas o mapeamento de ID de Entra não foi atualizado.
 - Resolução: Corrija manualmente o tipo em Configurações Avançadas em Mapeamentos de Atributos.
- Sintoma: A referência do gerente nunca é preenchida
 - Causa raiz: Um usuário estava no escopo antes de seu gerente estar; o provisionamento não é preenchido automaticamente.
 - Resolução: Reinicie o provisionamento para forçar a reavaliação completa de todos os usuários no escopo.

Segurança da IBM Verificar problemas específicos

- Sintoma: Os usuários provisionam, mas os grupos nunca aparecem no Acesso seguro
 - Causa raiz: Verifique se o conector SCIM personalizado está emitindo somente operações do usuário; nenhuma chamada POST /Groups é enviada (lacuna de capacidade de provisionamento de conta, não um erro de mapeamento).
 - Resolução: Capture um rastreamento de conector e confirme se ocorrem quaisquer chamadas/Grupos; Se não houver, provisione grupos por meio do Cisco AD Connector, importação de CSV ou um script agendado no endpoint Secure Access SCIM.
- Sintoma: A atualização da associação de grupo falha com 400 ou 404
 - Causa raiz: members[].value references Verifique os IDs de usuário internos em vez do acesso seguro do ID SCIM retornado na criação do usuário.
 - Resolução: Corrija o mapeamento de membros para usar a ID SCIM do Secure Access e execute uma sincronização completa novamente.
- Sintoma: Os grupos são exibidos, mas estão vazios
 - Causa raiz: Grupo enviado antes que seus usuários membros existissem no Secure Access; membership PATCH fez referência a usuários desconhecidos.
 - Resolução: Executar uma sincronização completa novamente agora que os usuários existem; certifique-se de que a ordenação de sincronização crie usuários antes de grupos.
- Sintoma: Loops de login SAML ou redirecionamentos repetidos
 - Causa raiz: Verifique se o ponto de extremidade do IdP está no proxy ou descriptografado pelo SWG, o que interrompe o fluxo de autenticação.
 - Resolução: Ignore a URL Verify IdP de SAML ou descriptografia (lista de domínios externos ou descriptografia seletiva).
- Sintoma: O usuário se autentica via SAML, mas nenhuma política baseada no usuário corresponde
 - Causa raiz: SAML NameID não corresponde ao usuário provisionado authName .
 - Resolução: Alinhe o formato NameID > no aplicativo Verify SAML com o mapeamento de atributo authName (geralmente e-mail ou UPN); teste novamente.
- Sintoma: O provisionamento pára de funcionar após semanas ou meses de estabilidade

- Causa raiz: O token SCIM foi girado ou expirou no Secure Access, mas não foi atualizado no conector Verify.
- Resolução: Atualize o token no Secure Access e atualize-o no aplicativo Verify custom; agenda o ritmo de atualização.
- Sintoma: Usuários duplicados criados na ressincronização
 - Causa raiz: externalId mapeada para um atributo mutável ou não exclusivo (por exemplo, nome para exibição, email alterável).
 - Resolução: Mapeie externalId para um identificador imutável (Verificar ID de usuário ou objectGUID); limpe as duplicatas e sincronize novamente.
- Sintoma: Desativado Verificar se os usuários permanecem ativos no Secure Access
 - Causa raiz: Ação de suspensão não mapeada para ativo:false ou operação de desativação desabilitada no conector.
 - Resolução: Habilite a operação de desativação e mapeie a suspensão para ativo:false; verificar com um usuário de teste.
- Sintoma: Alterações de atributo em Verificar não propagar
 - Causa raiz: Usuário ou atributo fora do escopo da política de provisionamento ou operação de atualização desabilitada.
 - Resolução: Revisar a política de provisionamento de aplicativos ou direitos; habilitar atualizações; acione uma sincronização manual.
- Sintoma: O Secure Access rejeita solicitações com erros de esquema ou estilo 501
 - Causa raiz: Carga não compatível com SCIM (matriz de esquemas ausente, URN incorreto, operação sem suporte).
 - Resolução: Reproduzir com o teste de ondulação de linha de base; Corrigir a carga útil ou o mapeamento; escale para IBM se o conector emitir a solicitação malformada.
- Sintoma: Identidade SWG ausente para usuários em roaming apesar do SAML funcionar
- Causa raiz: Esperando que o SAML direcione a identidade para um modo de implantação que usa a identidade passiva ou baseada em agente.
- Resolução: Confirme o método de aquisição de identidade para cada modo de implantação em relação à documentação do Secure Access; não criar SAML como a única origem de identidade.

Problemas genéricos de SCIM

Eles não são específicos da Cisco, mas aparecem de forma consistente nas implantações do Secure Access porque o transporte subjacente é o SCIM 2.0 padrão:

- Os estados de quarentena mascaram erros individuais: Se a sincronização parecer ter sido totalmente interrompida em vez de falhar por usuário, verifique se há um estado de quarentena ou suspensão no nível do aplicativo antes de investigar problemas de atributos individuais.
- 409 Conflito na desativação: Um padrão comum em que o IdP tenta desativar um usuário e o destino lança um conflito. Isso geralmente é um mapeamento de atributo ativo ou um problema de escopo de grupo, não um erro de sistema verdadeiro.
- Os campos em branco ou desmarcados nem sempre são propagados: Algumas implementações de servidor SCIM retêm o último valor não nulo; quando você limpa um campo no IdP, pode exigir que você primeiro insira um valor de espaço reservado.
- As alterações de URL ou configuração invalidam silenciosamente a autenticação: Qualquer alteração na URL do ponto final SCIM geralmente exige que você forneça o token do portador novamente. Os erros surgem como URL inválida mesmo quando o problema real é um token obsoleto.
- Nenhum webhook nativo ou fluxo de eventos: A automação que espera notificações por push em tempo real sobre alterações de usuário ou de política deve pesquisar a API de relatórios ou integrar-se por meio do Cisco XDR. O Secure Access não emite webhooks de provisionamento de saída.

Encaminhe para o Cisco TAC com logs de provisionamento do lado do IdP se as etapas anteriores não resolverem o problema. Os logs de provisionamento de back-end no lado do acesso seguro geralmente exigem acesso do TAC para recebimento.

Causa

A integração de provisionamento SCIM falhou ao enviar um ou mais registros devido a um token de portador expirado, incompatibilidade de mapeamento de atributo, grupo de destino ausente ou escopo de provisionamento insuficiente.

Conteúdo relacionado

- Cisco: [Provisionar usuários e grupos para acesso seguro via Entra ID](#)
- Cisco: [Provisionar usuários e grupos para acesso seguro via OKTA](#)
- Aprendizado da Microsoft: Problemas conhecidos de conformidade com o protocolo SCIM 2.0 - ID do Microsoft Entra
- Aprendizado da Microsoft: Solucionar erros da API SCIM da ID do Microsoft Entra
- Configure o SAML SSO no provedor de identidade: <https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider>
- Provisionamento para aplicativos personalizados (SCIM):
<https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications>
- Visão geral de provisionamento e governança (conector SCIM genérico):
<https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance>
- Ponte de provisionamento local (origens AD/LDAP):
<https://docs.verify.ibm.com/verify/docs/on-premises-provisioning>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.