BadSuccessor 2026 : Attaque Entra ID et AD DS Hybride

BadSuccessor Entra ID attaque 2026 : exploiter les dMSA pour escalader Domain Admin et compromettre votre tenant. Analyse technique et remédiation.

Résumé exécutif

BadSuccessor représente l'une des vulnérabilités les plus dangereuses identifiées en 2025-2026 pour les infrastructures Microsoft hybrides. Elle exploite les *delegated Managed Service Accounts* (dMSA) de Windows Server 2025 pour permettre une escalade de privilèges complète vers Domain Admin, avec propagation directe vers Entra ID via Entra ID Connect Sync. Un attaquant disposant uniquement de la permission `CreateChild` sur une OU peut compromettre l'ensemble du domaine Active Directory et le tenant Entra ID en quelques minutes.

Sévérité : Critique — escalade Domain Admin + compromission cloud Entra ID

Prérequis minimal : Permission `CreateChild` sur n'importe quelle OU du domaine

Environnements ciblés : AD DS Windows Server 2025 en configuration hybride Entra ID

Remédiation disponible : Patches Microsoft 2025 + durcissement des délégations d'administration

En 2026, la surface d'attaque des infrastructures Microsoft hybrides s'est considérablement élargie avec la démocratisation de Windows Server 2025 et l'adoption massive d'Entra ID

Connect Sync dans les entreprises françaises. La technique **BadSuccessor Entra ID attaque 2026**, initialement documentée par les chercheurs d'Akamai Security Research, s'est rapidement imposée comme l'une des menaces les plus critiques pesant sur les environnements Active Directory hybrides. Elle exploite une faille de conception fondamentale dans les *delegated Managed Service Accounts* (dMSA), une fonctionnalité introduite dans Windows Server 2025 pour simplifier la gestion des comptes de service. En abusant du mécanisme de succession de mots de passe inhérent aux dMSA, un attaquant disposant de permissions apparemment anodines — la simple capacité à créer des objets dans une unité organisationnelle — peut escalader ses privilèges jusqu'au niveau Domain Admin en quelques commandes, puis propager la compromission vers Entra ID via la synchronisation hybride d'Entra ID Connect Sync. Les équipes Red Team et les acteurs malveillants exploitent cette technique avec des outils open source modifiés depuis début 2026, rendant la menace immédiatement opérationnelle pour tout profil disposant de compétences intermédiaires en sécurité Active Directory. Cet article détaille l'anatomie complète de l'attaque, les prérequis techniques, les phases d'exploitation pas à pas, les indicateurs de compromission, et les contre-mesures à déployer en urgence pour protéger votre infrastructure AD DS et Entra ID.

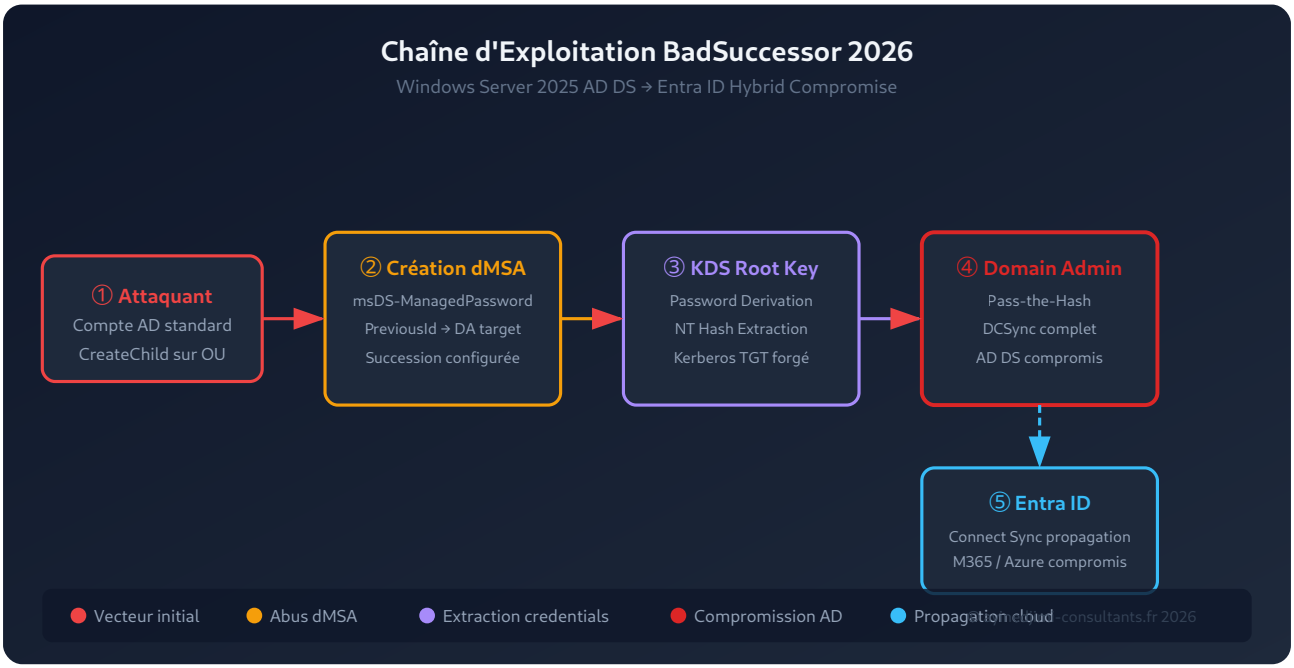

Figure 1 — Chaîne d'exploitation BadSuccessor 2026 : de la permission CreateChild sur une OU à la compromission totale d'AD DS et d'Entra ID via Entra ID Connect Sync.

BadSuccessor Entra ID : anatomie d'une attaque critique 2026

BadSuccessor est le nom donné à une technique d'attaque découverte par les chercheurs d'Akamai Security Research, exploitant une faille de conception dans les *delegated Managed Service Accounts* (dMSA), un type de compte introduit avec Windows Server 2025. Contrairement aux vulnérabilités classiques qui nécessitent une faille logicielle exploitable (dépassement de tampon, injection de code), BadSuccessor abuse d'une fonctionnalité légitime — le mécanisme de succession de comptes de service — pour effectuer une escalade de privilèges totale jusqu'au Domain Admin.

> ⚡ **Retour terrain**
>
> Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles (adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

Le principe est élégant dans sa simplicité destructrice : un dMSA peut être configuré pour succéder à un compte de service existant, héritant automatiquement de ses credentials via le *Key Distribution Service* (KDS). En 2026, les équipes Red Team et les acteurs malveillants ont pleinement intégré cette technique dans leurs arsenaux offensifs, souvent en combinaison avec des outils comme impacket et des scripts Python dédiés. La technique est référencée dans le cadre MITRE ATT&CK T1087 (Account Discovery) ainsi que des sous-techniques relatives à l'abus des comptes de service managés dans les environnements hybrides.

La criticité de BadSuccessor tient à son prérequis remarquablement bas : il suffit qu'un attaquant dispose de la permission `CreateChild` sur une unité organisationnelle (OU) du domaine.

Cette permission est couramment accordée à des comptes de service applicatifs, des administrateurs délégués de département, ou même des utilisateurs standard dans des environnements avec une délégation d'administration peu maîtrisée. Une fois cette seule condition remplie, l'escalade complète vers Domain Admin peut s'effectuer en moins de cinq minutes avec les outils disponibles publiquement en 2026.

Architecture cible : Entra ID Connect Sync et AD DS hybride

Pour comprendre l'impact de BadSuccessor sur les environnements hybrides, il est essentiel de saisir la relation entre **Active Directory Domain Services** (AD DS) on-premises et **Entra ID** (anciennement Azure Active Directory) dans le cloud. La majorité des grandes et moyennes entreprises françaises opèrent aujourd'hui en mode hybride : leur annuaire AD DS est synchronisé vers le cloud Microsoft via *Entra ID Connect Sync*, permettant l'accès aux ressources cloud avec les identités d'entreprise.

Cette architecture hybride crée une dépendance bidirectionnelle critique en matière de sécurité. Selon la documentation officielle Microsoft Entra Identity, Entra ID Connect Sync synchronise non seulement les attributs utilisateurs mais également les hachages de mots de passe via le mode Password Hash Sync (PHS) et les informations d'authentification Kerberos. Cette synchronisation signifie que compromettre un compte privilégié dans AD DS conduit directement à la compromission du même compte dans Entra ID.

En pratique, si un attaquant obtient les credentials d'un compte Domain Admin synchronisé via BadSuccessor, il dispose non seulement d'un accès total à l'infrastructure on-premises, mais également aux ressources cloud associées : Microsoft 365, SharePoint Online, Azure subscriptions, et l'intégralité des applications SaaS fédérées via Entra ID. C'est cette propagation automatique vers le cloud qui confère à BadSuccessor un niveau de criticité exceptionnel en 2026, bien au-delà des techniques d'escalade de privilèges AD classiques.

Le mécanisme dMSA : fonctionnement légitime et détournement

Les **delegated Managed Service Accounts** ont été introduits dans Windows Server 2025 comme évolution des Group Managed Service Accounts (gMSA). Leur objectif légitime est de permettre la migration transparente de comptes de service existants vers des comptes managés avec rotation automatique des mots de passe gérée par le KDS. La fonctionnalité de "succession" permet à un dMSA d'hériter des permissions d'un ancien compte de service durant la phase de migration.

Techniquement, la succession fonctionne via l'attribut `msDS-ManagedPasswordPreviousId` et le processus de dérivation de mot de passe par le KDS Root Key. Lorsqu'un dMSA est marqué comme successeur d'un compte cible, le Key Distribution Service génère un mot de passe calculé à partir des credentials du compte cible, accessible à tout hôte autorisé à lire le compte managé. Ce mécanisme suppose que seul un administrateur légitime — ayant accès à l'ancien compte — créera ce type de succession. C'est précisément cette hypothèse de sécurité implicite que BadSuccessor invalide.

L'attaquant crée un dMSA malveillant dans une OU où il dispose de droits `CreateChild`, puis configure ce dMSA comme successeur d'un compte privilégié ciblé — un Domain Admin ou un compte avec droits DCSync. Le KDS génère alors un mot de passe dérivé des credentials du compte cible, que l'attaquant peut calculer indépendamment. Les Shadow Credentials documentées par Alsid représentent une menace comparable via l'attribut `msDS-KeyCredentialLink`, mais BadSuccessor exploite un vecteur distinct avec des prérequis encore plus accessibles dans les configurations d'entreprise typiques.

> ### Avertissement éthique et légal
>
> Les techniques décrites dans cet article sont présentées à des fins de formation en cybersécurité défensive et de sensibilisation des équipes Blue Team et SOC. La reproduction de ces attaques sur des systèmes sans autorisation écrite préalable constitue une infraction pénale au sens de l'article 323-1 du Code pénal français, passible de deux

> ans d'emprisonnement et 60 000 euros d'amende. Ces informations ne doivent être utilisées que dans le cadre d'opérations Red Team contractuelles, de tests d'intrusion autorisés, ou d'environnements de laboratoire strictement isolés du réseau de production.

Exploitation pas-à-pas : de l'utilisateur non-privilégié au Domain Admin

Environnement de laboratoire requis

- Windows Server 2025 Domain Controller avec niveau fonctionnel de domaine Windows Server 2025
- Un compte utilisateur avec permission `CreateChild` sur une OU cible (compte de service applicatif, utilisateur délégué, etc.)
- Station d'attaque Linux : impacket (fork BadSuccessor), Python 3.10+, Kerberos utilities, BloodHound
- Réseau de laboratoire totalement isolé d'Internet et des environnements de production

La chaîne d'exploitation BadSuccessor suit une séquence reproductible en cinq phases distinctes. Pour une compréhension approfondie des primitives offensives sous-jacentes, la lecture de notre guide sur l'exploitation Active Directory avec impacket est fortement recommandée avant d'aborder cet article. Les techniques de pentest Active Directory complet servent de socle à la compréhension du contexte d'attaque.

Phase 1 — Reconnaissance et identification des permissions : L'attaquant commence par énumérer les ACL des OU du domaine pour identifier celles sur lesquelles il dispose de la permission `CreateChild`. Des outils comme BloodHound avec SharpHound ou des requêtes LDAP directes permettent cette énumération systématique. En 2026, des versions de BloodHound intègrent nativement la détection des vecteurs BadSuccessor et affichent les chemins d'attaque dMSA dans l'interface graphique.

Phase 2 — Identification du compte cible : L'attaquant identifie le compte privilégié à cibler pour la succession. Il choisit idéalement un Domain Admin ou un compte synchronisé avec Entra ID pour maximiser l'impact. La cartographie des comptes à haute valeur repose sur des requêtes LDAP classiques et l'analyse des membres des groupes Domain Admins, Enterprise Admins, et Administrators.

Phase 3 — Création du dMSA malveillant : L'attaquant crée un nouveau dMSA dans l'OU ciblée, en configurant l'attribut `msDS-ManagedPasswordPreviousId` pour pointer vers le compte cible. Cette étape peut s'effectuer via des outils LDAP standards (ldapadd, ldapmodify) ou des scripts Python basés sur impacket. La création d'un dMSA est une opération LDAP légitime qui, sur des configurations par défaut non durcies, ne déclenche aucune alerte de sécurité.

Phase 4 — Extraction du mot de passe dérivé par KDS : En utilisant les API KDS appropriées, l'attaquant calcule le mot de passe du dMSA — cryptographiquement dérivé des credentials du compte cible. Cette étape requiert l'accès au KDS Root Key depuis le domaine. Certaines variantes de l'attaque utilisent des techniques de coercition d'authentification pour forcer l'accès au KDS sur des configurations restrictives.

Phase 5 — Mouvement latéral et compromission totale : Avec le hash NT ou le ticket Kerberos du compte cible, l'attaquant effectue un Pass-the-Hash pour accéder aux systèmes cibles. Si le compte ciblé est Domain Admin, un DCSync permet d'extraire tous les hachages du domaine en quelques secondes. La technique s'articule naturellement avec le mouvement latéral dans les environnements Windows AD en 2026 pour une compromission complète de l'infrastructure.

Phase	Action offensive	Outil type	Détectabilité	Événement Windows
1 — Recon	Énumération ACL OU	BloodHound / LDAP	Faible	4662
2 — Targeting	Mapping comptes privilégiés	SharpHound / ldapsearch	Faible	4624, 4662
3 — Exploitation	Création dMSA malveillant	Python / LDAP scripts	Moyenne	5137 (création objet)
4 — Credential	Extraction KDS / NT Hash	impacket fork BadSuccessor	Haute	4769, 4768
5 — Impact	Pass-the-Hash / DCSync	secretsdump.py, mimikatz	Haute	4624, 4776, 4662

Indicateurs de compromission et stratégies de détection Blue Team

La détection efficace de BadSuccessor repose sur une surveillance proactive des événements LDAP et Kerberos dans l'environnement Active Directory. L'activation du mode d'audit étendu sur les Domain Controllers — notamment *Audit Directory Service Access*, *Audit Object Access*, et *Audit Account Management* — constitue un prérequis absolu que de nombreuses organisations n'ont pas encore activé en 2026.

Les principaux **indicateurs de compromission** à surveiller sont les suivants :

> **Événement 5137** : Création d'objet dans l'annuaire AD — surveiller spécifiquement la création de nouveaux objets de type `msDS-GroupManagedServiceAccount` dans des OU inhabituelles ou par des comptes non-administrateurs
>
> **Événement 4662** : Accès à un objet annuaire — alerter sur les accès aux attributs `msDS-ManagedPasswordId` et `msDS-ManagedPasswordPreviousId` par des comptes non-systèmes et non-Domain Controllers
>
> **Événement 4769** : Demandes de tickets de service Kerberos pour des comptes dMSA récemment créés ou peu connus de l'environnement

Événement 4670 : Modifications des permissions sur des OU sensibles, indicateur d'une préparation ou d'une élévation du niveau de délégation par un attaquant

Requêtes LDAP anormales : Recherches ciblant les attributs `msDS-GroupMSAMembership`, `msKds-RootKeyData`, ou `msDS-ManagedPasswordInterval` par des comptes non-Domain Controllers

Nouveaux dMSA avec liens de succession vers des comptes privilégiés : Tout dMSA dont le `msDS-ManagedPasswordPreviousId` pointe vers un compte dans les groupes Domain Admins, Enterprise Admins, ou Schema Admins doit être considéré comme suspect

Microsoft Defender for Identity (MDI) propose des détections comportementales spécifiques aux abus de dMSA depuis mi-2025. Les règles de détection Sigma communautaires pour BadSuccessor sont disponibles sur le dépôt SigmaHQ et s'intègrent dans Splunk, Elastic SIEM, et Microsoft Sentinel. Il est recommandé de corréler les événements DC avec les données NetFlow et les logs Entra ID pour identifier des patterns de propagation post-compromission vers le cloud.

Comparaison avec les techniques d'attaque AD classiques en 2026

BadSuccessor se distingue des techniques d'attaque Active Directory classiques par l'accessibilité de son vecteur d'entrée et la rapidité de son exécution. Une comparaison structurée met en lumière sa dangerosité spécifique par rapport aux techniques bien établies. Le Kerberoasting requiert l'identification de comptes de service avec des SPN valides et reste bloqué par des politiques de mots de passe robustes ; BadSuccessor contourne entièrement ces contrôles en s'appuyant sur le mécanisme de dérivation KDS indépendant de la politique de mots de passe.

Les *Shadow Credentials*, technique comparable exploitant l'attribut `msDS-KeyCredentialLink`, nécessitent des droits d'écriture sur cet attribut pour un compte cible spécifique — une permission généralement absente des délégations standards. BadSuccessor est statistiquement plus probable dans les environnements d'entreprise réels, car la délégation de gestion sur des OU est une pratique courante de distribution des tâches administratives, contrairement à la permission d'écriture sur `msDS-KeyCredentialLink`.

En termes de **bruyance réseau**, BadSuccessor génère moins de trafic Kerberos anormal que le Kerberoasting ou l'AS-REP Roasting, qui produisent de nombreuses requêtes TGS vers des comptes de service. Cela le rend plus difficile à détecter par des solutions NDR (Network Detection and Response) basées sur l'analyse comportementale du trafic Kerberos seul, sans corrélation avec les logs LDAP des Domain Controllers.

Technique	Prérequis minimal	Impact maximum	Détectabilité NDR	Correctif disponible
BadSuccessor 2026	CreateChild sur OU	Domain Admin + Entra ID	Faible	Patch WS2025 (2025)
Kerberoasting	Utilisateur AD standard	Comptes de service	Haute	Politique mots de passe
DCSync	Droits réplication AD	Domain Admin (hashes)	Haute	Restriction ACL
Shadow Credentials	Write msDS-KeyCredentialLink	Compte cible spécifique	Moyenne	Patch + ACL review
Pass-the-Hash	NT Hash valide obtenu	Variable selon compte	Haute	Credential Guard

Impact réel : entreprises et organisations françaises exposées en 2026

En France, l'adoption de Windows Server 2025 s'est accélérée tout au long de 2025 et 2026, notamment dans les secteurs financier, industriel, de la santé et des administrations publiques. Plusieurs milliers d'organisations françaises opèrent aujourd'hui des infrastructures hybrides AD DS / Entra ID avec des niveaux fonctionnels de domaine Windows Server 2025, leur ouvrant la possibilité d'utiliser les dMSA — et, par conséquent, les exposant au vecteur BadSuccessor si les patches et configurations de sécurité adéquats ne sont pas en place.

La *surface d'attaque* française est particulièrement exposée pour plusieurs raisons structurelles. Premièrement, les migrations vers Windows Server 2025 sont souvent conduites sans audit

préalable des délégations d'administration existantes sur les OU — des permissions accordées il y a plusieurs années dans le cadre de projets de délégation et jamais révisées constituent autant de vecteurs potentiels pour BadSuccessor. Deuxièmement, l'activation des dMSA est parfois effectuée de façon transparente lors des mises à niveau du niveau fonctionnel, sans évaluation spécifique du risque lié à cette fonctionnalité.

Les secteurs les plus exposés en France incluent les **établissements de santé** (qui ont massivement déployé Windows Server 2025 suite aux injonctions de modernisation post-cyberattaques), les **collectivités territoriales** (dont les équipes IT sont souvent peu nombreuses et les audits de délégation rares), et les **ETI industrielles** ayant opté pour des architectures hybrides Microsoft dans le cadre de leur transformation numérique 2025-2026.

À RETENIR

À retenir

BadSuccessor est opérationnel depuis 2025 : Des outils publics automatisent son exploitation pour des profils offensifs intermédiaires

Le prérequis est minimal : La permission `CreateChild` sur une OU suffit — auditez vos délégations d'administration en urgence

L'impact est maximal : De l'escalade Domain Admin à la compromission totale d'Entra ID en une seule chaîne d'attaque

La détection nécessite une préparation préalable : L'audit étendu des DC et les règles SIEM spécifiques doivent être activés avant l'incident

Le patch existe depuis 2025 : L'application des mises à jour Windows Server 2025 est la première priorité technique absolue

La remédiation complète va au-delà du patch : Audit ACL/OU, revue de tous les dMSA existants, restriction du scope Entra Connect Sync

Mitigation et hardening : protéger son infrastructure AD et Entra ID

La protection contre BadSuccessor s'articule autour de plusieurs axes complémentaires, dont certains constituent des bonnes pratiques générales de sécurité Active Directory recommandées par l'ANSSI dans ses guides de configuration. Microsoft a publié des mises à jour correctives en 2025 qui modifient le comportement du KDS lors de la création de comptes successeurs, mais leur seule application ne suffit pas à éliminer le risque dans les environnements existants comportant des configurations héritées vulnérables.

Mesure prioritaire 1 — Application des patches Windows Server 2025 : Installer l'intégralité des mises à jour Windows Server 2025 liées aux dMSA et au mécanisme KDS. Microsoft a renforcé les vérifications lors de la création de comptes successeurs pour limiter le vecteur d'exploitation original. Cette mise à jour est déployable via Windows Update, WSUS, ou Microsoft Endpoint Configuration Manager.

Mesure prioritaire 2 — Audit exhaustif des délégations d'administration : Inventorier toutes les OU du domaine et identifier les principals disposant de la permission `CreateChild`. Révoquer les délégations inutiles et appliquer rigoureusement le principe du moindre privilège. Des outils comme ADACLScanner ou des scripts PowerShell utilisant `Get-ACL` sur les objets AD permettent cet audit. Il est recommandé d'effectuer cette revue trimestriellement et après toute migration de niveau fonctionnel.

Mesure prioritaire 3 — Inventaire et validation de tous les dMSA existants : Lister tous les dMSA présents dans le domaine et vérifier que chacun possède un propriétaire légitime, une justification métier documentée, et un attribut `msDS-ManagedPasswordPreviousId` ne pointant vers aucun compte privilégié sans raison valide. Supprimer les dMSA orphelins ou non documentés. La commande `Get-ADServiceAccount -Filter * -Properties msDS-ManagedPasswordId, msDS-ManagedPasswordPreviousId` permet cet inventaire depuis n'importe quel membre du domaine.

Mesure prioritaire 4 — Restriction du scope Entra ID Connect Sync : Configurer **Entra ID Connect Sync** pour ne synchroniser que les comptes et groupes strictement nécessaires vers Entra ID. L'activation du filtrage par OU ou par groupe réduit considérablement l'impact d'une

compromission AD sur l'environnement cloud. Les comptes de service et les comptes techniques ne devraient jamais être synchronisés vers Entra ID sans nécessité explicite.

Mesure prioritaire 5 — Activation de Microsoft Defender for Identity et règles SIEM : Déployer MDI sur tous les Domain Controllers pour bénéficier des détections comportementales spécifiques aux abus dMSA. Intégrer les règles de détection Sigma BadSuccessor dans le SIEM de l'organisation (Microsoft Sentinel, Splunk, Elastic). Configurer des alertes prioritaires sur les événements 5137, 4662, et 4769 associés à des dMSA nouvellement créés.

- Appliquer immédiatement les patches Windows Server 2025 sur tous les Domain Controllers
- Auditer les ACL de toutes les OU avec ADACLScanner et identifier les permissions CreateChild excessives
- Inventorier et valider chaque dMSA existant dans l'annuaire AD
- Restreindre le scope de synchronisation Entra Connect aux comptes strictement nécessaires
- Déployer les règles de détection Sigma BadSuccessor dans le SIEM
- Activer Microsoft Defender for Identity sur tous les Domain Controllers
- Former les équipes AD admin aux IoC de BadSuccessor et aux procédures de réponse à incident
- Planifier un exercice Red Team incluant le vecteur BadSuccessor pour valider la détection en conditions réelles

---

FAQ : BadSuccessor, Entra ID et sécurité Active Directory en 2026

Comment BadSuccessor permet-il d'escalader les privilèges jusqu'au Domain Admin dans un environnement Entra ID ?

BadSuccessor exploite le mécanisme de succession des delegated Managed Service Accounts (dMSA) de Windows Server 2025. Un attaquant disposant uniquement de la permission `CreateChild` sur une OU crée un dMSA malveillant, en configurant son attribut `msDS-ManagedPasswordPreviousId` pour pointer vers un compte Domain Admin cible. Le Key

Distribution Service (KDS) génère automatiquement un mot de passe dérivé des credentials du compte ciblé, conformément au mécanisme de succession prévu pour les migrations. L'attaquant calcule ce mot de passe dérivé, obtient le hash NT ou un ticket Kerberos valide pour le compte Domain Admin, et effectue un Pass-the-Hash ou un DCSync pour extraire l'intégralité des hachages du domaine. Si le compte Domain Admin compromis est synchronisé vers Entra ID via Entra ID Connect Sync, la compromission se propage immédiatement au tenant cloud, donnant accès à Microsoft 365, Azure, et toutes les applications SaaS fédérées. Cette progression de l'utilisateur bas-privilégié au Domain Admin puis à Entra ID peut s'effectuer en moins de dix minutes dans un environnement non patché.

Quels sont les prérequis techniques pour exploiter BadSuccessor en 2026 ?

Les prérequis de BadSuccessor sont remarquablement accessibles, ce qui explique sa dangerosité particulière parmi les techniques d'attaque Active Directory documentées en 2026. L'attaquant doit disposer d'un compte utilisateur valide dans le domaine Active Directory ciblé — n'importe quel compte authentifié, même sans privilèges. Il doit ensuite identifier une OU sur laquelle ce compte (ou un groupe dont il est membre) dispose de la permission LDAP `CreateChild`, permission souvent accordée dans le cadre de délégations d'administration partielles pour des projets ou des départements spécifiques. Enfin, l'environnement doit opérer un niveau fonctionnel de domaine Windows Server 2025 avec la fonctionnalité dMSA disponible — ce qui est le cas de toute organisation ayant migré ou promu un Domain Controller Windows Server 2025. En 2026, des scripts Python open source basés sur des forks d'impacket automatisent l'intégralité de la chaîne d'exploitation en une seule commande, rendant l'attaque accessible sans nécessiter une compréhension approfondie des mécanismes cryptographiques KDS sous-jacents.

Comment détecter une attaque BadSuccessor dans les journaux Active Directory et Microsoft Sentinel ?

La détection efficace de BadSuccessor exige une journalisation avancée activée sur les Domain Controllers, notamment les catégories d'audit *Directory Service Access* et *Account Management*. Les événements prioritaires à surveiller sont l'événement 5137 (création d'objet dans l'annuaire) ciblant les nouveaux objets de type dMSA créés dans des OU inhabituelles ou par des comptes non-Domain Admins ; l'événement 4662 ciblant les accès aux attributs `msDS-`

`ManagedPasswordId`, `msDS-ManagedPasswordPreviousId`, et `msKds-RootKeyData` par des comptes non-systèmes ; et les événements Kerberos 4768/4769 pour des tickets liés à des dMSA récemment créés. Microsoft Defender for Identity (MDI) propose des alertes comportementales spécifiques depuis mi-2025. Les règles Sigma communautaires pour BadSuccessor sont disponibles sur SigmaHQ et directement importables dans Microsoft Sentinel via son connecteur de règles analytiques. Il est fortement recommandé de corréler ces événements avec les données NetFlow et les logs d'audit Entra ID pour identifier une propagation post-compromission vers le cloud.

Quelle est la différence entre BadSuccessor et les attaques par Shadow Credentials sur Active Directory ?

BadSuccessor et les Shadow Credentials partagent l'objectif d'obtenir des credentials permettant de s'authentifier en tant qu'un autre principal Active Directory, mais diffèrent fondamentalement dans leur mécanisme et leurs prérequis. Les Shadow Credentials exploitent l'attribut `msDS-KeyCredentialLink` : l'attaquant injecte un certificat dans cet attribut pour un compte cible, lui permettant ensuite de s'authentifier via PKINIT sans connaître le mot de passe — mais cela requiert des droits d'écriture sur l'attribut du compte cible spécifique, permission rarement accordée dans les environnements standards. BadSuccessor est plus permissif dans ses prérequis : la permission `CreateChild` sur n'importe quelle OU suffit, sans cibler un compte spécifique a priori, ce qui le rend statistiquement applicable dans un plus grand nombre d'environnements d'entreprise. Les deux techniques sont complémentaires dans un arsenal Red Team 2026 : BadSuccessor pour l'escalade initiale si `CreateChild` est disponible, Shadow Credentials pour la persistance post-compromission sur des comptes spécifiques. La référence de détection officielle pour les Shadow Credentials est disponible dans la documentation Alsid, aujourd'hui intégrée à la plateforme Tenable Identity Exposure.

Conclusion

BadSuccessor représente en 2026 une menace de premier rang pour l'ensemble des organisations opérant des environnements hybrides Active Directory / Entra ID. Sa dangerosité tient moins à sa

complexité technique — d'autres techniques AD sont plus élaborées — qu'à la combinaison redoutable d'un prérequis minimal accessible et d'un impact maximal couvrant à la fois l'infrastructure on-premises et le cloud Microsoft 365 via Entra ID Connect Sync. Les équipes de sécurité doivent traiter cette menace avec la même urgence qu'ont été traités EternalBlue ou PrintNightmare en leur temps.

La réponse défensive passe obligatoirement par trois piliers complémentaires : l'application des patches Windows Server 2025 comme action immédiate, un audit exhaustif et régulier des délégations d'administration AD et des dMSA existants comme action structurelle, et le déploiement de règles de détection spécifiques dans les outils SIEM et EDR couplé à Microsoft Defender for Identity comme action de surveillance continue. La formation des équipes AD admin aux vecteurs offensifs 2026 incluant BadSuccessor, combinée à des exercices Red Team réguliers validant l'efficacité des mesures défensives déployées, constitue le socle d'une posture de sécurité résiliente face à cette classe de menaces.