

الذكاء الاصطناعي الوكيل: ما الذي يحتاج مديرو تقنية المعلومات إلى معرفته؟



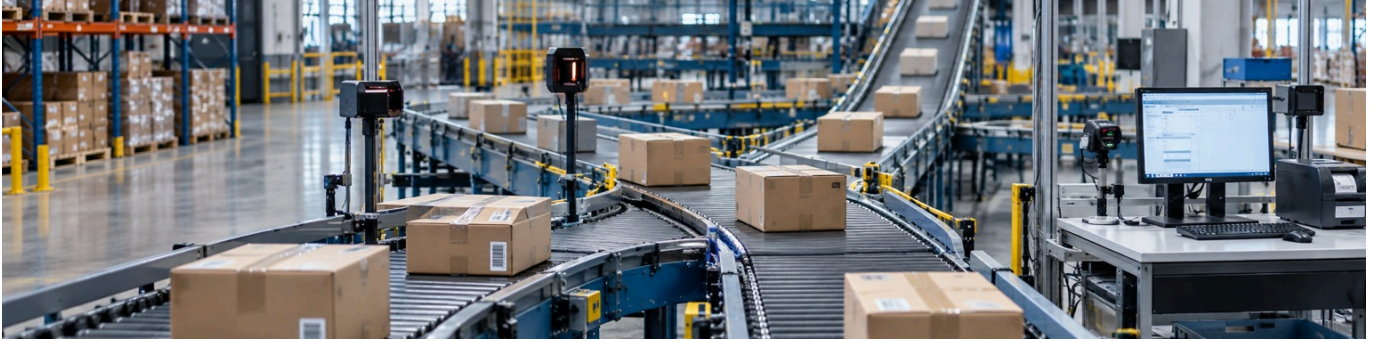
دليل عملي لتفويض المهام مع الحفاظ على التحكم

صلاحيات محددة. تنفيذ متحقق منه.
قرارات عملية لقادة التقنية في المؤسسات السعودية.

سبتمبر 2026 | النسخة العربية

ابدأ بالمهمة قبل اختيار الوكيل

القرار الأول لمدير تقنية المعلومات هو تحديد ما إذا كانت المهمة تحتاج أصلاً إلى تنفيذ يتكيف مع المستجدات.



يتجاوز الذكاء الاصطناعي المؤسسي إنتاج الإجابات إلى إنجاز العمل. وبالنسبة لمدير تقنية المعلومات، يتمثل التحول الأهم في الربط بين النموذج والأنظمة التي يستطيع التأثير فيها. فالإجابة المفيدة يمكن مراجعتها قبل أن يتصرف أحد بناءً عليها، أما الوكيل الذي يمتلك صلاحيات تشغيلية فيستطيع تعديل سجل أو إطلاق إجراء أو إنشاء التزام بينما لا تزال المهمة قيد التنفيذ.

تميّز Anthropic بين سير العمل ذي الخطوات المحددة مسبقاً، والوكلاء الذين يختارون مسار عملهم واستخدامهم للأدوات بصورة ديناميكية. وهذا التمييز مفيد لقرارات الاستثمار؛ إذ ينبغي أن تعالج المرونة مشكلة فعلية في التنفيذ، لأن زيادة الاستقلالية قد تضيف أيضاً زمن استجابة وتكلفة ومسارات محتملة للفشل. [1]

وجهة نظر سَحْب

تعامل مع الوكيل بوصفه تفويضاً للعمل ضمن حدود واضحة. حدّد المهمة والإجراءات المسموح بها وأدلة الإنجاز وآلية إعادة المهمة إلى شخص مسؤول، قبل اختيار المنصة.

اختر أبسط نمط تنفيذ يناسب المهمة

مثال	نقطة البداية المفضلة	خصائص المهمة
التحقق من طلب وفق مجموعة معروفة من الحقول الإلزامية.	الأتمتة التقليدية	قواعد ثابتة وخطوات متوقعة
تصنيف طلب خدمة ثم توجيهه عبر مسار الموافقات القائم.	سير عمل يتضمن خطوة بالذكاء الاصطناعي	الحاجة إلى التقدير ضمن عملية مستقرة
التحقق في حالة استثنائية للتسليم عبر أنظمة الطلبات والمخزون والناقل المعتمدة.	وكيل يعمل ضمن حدود محددة	الخطوة التالية تعتمد على ما يُكتشف

تتسم المهمة الأولى الواعدة بنهاية واضحة، وأدلة يمكن الوصول إليها، وتبعات محدودة إذا وقع خطأ. فالتحقيق في طلب يمكن أن ينتج تفسيراً موثقاً دون السماح برد مبلغ أو تغيير التزام بالتسليم. ويسمح فصل التحقيق عن التنفيذ للفريق باختبار قدرة مفيدة قبل توسيع الصلاحيات.

بالنسبة للمؤسسات السعودية، يجب أن تعكس عينة المهام ظروف التشغيل الفعلية. مراسلات بالعربية والإنجليزية، وأسماء الجهات المحلية، وصلاحيات على مستوى الفروع، والتطبيقات التي يستخدمها الموظفون فعلاً. ولا يثبت العرض السلس ببيانات تجريبية نظيفة أن الوكيل سيتعامل بكفاءة مع سجلات متعارضة أو طلبات ناقصة.

السؤال الاستثماري محدد: ما الخطوة الصعبة التي سيحسنها التنفيذ المتكيف، وكيف ستعرف المؤسسة ذلك؟ إذا عجز الفريق عن الإجابة، فبسط الحل المقترح قبل تمويل نشر أوسع للوكلاء.

حدّد صلاحية التصرف

ينبغي تحديد الاستقلالية لكل إجراء على حدة، لا منحها للتطبيق بأكمله.



قد يُسمح للوكيل بقراءة سجل خدمة وإعداد تحديث مقترح وإنشاء مسودة تذكّرة، مع استمرار منعه من تغيير حقوق الوصول. هذه صلاحيات مختلفة داخل المهمة الواحدة. ووصف التطبيق بأكمله بأنه مستقل أو خاضع لإشراف بشري يحجب القرارات التي تهمّ فعلًا.

توصي سَحْب بوضع اتفاق يحدد ضوابط الإجراءات لكل عملية نشر. ويجب أن يوضح الموارد المشمولة والعمليات المسموح بها وشروط الموافقة وحدود الإنفاق وزمن التشغيل والأحداث التي تستوجب تسليم المهمة إلى شخص مسؤول. وينبغي تضمين هذا الاتفاق في ضوابط قابلة للإنفاذ داخل التطبيق، إلى جانب تعليمات النموذج.

الصلاحية	حدود التشغيل	الأدلة المطلوبة
القراءة والتحقق	استخدام مصادر البيانات المعتمدة فقط ضمن نطاق الصلاحيات الممنوح للمستخدم صاحب الطلب.	تسجيل المصادر وقرارات الوصول.
إعداد تغيير	إنشاء مسودة لا يمكن أن تتحول خفية إلى معاملة منفذة.	عرض التغيير المقترح والسجلات المتأثرة.
تنفيذ إجراء محدود	السماح بعمليات محددة منخفضة الأثر ضمن حدود صريحة.	تسجيل التفويض والطلب والحالة الناتجة.
تصعيد إجراء ذي تبعات مهمة	اشتراط موافقة شخص مخوّل على الإجراء المحدد قبل تنفيذه.	ربط الموافقة بالإجراء ومعلوماته والسياق الراهن.

اجعل الموافقة قراراً مبنياً على معلومات واضحة

ينبغي أن توضح شاشة الموافقة ما الذي سيتغير، ولماذا اقترح التغيير، وما إذا كان قابلاً للتراجع. وإذا تغير السجل المستهدف أو المعلومات الجوهرية بعد الموافقة، فيجب طلب قرار جديد. أما زر «متابعة» العام فلا يقدم دليلاً كافياً على أن المراجع فهم المعاملة.

اربط التنفيذ بهوية قابلة للتتبع، ذات صلاحيات محدودة وعلاقة واضحة بالمستخدم أو الخدمة التي بدأت الطلب. وأبق بيانات الاعتماد خارج المحتوى الذي يراه النموذج. ويجب ألا تكتسب المهمة المفوّضة صلاحيات أوسع لمجرد انتقالها إلى وكيل أو أداة أخرى.

صمّم للتعامل مع عدم اليقين
عند غموض الهوية أو الصلاحية أو السجل المستهدف، أوقف الإجراء وسلّم المهمة مع المعلومات اللازمة بصورة منظمة. عدم اليقين ليس إذنًا بالارتجال.

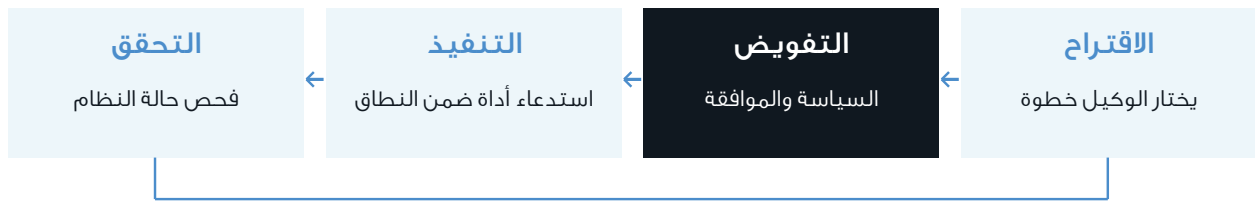
راجع ضوابط الإجراءات كلما تغيرت الأدوات أو صلاحيات الوصول إلى البيانات أو التبعات على الأعمال. ولا تبرر ترقية النموذج تلقائياً توسيع الصلاحيات؛ إذ تظل الحدود المعتمدة للمهمة هي القيد الحاكم.

ابن مسار تنفيذ خاضعاً للضوابط

ضع ضوابط قابلة للإنفاذ بين ما يقترحه الوكيل والنظام المؤسسي.



يجب ألا يكون النموذج صاحب القرار النهائي بشأن السماح بالإجراء الذي يقترحه. ويفصل التصميم الذي توصي به سحُب بين فهم المهمة والتفويض والتنفيذ والتحقق. ويمنح هذا الفصل مدير تقنية المعلومات نقاط تحكم واضحة، حتى عندما يتغير تسلسل خطوات التحقيق.



الاستمرار ضمن حدود المهمة فقط؛ وإلا التوقف أو التسليم إلى شخص مسؤول

زوّد الوكيل بالسياق المرتبط بالمهمة فقط، مع مصادر يمكن تحديدها. وقبل كل استدعاء لأداة، تتحقق بوابة السياسات من الهوية ونطاق الموارد ومعلومات الإجراء والموافقة المطلوبة. وتتيح موصلات الأدوات عمليات محدودة بمدخلات يجري التحقق من صحتها. ثم يفحص التحقق الحالة الناتجة في أنظمة الأعمال، ويوجّه حالات الإنجاز الجزئي أو غير المؤكد إلى مسار المعالجة والتعافي.

اجعل تبعات الإجراءات جزءاً أساسياً من التصميم

انتهاء مهلة الانتظار لا يثبت فشل الإجراء. فقد تُنشأ تذكرة حتى إذا لم يصل رد النظام إلى الوكيل. ولعمليات التي تغير حالة النظام، استخدم معرف طلب فريداً حيثما كان مدعوماً، وتحقق من السجل الناتج قبل إعادة المحاولة، وامنع تكرار التنفيذ. وإذا أمكن عكس الأثر، فحدّد إجراءً تعويضياً؛ وإن تعذر ذلك، فحدّد آلية لاحتواء الأثر والتعافي بتدخل بشري. افصل ذاكرة المهمة عن سجل الأعمال المعتمد. فقد تساعد الملاحظات المحفوظة على استمرارية العمل، لكن ينبغي ألا تتحول خفية إلى سياسات معتمدة أو حقائق متحقق منها. وحدّد مدة الاحتفاظ بها وأوجه إعادة استخدامها المسموح بها وكيفية التعامل مع التصحيحات أو المعلومات القديمة.

اشتراط وجود سجل تشغيل يربط الطلب الأصلي بإصدار الإعدادات واستدعاءات الأدوات والموافقات والنتيجة المتحقق منها. واحتفظ بالأدلة التشغيلية المفيدة مع ضوابط مناسبة للوصول والاحتفاظ، دون الاعتماد على الوصول إلى الاستدلال الداخلي الخفي للنموذج.

ابدأ بوكيل واحد قبل تعدد الوكلاء
لا تستخدم وكلاء متعددين إلا عندما تثبت الحاجة أن الفائدة تتجاوز تكلفة التنسيق. ويحتاج كل تسليم للمهمة إلى نطاق صريح، وحدود صلاحيات موروثه، ومسؤول واضح عن النتيجة النهائية.

أمن سلسلة الإجراءات كاملة

أهم المسار الممتد من المحتوى الخارجي إلى العمليات ذات الصلاحيات الحساسة.



يتطلب أمن الوكلاء الاهتمام بما يتجاوز النص الذي يُعرض على المستخدم. وتتناول إرشادات OWASP للذكاء الاصطناعي الوكيل المشكلة من خلال التهديدات ووسائل الحد منها عبر أنظمة الوكلاء. [2] وللمراجعة التي يقودها مدير تقنية المعلومات، حوّل هذا المنظور إلى سيناريوهات إساءة استخدام محددة تستهدف المهمة المقترحة والأدوات المتصلة بها. السيناريوهات التالية أسئلة عملية للمراجعة تقترحها سحب، وليست إعادة إنتاج لتصنيف خارجي للتهديدات. ويختبر كل منها إمكانية أن يؤثر مدخل يتحكم به مهاجم في إجراء لم تفوضه المؤسسة.

سيناريو إساءة الاستخدام	الاستجابة التصميمية	الاختبار قبل الإطلاق
مستند مسترجع يطلب من الوكيل تصدير سجلات داخلية.	التعامل مع المحتوى المسترجع كبيانات غير موثوقة، وتقييد الوجهات وصلاحيات الأدوات بصورة مستقلة.	إدراج تعليمات خبيثة في مستند واقعي والتحقق من منع التصدير.
وكيل يحاول الوصول إلى حالة تخص قسمًا آخر.	إنفاذ التفويض على مستوى المورد عند نقطة استدعاء الأداة.	طلب سجل يبدو صحيحًا لكنه خارج نطاق صلاحيات صاحب الطلب.
ملاحظة محفوظة تغير تفسير سياسة معتمدة.	الحفاظ على مرجعية المصادر وتقييد ما يمكن للذاكرة تحديثه.	إضافة ملاحظة متعارضة والتحقق من أولوية السياسة المعتمدة.
وكيل مفوض يحصل على وصول أوسع من نطاق المهمة الأصلية.	نقل قيود النطاق والموافقة عبر عمليات التفويض.	محاولة تنفيذ عملية محظورة عبر وكيل ثانٍ.
فشل متكرر يؤدي إلى محاولات لا تنتهي أو تغييرات مكررة.	تحديد ميزانيات وقواعد توقف وضوابط تمنع تكرار التنفيذ.	محاكاة انتهاء المهلة بعد تنفيذ المعاملة فعليًا.

أمن فريق التشغيل استجابة طوارئ قابلة للتطبيق

يجب أن يستطيع الفريق إيقاف الإجراءات الجديدة وسحب صلاحيات الأدوات وتحديد المعاملات الجارية، دون الاعتماد على تعاون الوكيل. وتدرّب على تحديد من يحق له تعليق التشغيل، وكيفية إبلاغ المستخدمين المتأثرين، وكيفية إعادة الخدمة إلى حالة آمنة. فزر الإيقاف وحده غير كافٍ دون إجراء للتعافي.

عند النشر في السعودية، وثّق مسارات انتقال الموجهات والمحتوى المسترجع وسجلات التتبع والنسخ الاحتياطية، ومن يمكنه الوصول إليها. واطلب من مسؤولي الخصوصية والأمن والامتثال المعنيين التحقق من توافق تدفق البيانات الكامل مع المتطلبات السارية. فموقع التطبيق الأساسي وحده لا يكفي لإثبات ما يحدث في كل خدمة متصلة به.

سؤال ما قبل الإطلاق

هل يستطيع الفريق إثبات أن المدخل الخبيث لا يمكنه تجاوز صلاحيات المهمة، وهل يستطيع احتواء الأثر إذا أخفق ضابط آخر؟

قيّم العمل المنجز

التفسير المقنع ليس دليلاً على حدوث الإجراء الصحيح.



تفصل إرشادات التقييم لدى Anthropic بين سجل تنفيذ الوكيل والحالة النهائية لبيئته. وتشير كذلك إلى الحاجة إلى تكرار التجارب لأن النتائج قد تختلف. [3] وينبغي لمديري تقنية المعلومات استخدام هذا التمييز للمطالبة بأدلة على العمل المنجز، بدل اعتماد الإجابة المصاغة بإتقان معياراً وحيداً للنجاح.

في حالة وكيل تذاكر الخدمة، قد يتطلب النجاح إنشاء التذكرة الصحيحة بالأولوية الصحيحة والمسؤول الصحيح. دون تغييرات غير مصرح بها في مواضع أخرى. أما تقييم الملخص المكتوب وحده فقد لا يكشف إسناد التذكرة إلى فريق خاطئ أو إنشاء نسخة مكررة أثناء إعادة المحاولة.

محور التقييم	الأدلة المطلوب جمعها	مثال على الفشل
نتيجة الأعمال	مقارنة السجل الناتج بالمهمة المقصودة.	يقول الوكيل إن التذكرة موجودة، لكنها لم تنشأ.
الالتزام بالحدود	فحص الإجراءات التي جرت محاولتها ونتائج التفويض.	محاولة بحث محظورة خلال تشغيل ناجح من الجوانب الأخرى.
القدرة على الصمود	اختبار البيانات الناقصة والتعارضات وانتهاء المهل وانقطاع التشغيل.	تشغيل مستأنف ينفذ التغيير نفسه مرتين.
تسليم المهمة إلى شخص مسؤول	التحقق من احتمال التصعيد وتوقيته.	يتلقى المراجع طلباً دون الأدلة اللازمة لاتخاذ القرار.
الأداء التشغيلي	قياس الزمن والتكلفة وجهد المراجعة من البداية إلى النهاية.	إجابة صحيحة تصل متأخرة بحيث تفقد فائدتها.

اختبر إعدادات النشر، لا النموذج وحده

اختبر الأعمال المعتادة والاستثناءات المشروعة ومحاولات إساءة الاستخدام باللغات والصيغ التي ستتعامل معها الخدمة. واحتفظ بمجموعة اختبار مستقلة لقرارات الإطلاق، حتى لا يحول الضبط التقييم إلى عرض متدرب عليه.

قيّم النموذج والتعليمات والأدوات والاسترجاع والصلاحيات معاً، وأعد الاختبار عند تغييرها. واستخدم فحوصاً حتمية للسجلات والتفويض، مع مراجعة بشرية بمعايير متسقة للأحكام التي تحتاج إليها.

حدّد معايير القبول قبل التجربة

اتفق على الإخفاقات التي تمنع الإطلاق، وتلك التي يمكن التعامل معها عبر التصعيد. ويجب ألا يحجب ارتفاع متوسط تقييم المهام إجراءات غير مصرح بها أو فشلاً في فئة حرجية من العمل.

واصل مراجعة عينات أثناء التشغيل الفعلي. وافصل بين حالات الرفض الآمن وإخفاقات التنفيذ والإنجاز المستقل والمهام التي استكملها شخص بعد تعثر الوكيل. فهذا يكشف ما إذا كانت الموثوقية تتحسن أم أن العمل ينتقل إلى المراجعين.

انشر لتحقيق القيمة مع مسار للخروج

استثمر في أدلة التنفيذ المفيد، لا في مظهر الاستقلالية.



ينبغي قياس اقتصاديات الوكيل على مستوى المهمة الكاملة. فاستخدام النموذج مجرد عنصر واحد؛ إذ تستهلك خدمات الأدوات وإعادة المحاولات والمراقبة والمراجعة البشرية وتصحيح الأخطاء موارد أيضاً. وقارن العملية المدعومة بالوكيل بالطريقة الحالية لتحقيق النتيجة المقبولة نفسها.

مقياس عملي للتكلفة

تكلفة المهمة المقبولة = إجمالي تكلفة التشغيل خلال فترة القياس / عدد المهام المنجزة وفق معيار القبول المتفق عليه. أدرج تكلفة عمليات التشغيل غير الناجحة في البسط، واعرض المهام المنجزة بمساعدة بشرية بصورة منفصلة.

ابدأ بتحقيق ضمن مكتب الخدمة

لنأخذ تجربة داخلية توضيحية في تقنية المعلومات لتحقيق في حوادث التطبيقات المتكررة. ابدأ بالسماح للوكيل بقراءة التذاكر ومقالات المعرفة المعتمدة، وجميع الأدلة، وإعداد توصية أولية. وأبق تغييرات الوصول وتعديلات إعدادات بيئة الإنتاج والرسائل الخارجية خارج نطاق صلاحياته الأولية.

قارن النتائج بحالات سابقة داخل بيئة معزولة، ثم شغل الوكيل إلى جانب الموظفين دون تنفيذ تغييرات. وانتقل إلى مجموعة محدودة من المستخدمين الفعليين عندما تدعم الأدلة ذلك، وقيّم كل صلاحية مضافة على حدة.

قبل الالتزام	الأدلة المطلوب طلبها
اختيار موزّد أو منصة	إثبات إنفاذ الصلاحيات وتصدير سجلات التتبع وإدارة إصدارات الإعدادات وسحب الوصول داخل بيئتك.
توسيع التجربة	عرض نتائج مهام متحقق منها، وعبء عمل المراجعين، وفئات الإخفاق، والتكلفة الإجمالية مقارنة بخط الأساس.
إضافة صلاحيات تشغيلية	اعتماد الإجراء الجديد المحدد واختبار مسارات فشله والتعافي منه.
التخطيط للخروج	تصدير تعريفات المهام والأدلة، وإلغاء بيانات الاعتماد، وإثبات وجود بديل يدوي قابل للتطبيق.

حدّد مسبقاً أسباب الإيقاف المؤقت: إجراءات غير مصرح بها، أو إخفاقات يتعذر تتبعها، أو عبء مراجعة مفرط، أو تكلفة غير مقبولة للمهمة المنجزة. ويجب أن يستند التوسع إلى الأدلة التشغيلية.

قرار مدير تقنية المعلومات

الهدف هو خدمة مفيدة بحدود صريحة ونتائج يمكن إثباتها. ويمكن لسحب دعم تقييم المهام المرشحة وتصميم ضوابط التنفيذ وتقييم تجربة محدودة النطاق. ابدأ بمهمة واحدة يمكن التحقق من نتائجها وحصص صلاحياتها، ولا تتوسع إلا عندما تبرر الأدلة ذلك.

الأدلة والمراجع

مصادر أولية تدعم منظوراً عملياً لمديري تقنية المعلومات.



تقدم هذه المقالة توصيات أصلية وسيناريوهات مؤسسية توضيحية طُورت لسُحب. وتدعم المنشورات الخارجية المفاهيم المشار إليها بالمراجع المرقمة. والأمثلة تصاميم مقترحة، وليست ادعاءات بنتائج مقاسة لدى عملاء.

Anthropic | Building effective agents [1]

نُشر في 19 ديسمبر 2024. يدعم التمييز بين سير العمل المحدد مسبقاً والوكلاء الموجهين ديناميكياً، والموازنة بين التعقيد وأداء المهمة.

[قراءة المصدر](#)

OWASP | Agentic AI – Threats and Mitigations [2]

نُشر في 17 فبراير 2025. مرجع لأمن الوكلاء يستند إلى نمذجة التهديدات. والسيناريوهات في هذه المقالة أمثلة عملية للمراجعة تقترحها سُحب، وليست تصنيف OWASP.

[قراءة المصدر](#)

Anthropic | Demystifying evals for AI agents [3]

يدعم تقييم سجلات التنفيذ والنتائج النهائية وتكرار التجارب وتقييم نظام الوكيل كما يُنشر فعلياً.

[قراءة المصدر](#)

لنكمل الحوار

ما المهمة التي يمكن لمؤسستك تفويضها بأمان، وما الأدلة التي تبرر هذا القرار؟ استكشف مع سُحب تجربة محدودة النطاق للذكاء الاصطناعي الوكيل.

رُوجعت المصادر في سبتمبر 2026. تتطلب التصاميم التقنية التحقق داخل البيئة المستهدفة. وتعرض الصور مشاهد مؤسسية توضيحية.