



AMG

AIR-GAP MAIL GATEWAY



جهاز 2U يُركب في الحامل

تدفق البريد والطابور: قواعد ترحيل لا لبس فيه

أين تدخل كل رسالة، وأين تنتظر، ومتى تُسَلَّم، وماذا يحدث إن لم تُسَلَّم؛ كل ذلك بقاعدة صريحة لا بالتخمين.

لمن: مسؤولو البريد الإلكتروني

في هذا الكتالوج: القواعد التسع الثابتة، ودورة حياة الرسالة، والديمومة، والطابور، والإعدادات، وما يحدث عند الفشل

<https://www.bardin.tech/ar/bardingate-amg/>

AMG مُرَحِّل شفاف، والشفافية تعني ألا يتوقف أي قرار على المحتوى أو الأسماء. فالاتجاه والوجهة والمصير تتبع قواعد بسيطة قليلة، يمكن اختبار كل منها.



تسع قواعد ثابتة

- 1 خادم MTA واحد بالضبط يُضبط في كل شبكة.
- 2 عنوانا IP مختلفان. لا يمكن أن تتشارك الجهة الآمنة وغير الآمنة عنوانًا واحدًا.
- 3 يتصل كلاهما مباشرة. NAT وموازنات الحمل ووكلاء SMTP وترويسات المصدر المُمرَّر خارج هذا الإصدار.
- 4 لا يرسل البريد إلا هذان العنوانان. ولا يكون AMG مُرَحِّلًا مفتوحًا أبدًا.
- 5 المستلم والمرسل والنطاق والترويسات والنص لا تحدد الاتجاه أبدًا. فالاتجاه يأتي فقط من عنوان IP للجهة المتصلة.
- 6 يبقى المغلف متعدد المستلمين كاملاً ويذهب إلى MTA المقابل؛ ولا يُقسَّم حسب نطاق المستلم.
- 7 لا يُعدَّل المحتوى. لا يُضاف إلا ترويسة التتبع القياسية Received.
- 8 الفشل الدائم ينشئ إشعار DSN قياسيًا يعود إلى MTA المصدر، لا إلى الوجهة التي فشلت.
- 9 لا يشغّل هذا الإصدار صناديق بريد ولا فحص محتوى ولا مسحًا ولا سياسة SPF/DKIM/DMARC ولا التحقق من المستلم.



🔒 الاتجاه هو عنوان IP، ولا شيء غيره

لا تستطيع رسالة بترويسات مزورة أو مستلم غريب أن تغيّر اتجاهها، لأن الاتجاه يُقرأ من عنوان الجهة المتصلة مباشرة عبر TCP، ولا يُسمح إلا بعنوانين.

📌 نقل ناجح، خطوة بخطوة

<p>١</p> <p>تتصل الجهة الأخرى</p> <p>يتصل MTA المصدر ويجتاز ملف الأمان لتلك الجهة: عنوان IP مسموح، و TLS، و mTLS أو AUTH إن ضُبطا.</p>	<p>٢</p> <p>استلام دائم</p> <p>يستلم Postfix معاملة SMTP كاملة في طاير دائم، ثم يردّ بـ ٢٥٠.</p>	<p>٣</p> <p>حفظ آمن</p> <p>تبقى الرسالة قابلة للاسترداد بعد إعادة التشغيل وبعد انقطاع مفاجئ للكهرباء.</p>
<p>٤</p> <p>محاولة عند الوجهة</p> <p>يرسل Postfix الرسالة نفسها إلى MTA المقابل على عنوان IP والمنفذ المضبوطين.</p>	<p>٥</p> <p>سُلمت</p> <p>عند نجاح التسليم تصبح الحالة «سُلمت» ويتبع المحتوى مدة الاحتفاظ المضبوطة.</p>	<p>٦</p> <p>سجل وحدث</p> <p>تُسجّل بيانات وصفية منقّحة وسجل تدقيق، ويذهب حدث منظّم إلى نظام SIEM لديك.</p>

🔄 دورة حياة الرسالة

قُبِلت ← في الطاير الدائم ← سُلمت

انتهت مدتها: DSN

فشلت: DSN

مؤجلة

التأجيل مؤقت ويحمل سببًا ثابتًا منقّحًا وموعد المحاولة التالية؛ أما الفشل وانتهاء المدة فنهائيان، ويُبلّغ المرسل في الحالتين.

الحالة	ما يحدث
قُبِلت	لا يُردّ بـ SMTP 250 إلا بعد أن يحفظ Postfix الرسالة حفظًا دائمًا وفق ملف ديمومة نظام الملفات المضبوط.
مؤجلة	إعادة محاولة محدودة ودائمة. «أعد المحاولة الآن» تطلب محاولة إضافية واحدة، لكنها لا تتجاوز أبدًا ضوابط التوجيه أو TLS أو القبول أو السعة أو التبديل.
سُلمت	يتبع المحتوى مدة الاحتفاظ المضبوطة؛ وتبقى البيانات الوصفية للطاير.
فشلت أو انتهت مدتها	إشعار DSN قياسي إلى MTA المصدر، مع تحذير قبل انتهاء المدة. ولا يُسمح بأي حذف صامت.

📁 الديمومة

- الرسالة المقبولة غير المسلّمة تصمد أمام إعادة تشغيل العملية أو الحاوية، وإعادة تشغيل المضيف، والانقطاع المفاجئ للكهرباء، وتعطل قرص مادي واحد؛ يوقّر ذلك التخزين الدائم و RAID الجهاز، مع التشفير.
- لحظة القبول هي لحظة الديمومة، فلا تُقبل رسالة ثم تضيع.

ضغط السعة والصيانة

- لا يُحذف الطابور غير المسلّم أبدًا لتخفيف الضغط. يُحذف أولاً المحتوى المسلّم المحتفظ به، الأقدم فالأحدث؛ وإن بقيت السعة المحمية غير كافية، يُرد على القبول الجديد بخطأ مؤقت 4xx فيعيد MTA المرسل المحاولة لاحقًا.
- الصيانة والتحديثات: يتوقف القبول الجديد مؤقتًا بـ 4xx، وتبلغ معاملات SMTP المفتوحة نقطة آمنة، ويُحفظ الطابور، ويُطبّق التحديث ويُتحقق من السلامة، ثم يستأنف العمل أو يعود إلى الإصدار السابق.

لماذا 4xx بدل الحذف

الخطأ المؤقت 4xx يطلب من MTA المرسل الاحتفاظ بالرسالة والمحاولة لاحقًا، فلا يكون الجهاز أبدًا موضع ضياع رسالة. ولو حُذف البريد لإفساح المجال لصار AMG هو نقطة الضياع.

الإعدادات والقيم الافتراضية

الإعداد	القيمة الافتراضية	ملاحظة
عمر الطابور	٥ أيام	قابل للتعديل ضمن حدود آمنة؛ مع تحذير قبل انتهاء المدة
حجم الرسالة	50 MiB	قابل للضبط
المحتوى المسلّم	يُحذف بعد التسليم	يمكن الاحتفاظ به لمدة تحت سقف تخزين صريح
البيانات الوصفية للطابور	سنة واحدة	قابل للضبط ضمن نطاقات آمنة
تدقيق الأمن	خمس سنوات	قابل للضبط ضمن نطاقات آمنة
إعادة المحاولة والتزامن	متحفظ	إعدادات منتقاة؛ ولا تُعرض مفاتيح Postfix الخام أبدًا

لا يوجد سقف مصطنع في الترخيص على الإنتاجية أو النطاقات أو المستلمين أو عدد الرسائل في الطابور؛ فالحدود تتبع العتاد والتخزين المعتمدين.



تطبيق إعداد: خطوة بخطوة وقابل للتراجع



التحضير < postfix check < تفعيل ذري < إعادة التحميل < بوابة السلامة < اعتماد أو تراجع

بعد أي تعطل في أي خطوة، تُعاد بناء الحالة من نسخة الإعدادات الفعّالة، وبصمة الملف المؤلّد، وملاحظة التشغيل والطابور. ملفات Postfix مشتقة، وليست المصدر أبدًا.

عند حدوث خطأ



الموقف	السلوك
جهة غير معروفة، أو العنوان نفسه مضبوط مرتين	مرفوض؛ لا يُقبل البريد ولا تُفعّل الإعدادات
هوية TLS غير صالحة أو سرّ مطلوب مفقود	لا اتصال؛ ولا رجوع إلى نمط أضعف
اتجاه ملتبس أو إعدادات مشوّهة	يُرفض قبل التطبيق
فشل Postfix أو بيئة التشغيل أو SIEM	لا يُعلن تسليم رسالة مقبولة لم تُسلّم أبدًا؛ وعطل SIEM لا يوقف SMTP أبدًا

ما الذي يُختبر ✓

- الاتجاهان مع مستلم واحد وعدة مستلمين، وإثبات أن تغيير المستلم أو النطاق أو الترويسات لا يغيّر الاتجاه أبدًا.
- لا استعلام DNS أثناء الترحيل؛ و TLS في أنماطه المطلوب والانتهازي والمُعطل، مع mTLS و AUTH اختياريين.
- انقطاع الكهرباء وإعادة التشغيل حول الرد ٢٥٠، وتفعيل الإعدادات، والتسليم، والتنظيف؛ وضغط القرص.
- لا محتوى ولا موضوع ولا سرّ في السجلات أو قاعدة البيانات أو التشخيص أو SIEM.

✦ كم من العمل يقع عليك؟

تُدخل عناوين IP والمنفذين، والشهادات إن أردتها، ثم تضغط «تطبيق». أما الباقي، أي الطابور وإعادة المحاولة وإشعارات DSN والأحداث، فيعمل وحده.

الرسالة المقبولة إما تُسلّم وإما تنتهي بطريقة قياسية ظاهرة؛ ولا نتيجة ثالثة.

كتالوجات أخرى لهذا المنتج

كتالوج ٤

التشغيل والتكامل

كتالوج ٣

الأمن والعزل

كتالوج ١

نظرة عامة على المنتج



للاستشارة وطلب عرض توضيحي ومعلومات الاتصال:

<https://www.bardin.tech/ar/bardingate-amg/>

قد تتغير المواصفات دون إشعار مسبق.