دليل مستخدم حصن

منصة أمن Active Directory، للإصدار 1.32 وما بعده: التثبيت، والفحص، وقراءة النتائج، والمراقبة، والتقارير.

English العربية

---

1. ماذا يفعل حصن

يقيّم حصن أمن Active Directory وخوادم Windows التابعة له، ويتابع كل ملاحظة حتى تُعالَج، ويراقب وحدات التحكم بالنطاق لاكتشاف الهجمات والتغييرات على أكثر الكائنات حساسية (الطبقة صفر). وهو خدمة Windows واحدة مع واجهة ويب.

- **للقراءة فقط.** لا يكتب حصن أبداً في Active Directory أو سياسات المجموعة أو الخوادم، ولا يثبّت شيئاً على وحدات التحكم بالنطاق. يُنشئ سكربتات الإصلاح والتراجع ليراجعها المسؤول وينفذها بنفسه.
- **دون اتصال بالإنترنت.** لا يحتاج إلى الإنترنت للتشغيل أو التفعيل. تصل التحديثات ملفاتٍ موقَّعة تنسخها إليه.
- **لا قيم تجزئة لكلمات المرور.** لا يقرأ حصن قيم التجزئة (hashes) ولا يخزّنها. يُشغَّل تدقيق كلمات المرور الاختياري منفصلاً، ولا يستورد حصن منه إلا أسماء الحسابات.
- **بالعربية والإنجليزية** في الواجهة والتقارير وهذا الدليل.

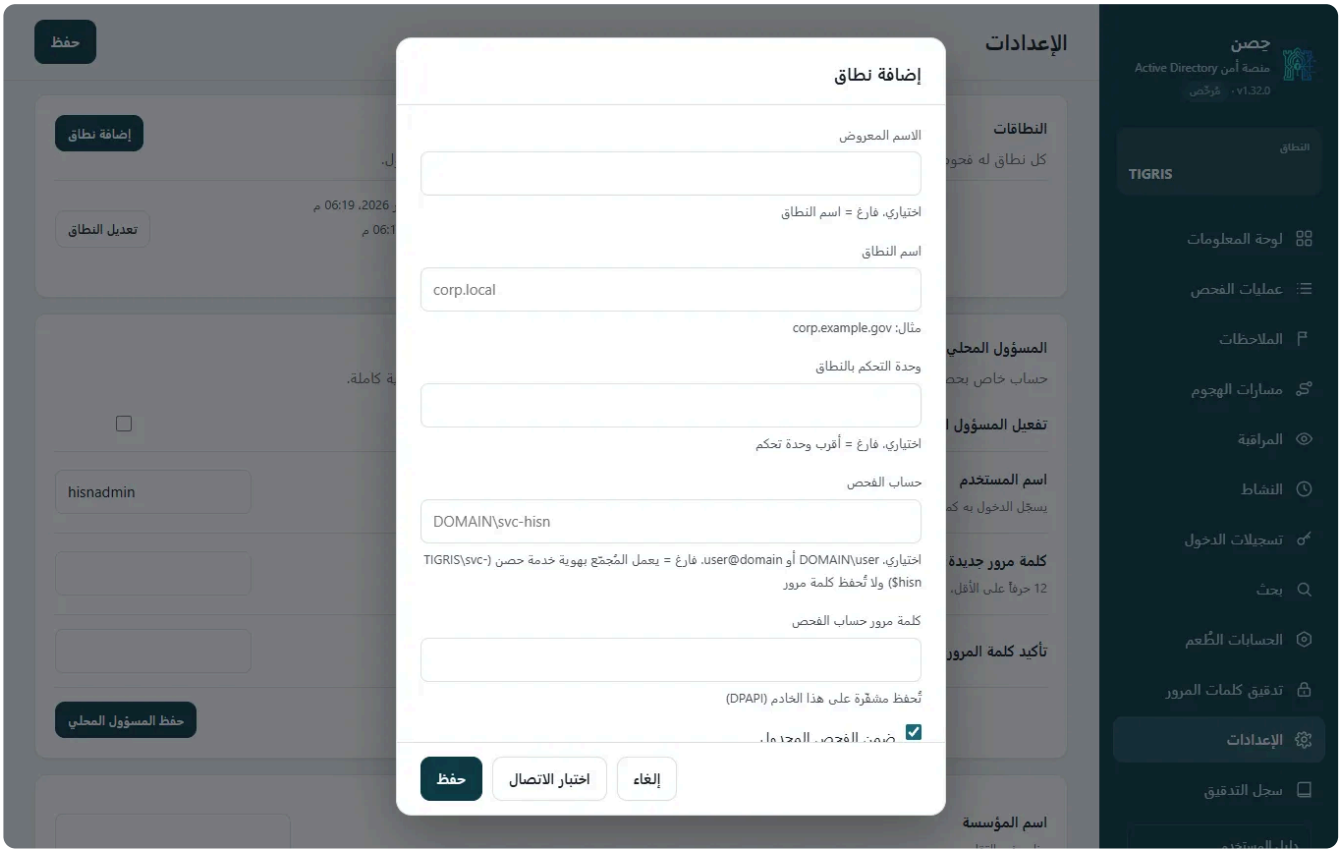
---

2. البدء السريع

من التثبيت إلى أول نتائج في خمس خطوات. كل خطوة تحيل إلى قسمها الكامل.

1. **ثبّت** `Hisn-Setup-v<version>.exe` على خادم منضم إلى النطاق، وأنهِ الإعداد مع تحديد خيار فتح واجهة حصن (القسم 4).
2. **سجّل الدخول** بحسابك في النطاق (عضو في **Hisn-Admins**) أو بالمسؤول المحلي المدمج الذي أنشأته أثناء الإعداد (القسم 5).

3. **تحقّق من النطاق** في *الإعدادات ← النطاقات*. يضيف الإعداد نطاق الخادم نفسه؛ افتحه بزر **تعديل النطاق** واضغط **اختبار الاتصال** (القسم 7).
4. **شغّل فحصاً**: *عمليات الفحص ← بدء فحص جديد*، أو زر الفحص في لوحة المعلومات. يستغرق النطاق المتوسط من دقيقة إلى 5 دقائق.
5. **اقرأ لوحة المعلومات**، ثم افتح *الملاحظات* وابدأ بالأعلى خطورة (القسم 8).



الخطوة 3: نموذج النطاق. الحقول الفارغة اختيارية، وزر **اختبار الاتصال** يتحقق مما سيحتاجه الفحص.

3. المتطلبات

البند	المتطلب
الخادم	Windows Server 2016 أو أحدث، منضم إلى النطاق. أبسط خيار هو وحدة تحكم بالنطاق؛ ويعمل أيضاً على خادم عضو مثبَّت عليه «Active Directory module for Windows PowerShell» من أدوات RSAT.
PowerShell	الإصدار 5.1 (مضمَّن في Windows Server 2016 وما بعده).
المتصفح	Microsoft Edge أو Chrome أو Firefox. **Internet Explorer** **غير مدعوم**، وهو المتصفح الوحيد على Server 2016/2019، لذا افتح الواجهة من جهازك أو ثبّت Edge أو Chrome على الخادم.
القرص	نحو 300 ميغابايت للبرنامج، ويزيد سجل الفحوص من 1 إلى 5 ميغابايت لكل فحص في نطاق متوسط. تُحفظ البيانات الخام للفحوص القديمة مضغوطة. لا يبدأ فحص ولا نسخ احتياطي إذا قلّت المساحة الحرة عن 2 غيغابايت (قابلة للتعديل في الإعدادات).
الذاكرة	يعمل جامع البيانات في PowerShell على خادم حصن ويحتاج نحو 1 غيغابايت حرة لدليل من 20,000 حساب (قياس فعلي، انظر أدناه)، وأكثر للأدلة الأكبر.
الشبكة من خادم حصن	إلى وحدات التحكم: LDAP 389، والكتالوج العمومي 3268، وخدمات ويب AD 9389، وSMB 445 (لـ SYSVOL)، وRPC 135 والمنافذ الديناميكية، وWinRM 5985. إلى الخوادم الأعضاء: WinRM 5985. إلى هيئات الشهادات: RPC وHTTP/HTTPS. إلى الواجهة من أجهزة المسؤولين: HTTPS 8443 (قابل للتغيير).

حجم الفحص المقيس

قيس على وحدة تحكم في بيئة اختبار (جهاز افتراضي، وحدة تحكم واحدة، وجامع البيانات يعمل عليها مباشرة)، بعد إضافة حسابات معطلة وأجهزة ومجموعات متداخلة اصطناعية. لم تُفحص خوادم أعضاء.

الدليل	مدة الجمع	أقصى ذاكرة للجامع	التحليل	حجم البيانات
20,017 مستخدماً / 5,001 جهاز / 557 مجموعة	6 دقائق	981 ميغابايت	5 ثوانٍ / 226 ميغابايت	62 ميغابايت

يضيف كل خادم عضو اتصال WinRM (حتى 300 خادم في الفحص الواحد)، وتطيل وحدات التحكم البعيدة عبر رابط بطيء مدة الجمع. تحمل الأدلة الحقيقية خصائص أكثر لكل حساب، فاعتبر هذه الأرقام حداً أدنى.

4. التثبيت والترقية

1. انسخ `Hisn-Setup-v<version>.exe` إلى الخادم وشغّله بصلاحيات المسؤول. طابِق قيمة SHA-256 للملف مع القيمة المنشورة مع التنزيل. إذا ظهرت نافذة SmartScreen فاختر *More info* ← *Run anyway*.
2. اختر اللغة واقبل الترخيص، ثم حدّد الخيارات: منفذ HTTPS (الافتراضي 8443)، ومن يمكنه فتح الواجهة (المسؤولون عبر الشبكة، أو هذا الخادم فقط).
3. أنشئ **المسؤول المحلي المدمج** (حساب خاص بحصن يُستخدم عند تعذّر الدخول بحساب النطاق)، وحدّد النطاق الأول.
4. أنهِ الإعداد مع تحديد خيار فتح واجهة حصن. قد يستغرق التشغيل الأول حتى دقيقتين لإنشاء شهادة HTTPS.

ينشئ الإعداد الخدمة `HisnConsole` (بحساب LocalSystem وتشغيل تلقائي)، ومجموعتي AD **Hisn-Admins** و**Hisn-Viewers** (ويضيفك إلى Hisn-Admins)، وقاعدة جدار حماية لمنفذ الواجهة، ومجلداً في قائمة ابدأ. يُثبَّت البرنامج في `C:\Program Files\Hisn`، ويرفض الإعداد أي مجلد خارج Program Files.

الترقية: شغّل الإعداد الجديد فوق التثبيت الحالي. يبقى السجل والإعدادات والنطاقات والترخيص وحالات الملاحظات كما هي. يأخذ الإعداد نسخة احتياطية من البيانات قبل أي تغيير، ويتوقف إذا فشلت، ويرفض تثبيت إصدار أقدم فوق إصدار أحدث. للتثبيت الصامت: `Hisn-Setup-v<version>.exe /S`.

5. تسجيل الدخول والصلاحيات

افتح `https://<server>:8443`. يحذّر المتصفح في المرة الأولى من الشهادة الموقَّعة ذاتياً؛ اختر *Advanced* ← *Continue*، أو ضع شهادتك في `C:\ProgramData\Hisn\tls`.



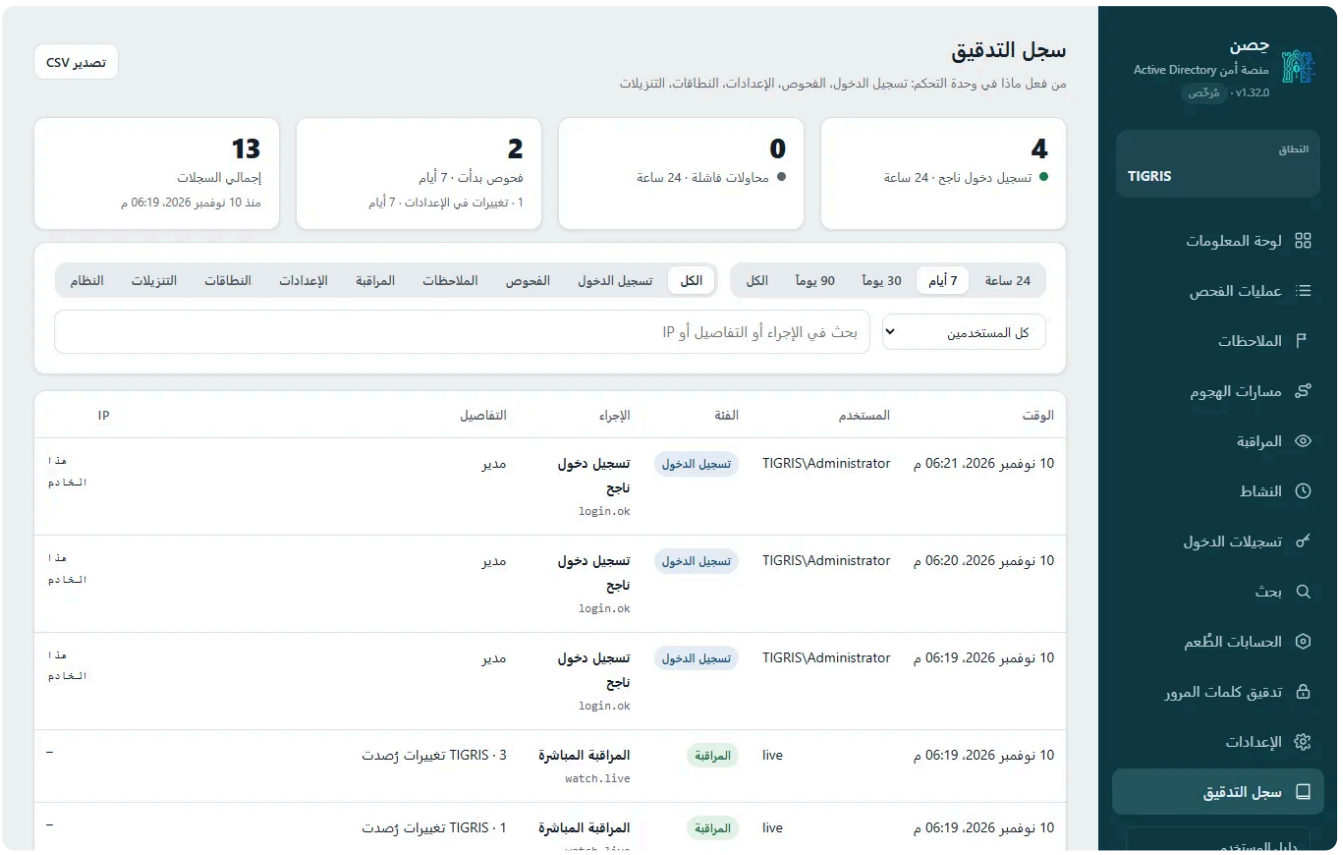
صفحة تسجيل الدخول. استخدم `DOMAIN\user` أو `user@domain`، أو اسم المسؤول المحلي المدمج. الرابط أسفل الزر يبدّل اللغة.

من	يستطيع
أعضاء **Hisn-Admins**	تشغيل الفحوص، وإدارة الملاحظات، وتنزيل سكربتات الإصلاح، وتغيير الإعدادات، واستيراد المحتوى والتراخيص.
أعضاء **Hisn-Viewers**	عرض لوحة المعلومات والملاحظات والمراقبة والنشاط والتقارير.
المسؤول المحلي المدمج	كل شيء؛ ويُقفل 15 دقيقة بعد 10 كلمات مرور خاطئة.

تنتهي الجلسة بعد 30 دقيقة دون نشاط أو بعد 12 ساعة. خمس كلمات مرور خاطئة من المستخدم والعنوان نفسيهما تقفل ذلك الدخول 15 دقيقة.

في أسفل الشريط الجانبي: زر **ع / EN** يبدّل اللغة، وزر المظهر يتنقل بين *تلقائي* (يتبع Windows) و*فاتح* و*داكن*، ويُحفظ الاختيار في هذا المتصفح. على الهاتف ينطوي الشريط الجانبي في زر القائمة أعلى الصفحة. كل الصفحات تعمل بلوحة المفاتيح: Tab للتنقل، وEnter أو المسافة لفتح صف، وEscape لإغلاق نافذة، ورابط «تخطَّ إلى المحتوى» هو أول محطة.

سجل التدقيق. يُسجَّل كل دخول وكل تغيير في الواجهة (الإعدادات، وحالات الملاحظات، والتصدير، والاستعادة) في صفحة *سجل التدقيق* مع المستخدم والعنوان. يمكن للمسؤولين تصفيته وتصديره بصيغة CSV.



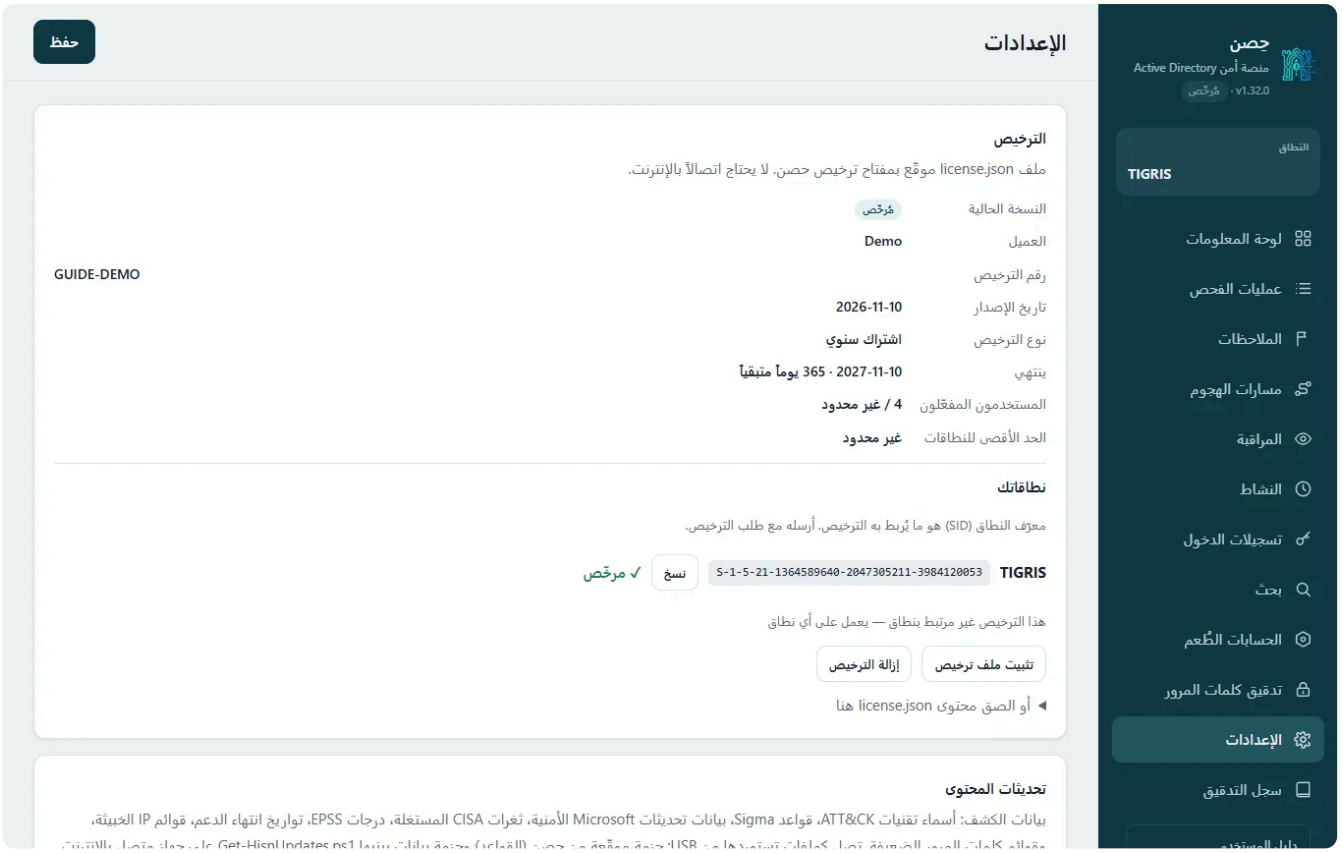
سجل التدقيق: من فعل ماذا داخل حصن نفسه.

---

6. الترخيص

بلا ترخيص يعمل حصن في **الوضع التجريبي**: فحص كامل واحد لنطاق واحد، مع كل نتائج ذلك الفحص وتقاريره. أما الميزات المستمرة (الجدولة، والسجل، وتعدد النطاقات، والمراقبة، والمراقبة المباشرة، والتنبيهات، والشعار، وتحديثات المحتوى، وSIEM) فتحتاج إلى ترخيص.

ثبّت ملف `license.json` الذي تستلمه من *الإعدادات ← الترخيص ← تثبيت ملف ترخيص*، أو الصق محتواه. تعرض البطاقة الإصدار ونوع الترخيص وتاريخ الانتهاء والمستخدمين المفعّلين والحد الأقصى للنطاقات. وتحت قائمة نطاقاتك يظهر معرّف كل نطاق (SID): أرسله مع طلب الترخيص، لأن الترخيص يُربط بمعرّفات النطاقات لا بالخادم.



الإعدادات ← الترخيص. انسخ معرّف النطاق لطلب الترخيص، وثبّت الملف الذي تستلمه بزر **تثبيت ملف ترخيص**.

النوع	السلوك
اشتراك	يعمل حتى تاريخ الانتهاء، ثم 14 يوماً إضافية مع تنبيه، ثم للقراءة فقط (تبقى النتائج السابقة متاحة للعرض).
دائم مع صيانة	لا ينتهي للإصدارات الصادرة قبل تاريخ الصيانة. الإصدارات الأحدث وحزم المحتوى الجديدة تحتاج إلى تجديد الصيانة.
تجريبي	14 يوماً بكل الميزات.

تُحسب فئات الحجم بعدد المستخدمين المفعّلين (S · 1,000 M · 5,000 L · 20,000 XL بلا حد). تجاوز الفئة يُظهر تنبيهاً ولا يمنع الفحص أبداً.

---

7. النطاقات وحسابات الفحص

أضف كل نطاق من *الإعدادات* ← *النطاقات* ← *إضافة نطاق* (الصورة في البدء السريع): اسم DNS، واختياراً وحدة تحكم مفضّلة، واختيارياً حساب فحص (`DOMAIN\user`؛ وتُخزَّن كلمة مروره مشفّرة بـ Windows DPAPI). اترك الحساب فارغاً ليفحص حصن بهوية خدمته؛ ويذكر النموذج الهوية التي تعمل بها الخدمة.

على وحدة تحكم تعمل الخدمة فيها بحساب LocalSystem، يصل الفحص إلى الأجهزة الأخرى بحساب جهاز وحدة التحكم (`DOMAIN\DC$`).

اضغط **اختبار الاتصال**. يتحقق من أربعة أمور ويشرح سبب أي فشل:

الاختبار	لازم لـ	الصلاحيات
قراءة الدليل (LDAP)	كل الفحوص تقريباً	أي مستخدم في النطاق
PowerShell عن بُعد (WinRM) إلى PDC	إعدادات وحدات التحكم: التوقيع، SMB، خدمة الطباعة، حماية LSA، سياسة التدقيق، جدار الحماية، التحديثات	Domain Admins (مسؤول على وحدات التحكم). مجموعة Remote Management Users وحدها تسمح بالاتصال دون قراءة هذه الإعدادات، فيعرضها حصن «غير مُقيَّمة»
سجل الأمان (Security)	«غيّره» في المراقبة، والمراقبة المباشرة، وتسجيلات الدخول، وقفل الحسابات	Event Log Readers على وحدات التحكم
SYSVOL	محتوى سياسات المجموعة وإعداداتها، والسكربتات، والأسرار في SYSVOL	أي مستخدم في النطاق

الخوادم الأعضاء (الفحوص من S-001 إلى S-015 وجلسات المسؤولين) تُقرأ عبر WinRM، وتحتاج إلى أن يكون حساب الفحص (أو حساب جهاز وحدة التحكم عند عدم تحديد حساب) في مجموعة Administrators المحلية على كل خادم. تُقرأ حتى 300 خادم في الفحص الواحد.

لنطاق في غابة أخرى استخدم حساباً من ذلك النطاق، ويجب أن تسمح علاقة الثقة بذلك.

تشغيل الخدمة بحساب gMSA (مستحسن)

تعمل خدمة حصن افتراضياً بحساب LocalSystem. هذا يعمل، لكنه على وحدة التحكم يفحص بحساب جهاز وحدة التحكم نفسها، وحساب الفحص المكتوب في الإعدادات يعني كلمة مرور مخزّنة على الخادم. أما **حساب الخدمة المُدار للمجموعات** (gMSA) فيتجنب الأمرين: ينشئ Windows كلمة مروره ويغيّرها دورياً، ولا يستطيع استخدامه إلا خادم حصن، ولا يخزّن حصن شيئاً.

نفّذ ما يلي على وحدة تحكم بصلاحية Domain Admin (حصن لا ينفذها بنفسه أبداً). استبدل `HISNSERVER` باسم الخادم المثبَّت عليه حصن؛ ويكتب الإعداد هذه الأوامر بأسمائك في `C:\ProgramData\Hisn\Create-Hisn-gMSA.txt` .

```
# 1. once per forest - skip if Get-KdsRootKey already returns a key
Add-KdsRootKey -EffectiveImmediately          # then wait 10 hours for it to rep
# (single-DC lab only:  Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))

# 2. the account - only the Hisn server may fetch its password
New-ADServiceAccount -Name svc-hisn -DNSHostName svc-hisn.corp.example `
    -PrincipalsAllowedToRetrieveManagedPassword 'HISNSERVER$'

# 3. the read rights from the table above
Add-ADGroupMember 'Event Log Readers'       -Members 'svc-hisn$'
Add-ADGroupMember 'Remote Management Users' -Members 'svc-hisn$'
```

ثم على خادم حصن، بصلاحيات المسؤول:

```
Install-ADServiceAccount svc-hisn
Test-ADServiceAccount svc-hisn      # must print True
```

شغّل الإعداد مرة أخرى (يحتفظ ببياناتك) وأدخل `CORP\svc-hisn$` في خيار التشغيل بحساب gMSA، أو نفّذ `Install-HisnConsole.ps1 -ServiceAccount CORP\svc-hisn$` . يتحقق الإعداد من الحساب بـ `Test-ADServiceAccount` ، ويمنحه الصلاحيات على `C:\ProgramData\Hisn` ، ويعيد تشغيل الخدمة. في *الإعدادات ← النطاقات* اترك حساب الفحص فارغاً لكل نطاق يستطيع حساب gMSA قراءته.

- **النطاقات والغابات الأخرى.** العضوية في المجموعات خاصة بكل نطاق: أضف `svc-hisn$` إلى Event Log Readers وRemote Management Users في كل نطاق فرعي أو غابة موثوقة، أو احتفظ بحساب فحص لذلك النطاق.
- **فحوص الخوادم الأعضاء** ما زالت تحتاج إلى الحساب في مجموعة Administrators المحلية على كل خادم، كأي حساب فحص.
- **إعدادات وحدات التحكم** (التوقيع، SMB، خدمة الطباعة، حماية LSA، سياسة التدقيق، التحديثات، dcdiag) تحتاج مسؤولاً على وحدات التحكم. في مجموعة Remote Management Users يستطيع حساب gMSA الاتصال دون قراءتها، فتظهر هذه الفحوص «غير مُقيَّمة»: عيّن حساب فحص من Domain Admins لهذا النطاق (صفحة النطاقات) لتقييمها.
- **الانتقال إلى خادم جديد** يعني إضافة الخادم الجديد إلى `PrincipalsAllowedToRetrieveManagedPassword` (`Set-ADServiceAccount svc-hisn -PrincipalsAllowedToRetrieveManagedPassword 'NEWSERVER$'`). والنسخة الاحتياطية المستعادة هناك لا تحتاج إلى إعادة إدخال أي كلمة مرور.

8. لوحة المعلومات

تعرض لوحة المعلومات حالة النطاق بنظرة واحدة. النطاق المعروض هو المختار في المربع أعلى الشريط الجانبي.



النصف العلوي من لوحة المعلومات.

1. **الدرجة والتقدير** (من 0 إلى 100، ومن A إلى F)، والتغيّر منذ الفحص السابق، وتطور الدرجة عبر آخر الفحوص.
2. **آخر فحص والفحص القادم**، وعدد فحوص هذا النطاق.
3. **أعداد النطاق**: المستخدمون والأجهزة المفعّلة، ووحدات التحكم، وحسابات الطبقة صفر، وسياسات المجموعة، وعلاقات الثقة، وهيئات إصدار الشهادات.
4. **الملاحظات المفتوحة** حسب الخطورة، وعدد الفحوص الناجحة والفاشلة وغير المُقيَّمة في آخر فحص.
5. **تقدّم المعالجة**: الملاحظات المفتوحة، والعائدة للظهور، والمُقرّ بها، والمؤجّلة، وتحت استثناء مخاطرة، والمُصلحة؛ وكم منها له مسؤول أو تجاوز موعده.
6. **المراقبة**: التغييرات التي تنتظر المراجعة، الأحدث أولاً.



النصف السفلي: أهم الملاحظات، ومسارات الهجوم، وتغطية الأطر، والمراقبة المباشرة.

وفي الأسفل: **أهم الملاحظات** (ومنها يُفتح التقرير)، وملخص **مسارات الهجوم**، و**تغطية الأطر** لكل معيار (انقر أياً منها لفتح صفحة الامتثال للمعايير)، وحالة **المراقبة المباشرة** مع الفاصل الزمني والتغييرات المرصودة وعدد المصادر المقروءة دون خطأ.

---

9. عمليات الفحص والملاحظات

شغّل فحصاً من *عمليات الفحص* ← *بدء فحص جديد* أو من لوحة المعلومات، أو جدوله من *الإعدادات* ← *الفحص المجدول* (يومي أو أسبوعي؛ الافتراضي يوم الأحد الساعة 02:00). يستغرق النطاق المتوسط من دقيقة إلى 5 دقائق، و20,000 حساب نحو 6 دقائق (انظر حجم الفحص المقيس).



عمليات الفحص: كل فحوص النطاق المختار. انقر أياً منها لعرض تفاصيله.

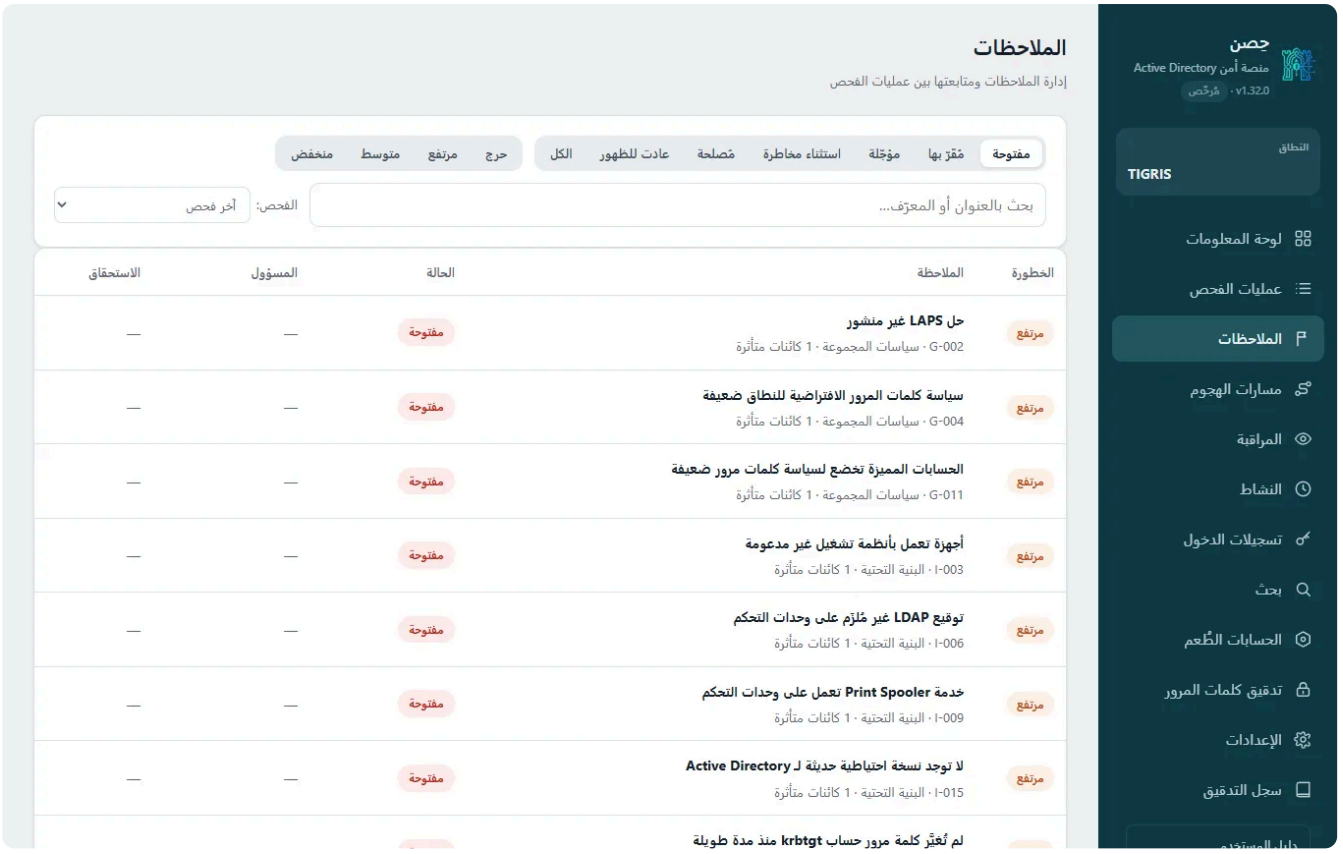
تعرض صفحة الفحص حالته ودرجته وعدد الملاحظات حسب الخطورة، و**التنزيلات** (التقرير، والملاحظات بصيغة JSON أو Excel، وسكربتا الإصلاح والتراجع لكل الملاحظات)، وسجل الفحص. زر **إنشاء تقرير...** يفتح منشئ التقارير (القسم 11).



تفاصيل الفحص مع التنزيلات والسجل.

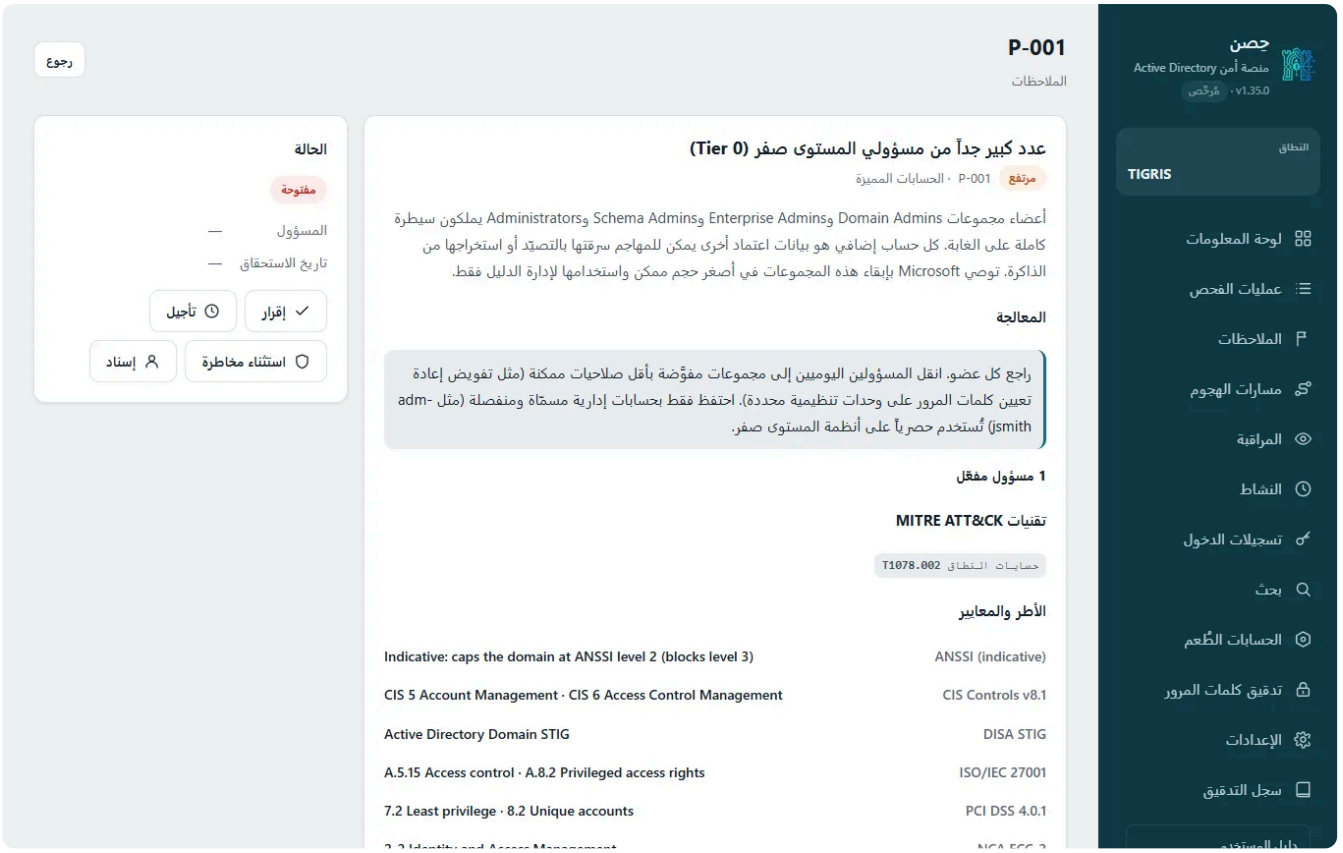
الملاحظات

تعرض صفحة *الملاحظات* ما فشل، مع تصفية حسب الحالة (مفتوحة، مُقَرّ بها، مؤجّلة، استثناء مخاطرة، مُصلحة، عادت للظهور) والخطورة، وبحث بالعنوان أو رقم الفحص. تحتفظ كل ملاحظة بحالتها بين الفحوص: عندما لا يجد الفحص التالي المشكلة تصبح *مُصلحة*، وإن عادت تُعلَّم *عادت للظهور*.



الملاحظات، مصفّاة لإظهار المفتوحة.

تُفتح الملاحظة بشرح وطريقة المعالجة والكائنات المتأثرة وتقنيات MITRE ATT&CK والضوابط المرتبطة بها في كل إطار. وفي الجانب: **إقرار**، و**تأجيل** (حتى 90 يوماً)، و**استثناء مخاطرة** (حتى سنة، مع سبب)، و**إسناد** إلى مسؤول مع موعد. يُحفظ كل إجراء في سجل الملاحظة.



ملاحظة واحدة: معناها، وطريقة إصلاحها، وارتباطها بالأطر.

وفي الأسفل **سكربت الإصلاح** و**سكربت التراجع** لتلك الملاحظة. اقرأهما، وشغّل الإصلاح مع `-WhatIf` أولاً، واحتفظ بسكربت التراجع. حصن لا يشغّلهما بنفسه أبداً.



سكربتا الإصلاح والتراجع، مع تعليقات تشرح الإصلاح الصحيح.

- **الدرجة.** يُوزَن كل مجال حسب الخطورة (حرج 10، مرتفع 5، متوسط 3، منخفض 1). أي ملاحظة حرجة مفتوحة تُبقي الدرجة عند 59 (التقدير F)، لأن مساراً حرجاً واحداً يكفي للسيطرة على النطاق.
- **لم يُقيَّم** تعني أن البيانات تعذّرت قراءتها (مثلاً فشل WinRM إلى وحدة تحكم). تذكر الملاحظة تحت الفحص السبب، ولا تُحسب ناجحة أبداً.

---

10. مسارات الهجوم

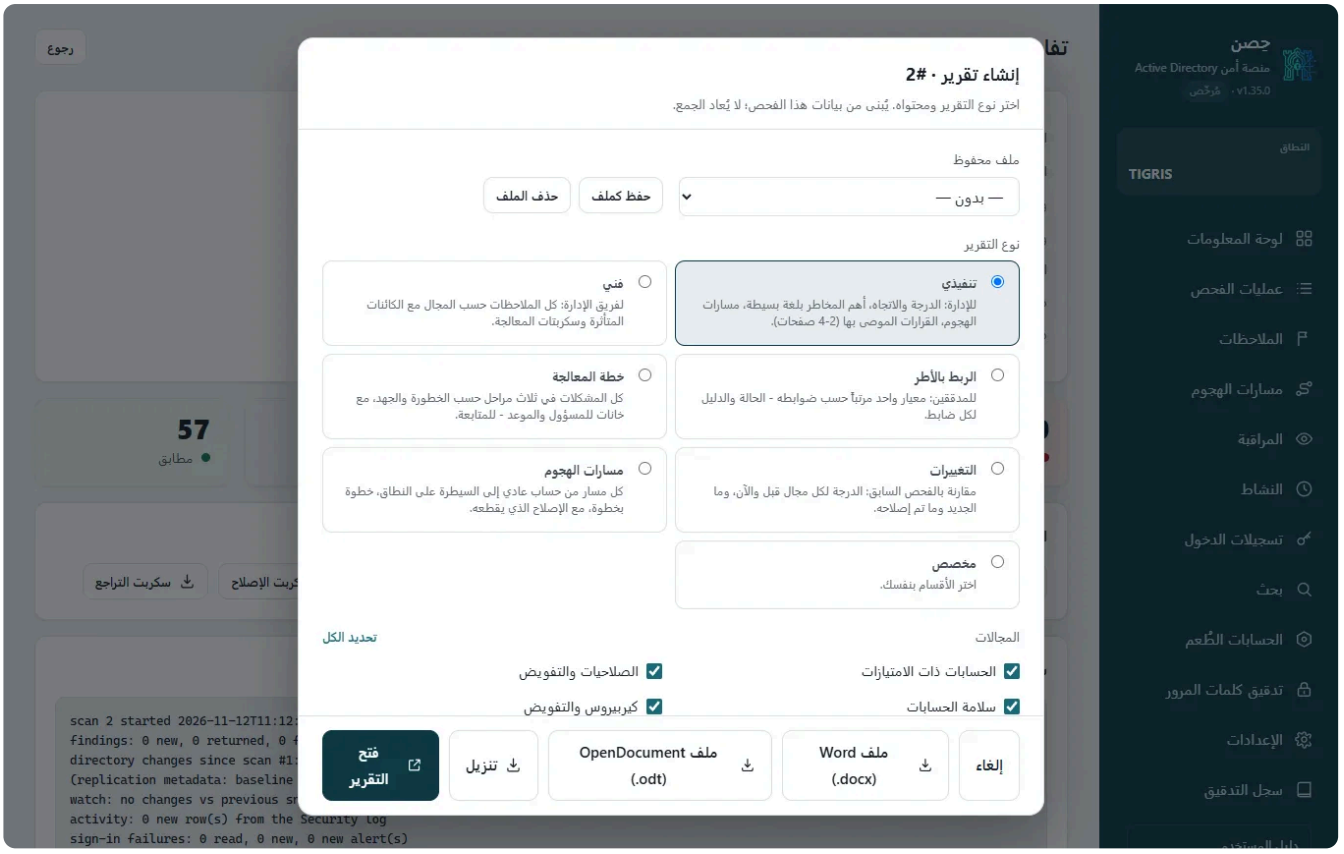
بعد كل فحص يربط حصن الصلاحيات وعضويات المجموعات والتفويض وحقوق المسؤول والجلسات وقوالب الشهادات في رسم بياني، ويعرض كل سلسلة من حساب عادي إلى السيطرة الكاملة على النطاق (الطبقة صفر). يذكر كل مسار التغيير الواحد الذي يقطعه (*اقطع هنا*) مع أمر PowerShell لتنفيذه، ويعرض أعلى الصفحة التغيير الواحد الذي يغلق أكبر عدد من المسارات (*أفضل خطوة واحدة*).

تعرض البطاقات عدد المستخدمين العاديين الذين لديهم مسار، وعدد المسارات المختلفة، وأقصر مسار بالخطوات، وأفضل خطوة واحدة. النتيجة المطلوبة بعد فحص كامل هي «لا توجد مسارات هجوم». وتنبّه الصفحة عندما تكون بيانات الصلاحيات في الفحص ناقصة؛ عندها أعد الفحص بالإصدار الحالي قبل الاعتماد على النتيجة.

---

11. التقارير

افتح فحصاً وانقر **إنشاء تقرير...**. كل تقرير ملف HTML واحد يُطبع بصيغة PDF بحجم A4، بالعربية أو الإنجليزية، مع رقم تقرير وبصمة SHA-256 للتحقق من أي نسخة مقابل الواجهة. تُبنى التقارير من بيانات الفحص، ولا يُجمع شيء من جديد.



منشئ التقارير: اختر النوع والمجالات والخيارات، ثم نزّل التقرير أو افتحه.

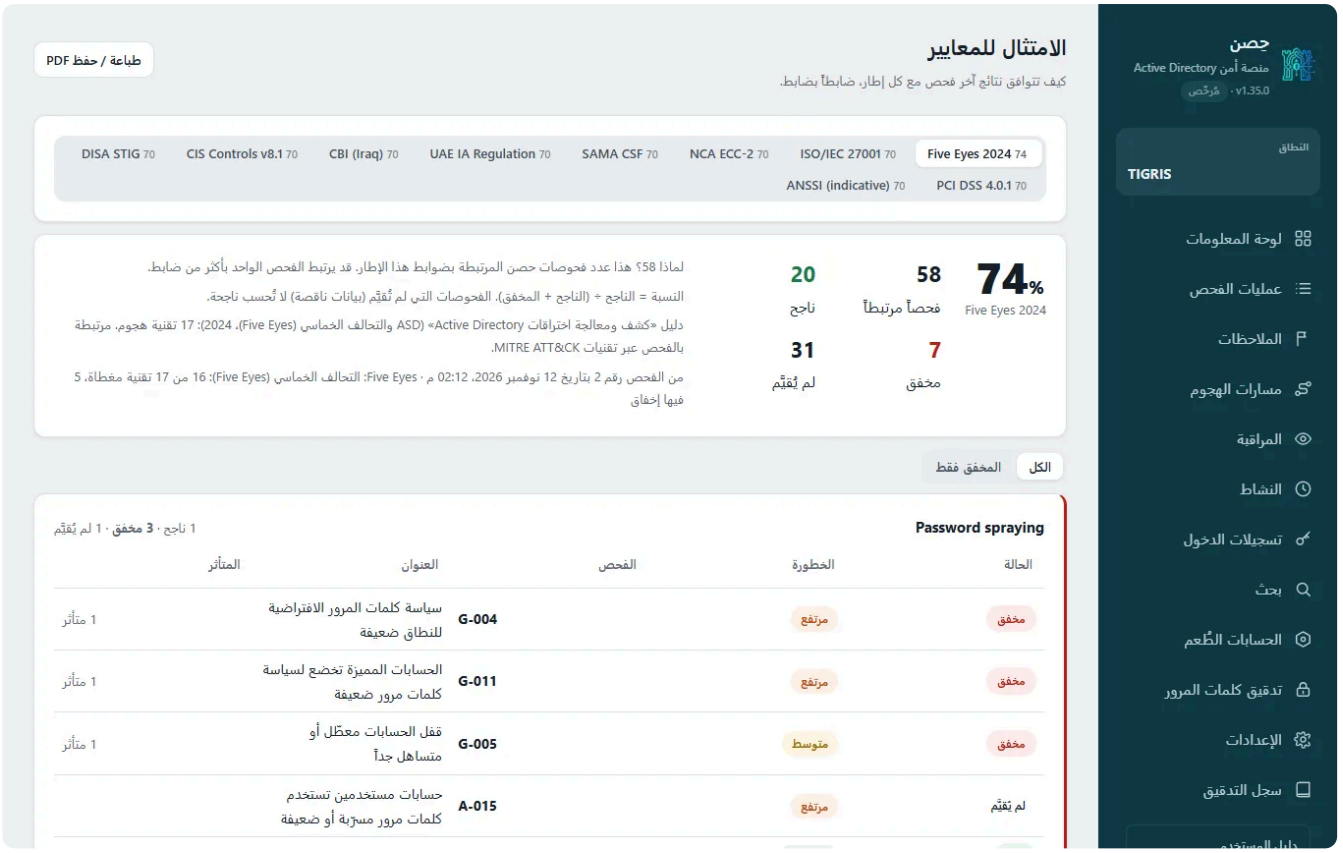
النوع	لمن	المحتوى
تنفيذي	الإدارة	الدرجة واتجاهها، وأهم المخاطر بلغة بسيطة، ومسارات الهجوم، والقرارات الموصى بها (من 2 إلى 4 صفحات)
فني	فريق الإدارة التقنية	كل الملاحظات حسب المجال، والكائنات المتأثرة، وسكربتات الإصلاح، وتغطية ATT&CK
الربط بالأطر	المدققون	إطار واحد (ISO/IEC 27001، NCA ECC)، إطار SAMA للأمن السيبراني، لائحة ضمان المعلومات الإماراتية، ضوابط الصمود السيبراني للبنك المركزي العراقي، ANSSI، DISA STIG، PCI DSS 4.0.1، CIS Controls v8.1، التحالف الخماسي) مرتباً حسب ضوابطه، مع الحالة والدليل
خطة المعالجة	متابعة المشروع	كل المشكلات في ثلاث مراحل حسب الخطورة والجهد، مع خانات للمسؤول والموعد والإنجاز
التغييرات	مراجعات التقدم	درجة كل مجال قبل والآن، وما الجديد وما أُصلح
مسارات الهجوم	فريق الأمن	كل مسار خطوة بخطوة، مع الإصلاح الذي يقطعه
مخصص	أي جهة	أي من الأقسام الـ 21

الخيارات: المجالات، ومستويات الخطورة، واللغة، والتصنيف (بدون، للاستخدام الداخلي، سري، سري للغاية)، وسكربتات الإصلاح (للمسؤولين فقط)، والفحوص الناجحة، والمظهر (**Ishtar** ملوّن، و**Formal** هادئ). احفظ مجموعة الخيارات **ملفاً محفوظاً** يمكن إرساله بالبريد بعد كل فحص مجدول. ضع شعار مؤسستك في *الإعدادات ← شعار المؤسسة*.

---

12. الامتثال للمعايير

افتح صفحة *الامتثال للمعايير* من بطاقة تغطية الأطر في لوحة المعلومات. تعرض كيف يرتبط آخر فحص بكل إطار، ضابطاً بضابط. حصن **يربط** فحوصه بالأطر، ولا يمنح شهادة امتثال.



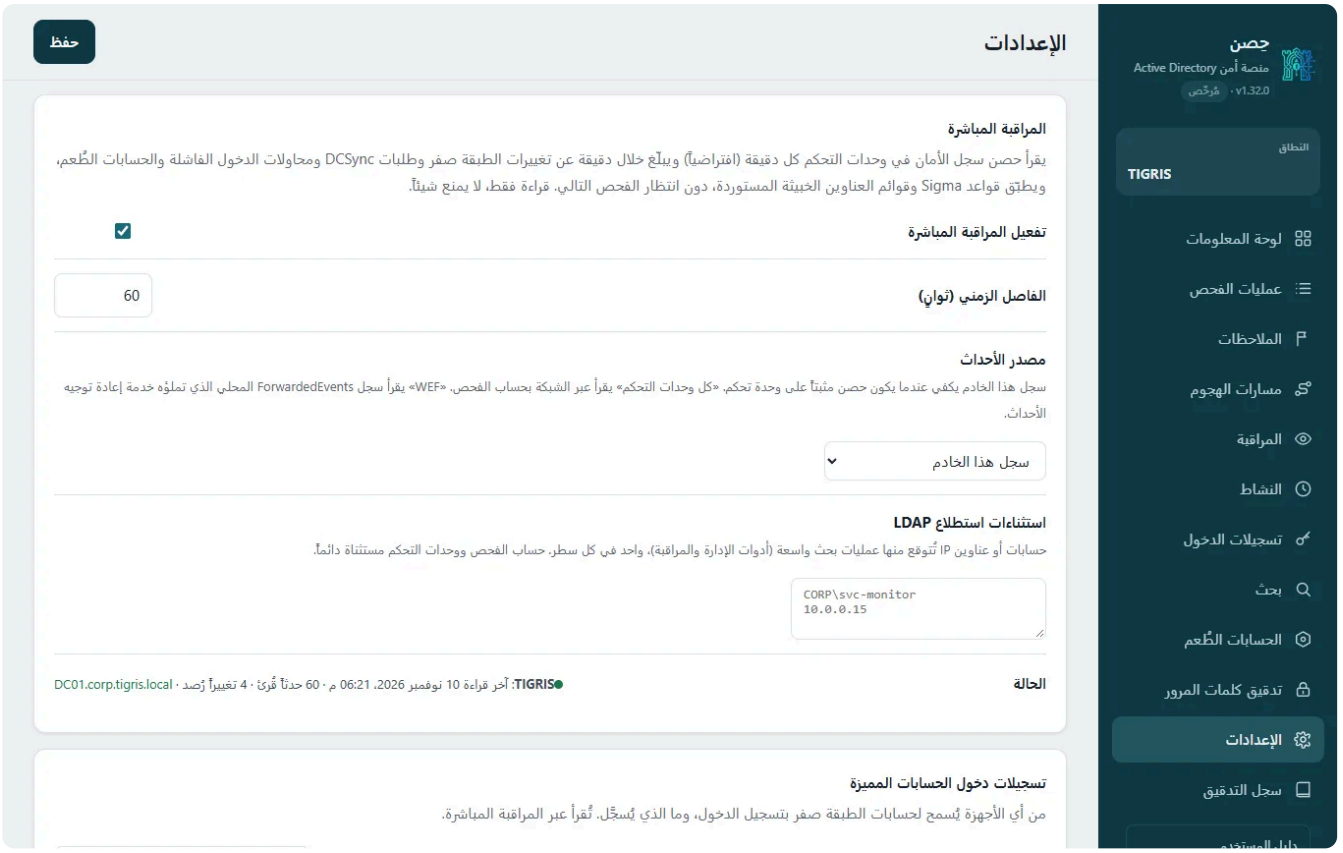
الامتثال لإطار واحد، مع الفحوص تحت كل ضابط.

- تبدّل التبويبات في الأعلى الإطار. النسبة هي *الناجح ÷ (الناجح + الفاشل)*؛ والفحوص التي تعذّر تشغيلها تظهر *لم يُقيَّم* ولا تُحسب ناجحة أبداً.
- قد يرتبط الفحص الواحد بأكثر من ضابط. خيار *المخفق فقط* يخفي الناجح. زر **طباعة / حفظ PDF** يطبع الصفحة.
- ANSSI موسوم بأنه *إرشادي*: مستوياته تقديرية من فحوص حصن.

---

13. المراقبة المباشرة والمراقبة والنشاط

تقرأ **المراقبة المباشرة** سجلات الأمان في وحدات التحكم كل 15 إلى 900 ثانية (الافتراضي 60) وتبلّغ خلال دقيقة تقريباً عن: تغييرات الطبقة صفر، وDCSync، وKerberoasting وAS-REP roasting، واستطلاع LDAP، ورش كلمات المرور، والتخمين المتكرر، وموجات قفل الحسابات، وتعداد المستخدمين، واستخدام الحسابات الطُعم، ودخول حسابات الطبقة صفر من أجهزة خارجها، وتطابقات قواعد Sigma، والدخول من عناوين مدرجة في قوائم التهديدات المستوردة. تُقرأ عدة نطاقات في الوقت نفسه، وأي نافذة زمنية تعذّرت قراءتها تُعاد قراءتها لاحقاً. فعّلها من *الإعدادات ← المراقبة المباشرة*.

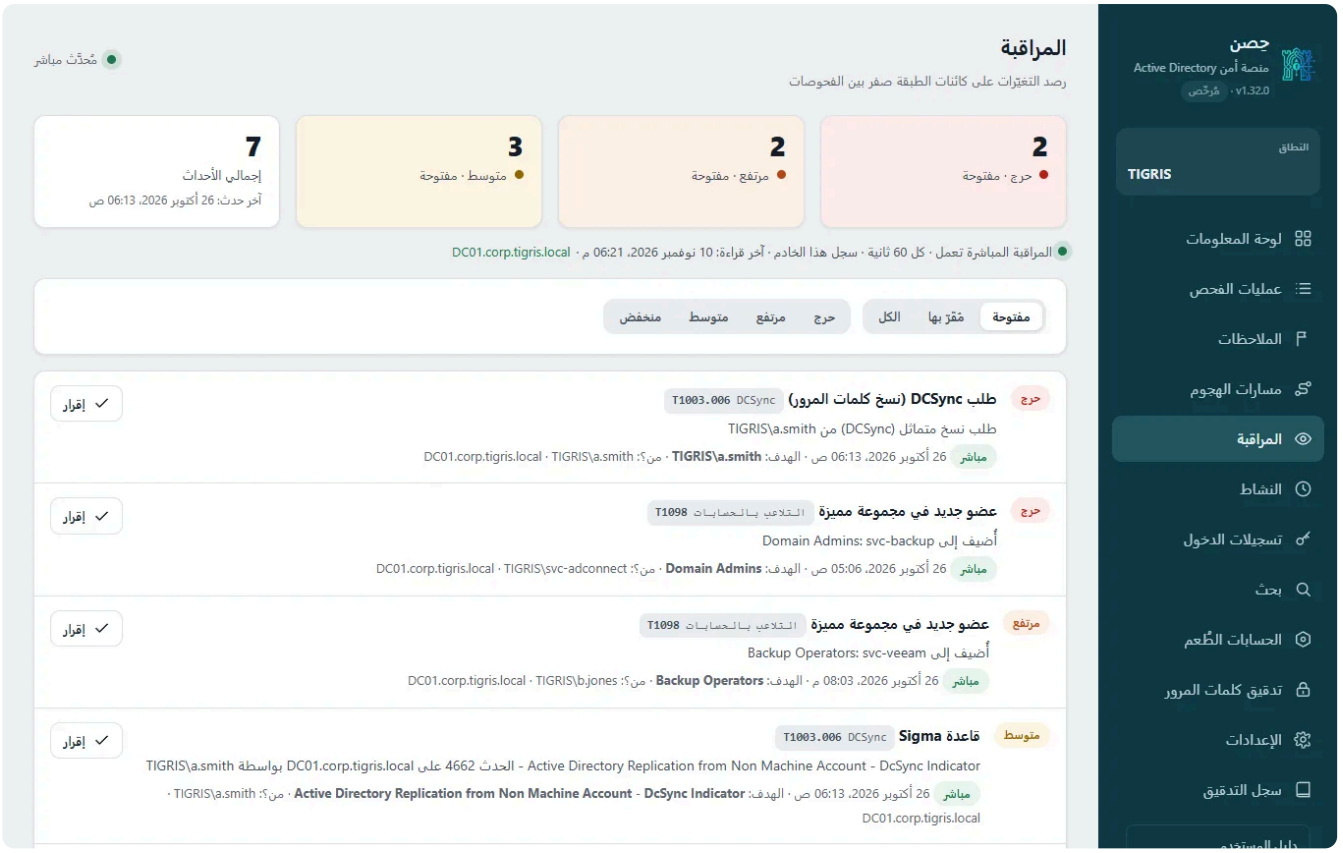


الإعدادات ← المراقبة المباشرة، مع سطر الحالة في الأسفل.

مصدر الأحداث: سجل هذا الخادم (عندما يعمل حصن على وحدة تحكم)، أو كل وحدات التحكم عبر الشبكة، أو سجل ForwardedEvents عندما يرسل Windows Event Forwarding سجلات وحدات التحكم إلى هذا الخادم.

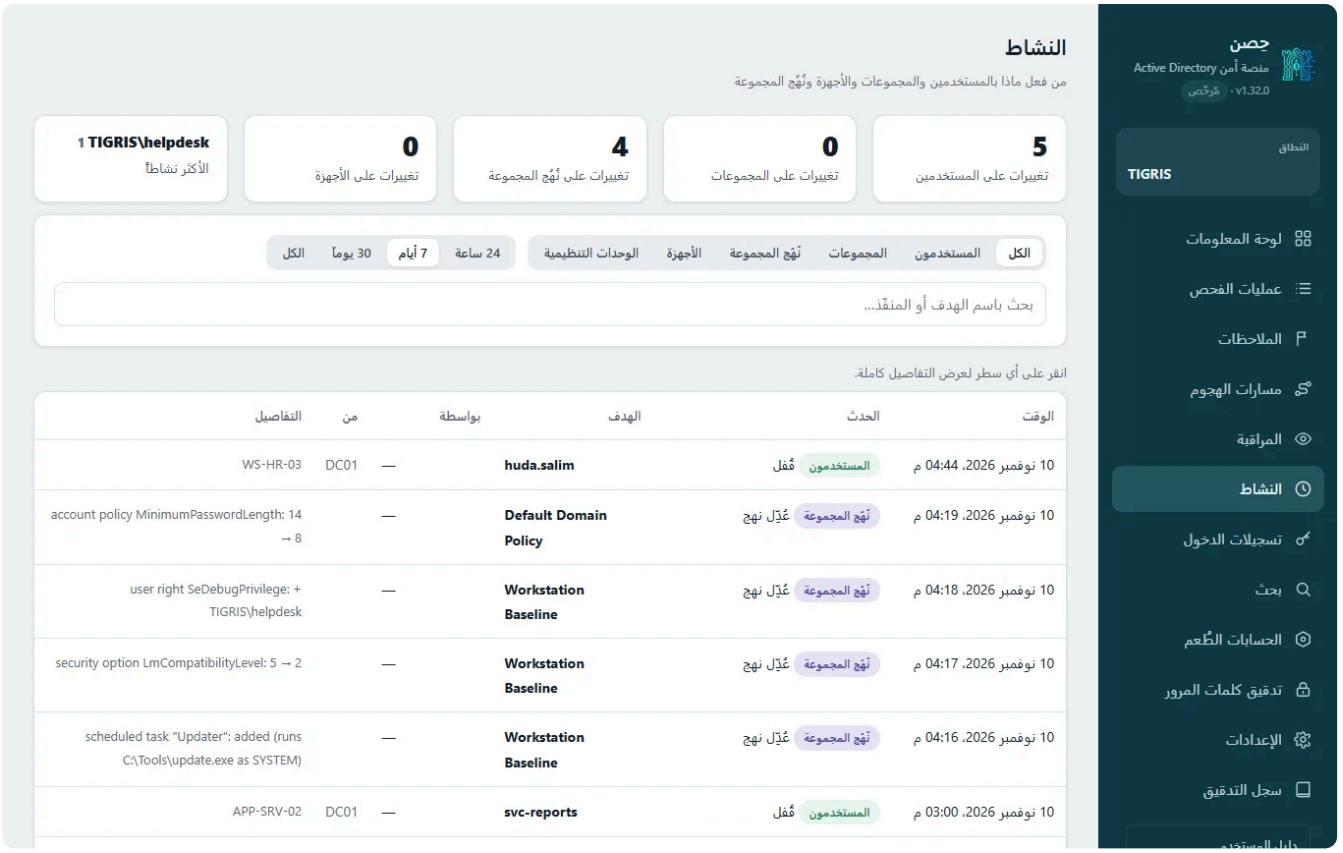
> **سياسة التدقيق المطلوبة على وحدات التحكم** (Default Domain Controllers Policy ← Advanced Audit Policy Configuration، نجاح وفشل): Kerberos Authentication Service، وKerberos Service Ticket Operations، وCredential Validation، وLogon، وUser Account Management، وSecurity Group Management، وComputer Account Management، وDirectory Service Changes، وDirectory Service Access. يخبرك الفحص M-001 بما ينقص منها.

تعرض صفحة **المراقبة** كل تغيير وتنبيه، من المراقبة المباشرة ومن مقارنة كل فحص بسابقه: المجموعات المميزة، وAdminSDHolder، وصلاحيات جذر النطاق، وسياسات وحدات التحكم، وقوالب الشهادات، وعلاقات الثقة، وkrbtgt، ووحدات التحكم، وأدوار FSMO. لكل بند خطورته وتقنية MITRE ATT&CK والهدف والفاعل ووحدة التحكم. والتغيير الذي يجده الفحص دون حدث مطابق في سجل الأمان يُعلَّم *تغييراً صامتاً* (حدث والتدقيق متوقف، أو مُسح السجل). راجع البند ثم اضغط **إقرار**.



المراقبة: التنبيهات وتغييرات الطبقة صفر التي تنتظر المراجعة.

صفحة **النشاط** تجيب عن «من فعل ماذا»: تغييرات المستخدمين والمجموعات والأجهزة وسياسات المجموعة والوحدات التنظيمية من سجل الأمان ومن مقارنة الفحوص، مع الفاعل ووحدة التحكم. وفي سياسات المجموعة تذكر أي إعداد تغيّر (القسم 14). صفّ حسب النوع والوقت، وابحث بالهدف أو الفاعل، وانقر أي صف لعرض التفاصيل كاملة.



النشاط، ومنه تغييرات إعدادات سياسات المجموعة.

---

14. تسجيلات الدخول وقفل الحسابات والبحث

تحت قائمة *تسجيلات الدخول* ثلاثة تبويبات: **الدخول الفاشل**، و**دخول الحسابات المميزة**، و**قفل الحسابات**. كلها تقرأ ما سجّلته المراقبة المباشرة والفحوص، ولا يتغير شيء في Active Directory.

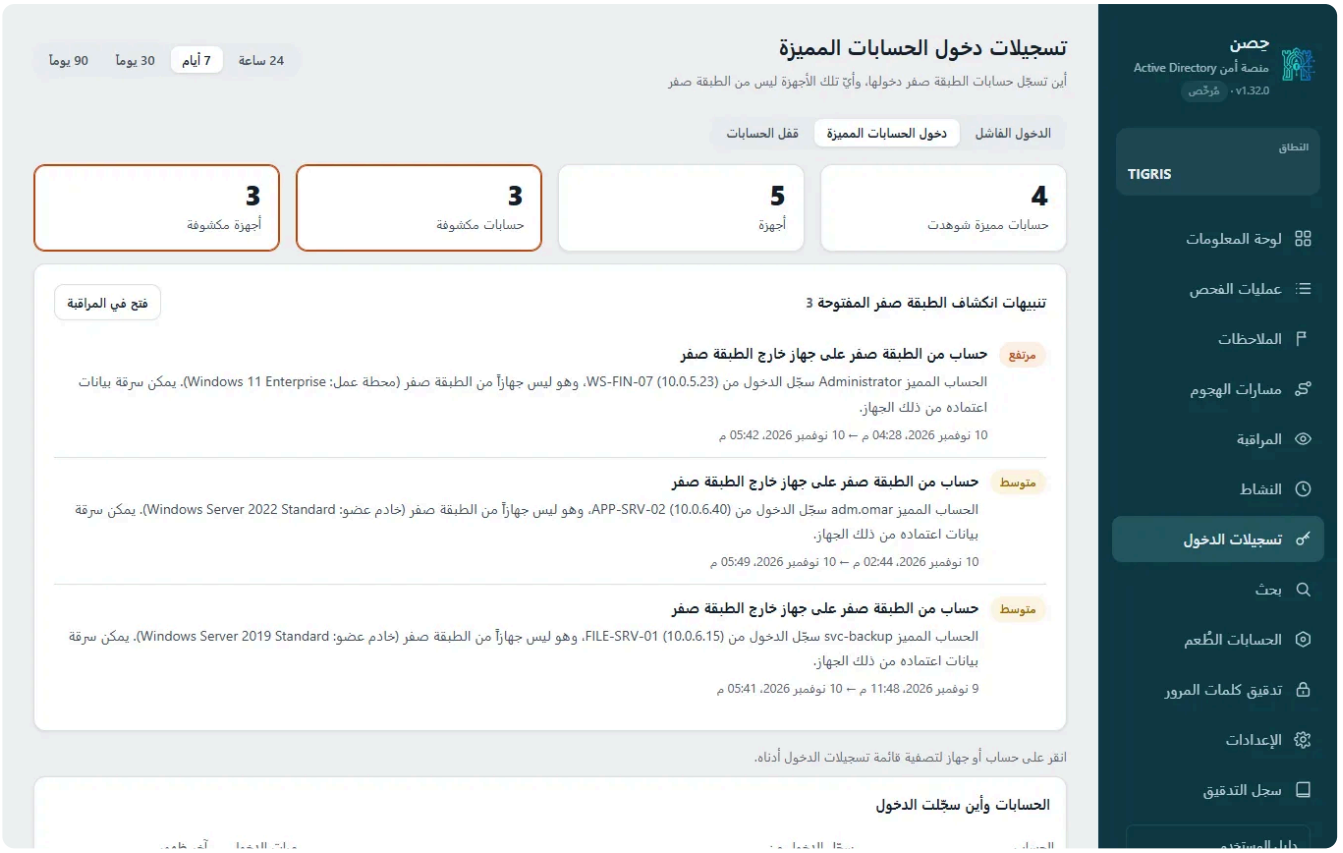
يعرض تبويب **الدخول الفاشل** كلمات المرور الخاطئة وأسماء الحسابات غير الموجودة حسب الحساب وحسب المصدر، خلال 24 ساعة أو 7 أيام أو 30 يوماً، والتنبيهات الناتجة عنها (رش كلمات المرور، وتعداد المستخدمين، والتخمين المتكرر، والفشل على الحسابات المميزة، وموجات القفل).



الدخول الفاشل عبر الزمن، حسب الحساب وحسب المصدر.

دخول الحسابات المميزة

يترك الحساب المميز قيمة تجزئة كلمة مروره أو تذكرة Kerberos الخاصة به على كل جهاز يسجّل الدخول إليه، ومن يسيطر على ذلك الجهاز يستطيع أخذها. عندما تكون المراقبة المباشرة مفعّلة، يسجّل حصن عمليات الدخول الناجحة لحسابات الطبقة صفر (طلبات تذاكر Kerberos، الحدث 4768، والدخول على وحدة تحكم، الحدث 4624)، ويعرض أي حساب دخل من أي جهاز.



دخول الحسابات المميزة: ثلاثة حسابات من الطبقة صفر استُخدمت على أجهزة خارجها.

- **الطبقة صفر** (وحدة تحكم بالنطاق) و**مسموح** (جهاز في قائمة الأجهزة المسموحة) لا إشكال فيهما.
- **محطة عمل** و**خادم عضو** و**جهاز غير معروف**: بيانات اعتماد الحساب مكشوفة هناك. يُصدر حصن تنبيه دخول حساب من الطبقة صفر على جهاز من خارجها، بخطورة مرتفعة لمحطة العمل ومتوسطة لغيرها، مرة واحدة لكل حساب وجهاز في الأسبوع.
- تحت التنبيهات، اختر حساباً أو جهازاً لتصفية قائمة عمليات الدخول.

ما العمل: أدِر النطاق من محطات إدارة مخصصة أو خوادم قفز فقط، وأدرجها في *الإعدادات ← تسجيلات دخول الحسابات المميزة ← الأجهزة المسموحة*، سطراً لكل إدخال: اسم (`PAW-01`)، أو نمط (`PAW-*`)، أو عنوان، أو نطاق عناوين (`10.0.7.0/24`). يرفض حصن أي إدخال لا يستطيع استخدامه ويُظهر رسالة. ويُبلَّغ أيضاً عن حساب خدمة عضو في مجموعة من الطبقة صفر يعمل على خادم عضو؛ وهذا انكشاف حقيقي، فأخرجه من المجموعة بدلاً من السماح للخادم.



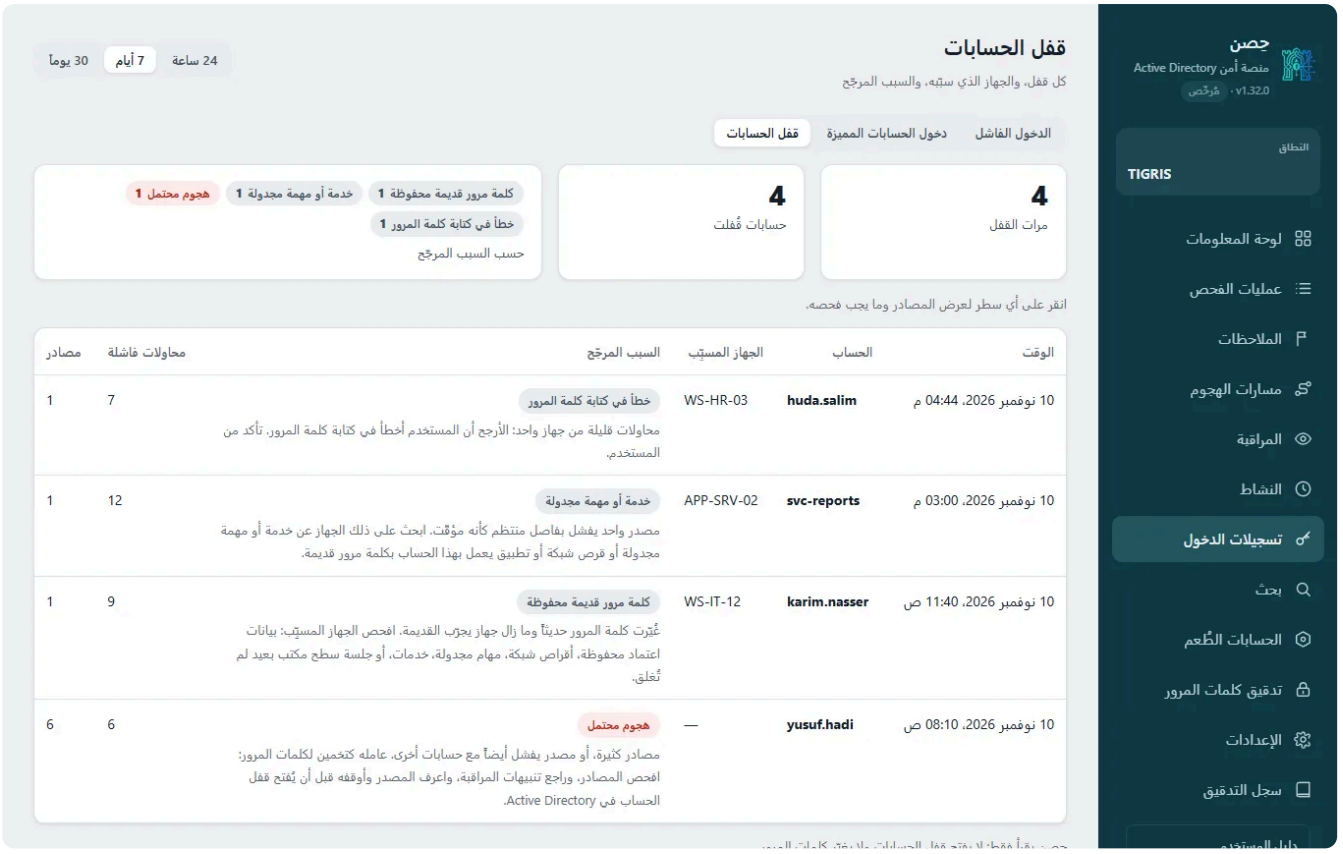
الإعدادات ← تسجيلات دخول الحسابات المميزة.

تأتي أسماء الأجهزة من الحدث نفسه أو من بحث DNS عكسي يجريه خادم حصن داخل شبكتك، ويمكن إيقاف هذا البحث. افتراضياً تُسجَّل الحسابات المميزة فقط، وتُحفظ عمليات الدخول 90 يوماً. تسجيل *كل المستخدمين* يحفظ طلبات التذاكر لكل مستخدم أيضاً؛ وفي نطاق كبير يعني ذلك صفوفاً كثيرة، فاختره فقط إن احتجت إلى سجل دخول للجميع.

> **سياسة التدقيق المطلوبة على وحدات التحكم:** Kerberos Authentication Service (نجاح) وLogon (نجاح). كلاهما مفعّل افتراضياً على وحدات التحكم.

قفل الحسابات

يظهر كل قفل حساب مع الجهاز الذي سبّبه (الجهاز المسيّب في الحدث 4740)، ومحاولات الدخول الفاشلة في الساعة التي سبقته، والسبب المرجّح. انقر أي صف لعرض المصادر وما يجب فحصه.



قفل الحسابات، ولكل قفل سببه المرجّح ومعناه.



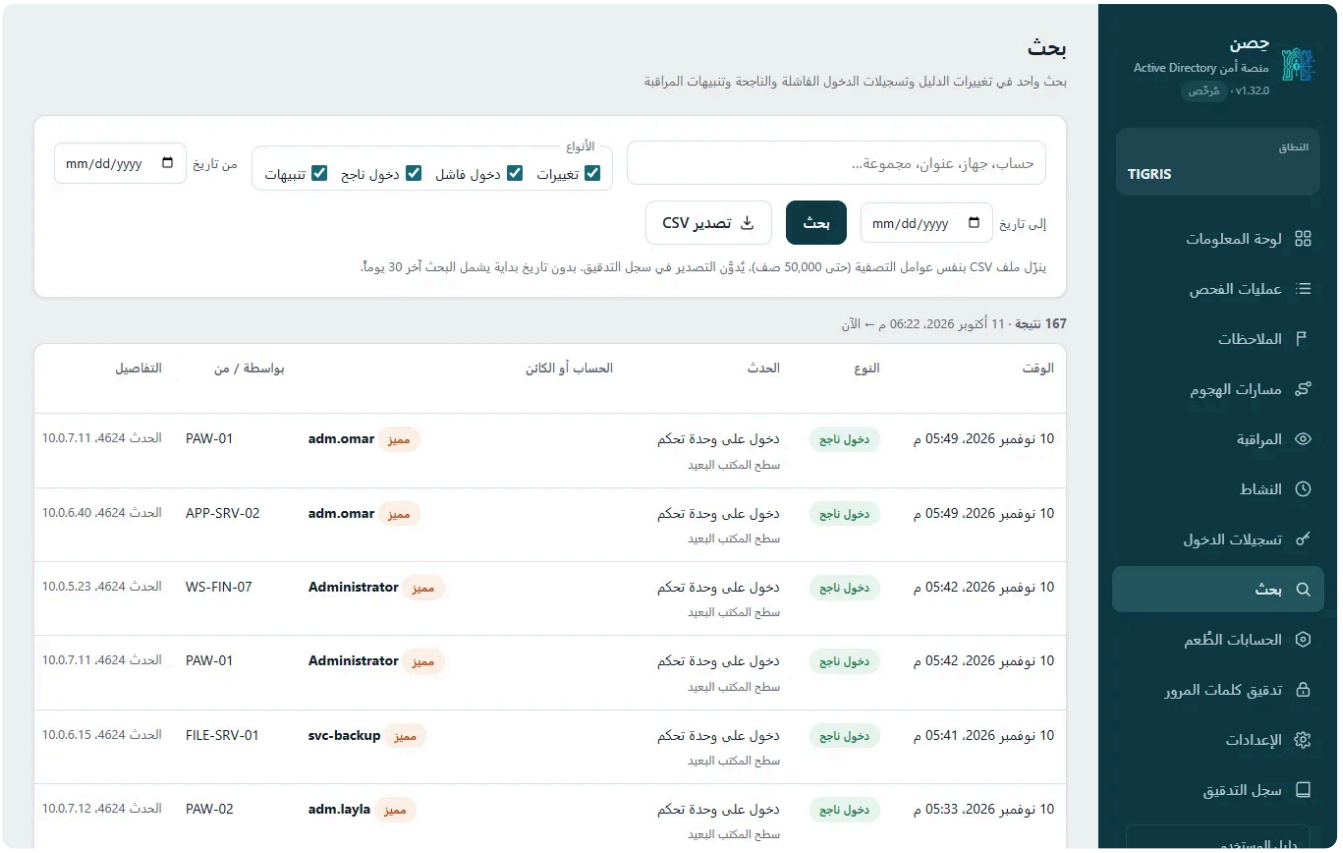
قفل مفتوح: جاءت المحاولات بفاصل منتظم، فالسبب المرجّح خدمة أو مهمة مجدولة.

السبب المرجّح	ماذا يعني	ما يجب فحصه
كلمة مرور قديمة محفوظة	غُيّرت كلمة المرور خلال آخر 7 أيام، وجهاز أو جهازان ما زالا يجرّبان القديمة	بيانات الاعتماد المحفوظة، والأقراص المعيَّنة، وملفات البريد على الأجهزة المذكورة
خدمة أو مهمة مجدولة	مصدر واحد يفشل بفاصل منتظم	الخدمات والمهام المجدولة ومجمّعات التطبيقات التي تعمل بذلك الحساب على المصدر
هاتف أو جهاز آخر	محاولات NTLM متكررة من جهاز واحد مسمّى	هاتف المستخدم أو برنامج بريده أو ملف شبكة Wi-Fi لديه
هجوم محتمل	مصادر كثيرة، أو مصدر يفشل أيضاً مع حسابات أخرى	تبويب الدخول الفاشل وتنبيهات المراقبة في الوقت نفسه
خطأ في كتابة كلمة المرور	محاولات قليلة من جهاز واحد	التأكد مع المستخدم
السبب غير معروف	لم تُسجَّل أي محاولة فاشلة قبل القفل	سياسة التدقيق على وحدات التحكم (الفحص M-001)

لا يفتح حصن قفل الحسابات. السبب تقدير مبني على الأحداث المسجّلة، وليس حكماً نهائياً.

البحث

تبحث صفحة *بحث* في كل ما سجّله حصن للنطاق في قائمة واحدة: تغييرات الدليل (النشاط)، والدخول الفاشل، والدخول الناجح، وتنبيهات المراقبة. صفِّ بالنص (حساب أو جهاز أو عنوان أو مجموعة) والنوع والتاريخ؛ ودون تاريخ بداية يُبحث في آخر 30 يوماً. زر **تصدير CSV** ينزّل النتيجة بعوامل التصفية نفسها (حتى 50,000 صف) لتسليمها للمدقق، ويُسجَّل التصدير نفسه في سجل التدقيق. تذكر الصفحة مدة حفظ كل نوع، ويمكن تغييرها من *الإعدادات*.



البحث في التغييرات والدخول الفاشل والناجح والتنبيهات.

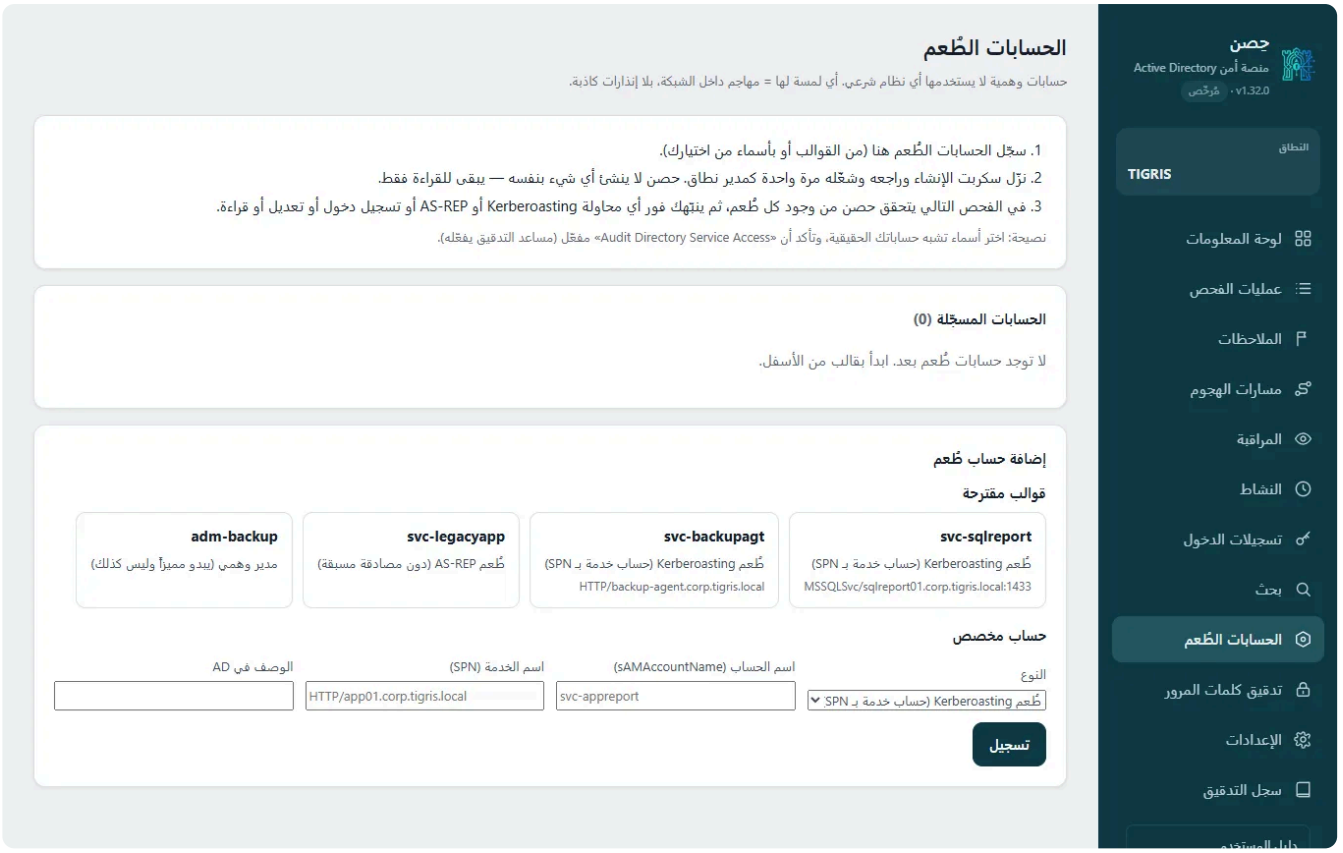
أي إعداد تغيّر في سياسة المجموعة

ابتداءً من جامع البيانات 1.3.0، تعرض صفحة *النشاط* أي إعداد تغيّر داخل سياسة مجموعة بين فحصين، مع القيمة القديمة والجديدة: حقوق المستخدمين، وخيارات الأمان، وسياسات كلمة المرور والقفل وKerberos، وإعدادات السجل (Registry)، والمجموعات المقيّدة، والمهام المجدولة، والسكربتات (انظر صورة النشاط في القسم 13). يسجّل الفحص الأول بعد الترقية نقطة البداية، وتظهر التفاصيل من الفحص الثاني. هويات خدمات Windows ومجمّعات تطبيقات IIS في حقوق المستخدمين تُوسَم بنوعها، لأن أسماءها لا يمكن استرجاعها من معرّفاتها. ولا تُجمع أبداً قيم كلمات المرور المخزّنة في سياسات المجموعة.

---

15. الحسابات الطُعم

الحسابات الطُعم حسابات لا يستخدمها أي شيء مشروع، فأي اقتراب منها يعني أن أحداً داخل الشبكة يبحث عن طريق للاختراق. يقترح حصن حسابات طُعم تجذب الهجمات الشائعة (حساب خدمة له SPN لاصطياد Kerberoasting، وحساب دون مصادقة Kerberos المسبقة لاصطياد AS-REP roasting، ومسؤول وهمي)، أو يأخذ أسماء تختارها.



الحسابات الطُّعم: سجّلها، وأنشئها بالسكربت، ويتحقق منها الفحص التالي.

1. سجّل الحسابات الطُّعم في هذه الصفحة (من القوالب، أو بأسماء تختارها تشبه حساباتك الحقيقية).
2. نزّل سكربت الإنشاء وراجعه، ثم شغّله مرة واحدة بصلاحية مسؤول النطاق. حصن لا ينشئ شيئاً بنفسه أبداً.
3. يتحقق الفحص التالي من وجود كل حساب. ومن بعدها ينبّه حصن إلى أي Kerberoasting أو طلب AS-REP أو دخول أو تغيير أو قراءة لأي حساب طُعم. قراءة الحسابات تحتاج إلى تفعيل *Audit Directory Service Access* على وحدات التحكم.

---

16. مستشعر استطلاع LDAP

لرصد التعداد على طريقة BloodHound، يجب أن تسجّل كل وحدة تحكم عمليات البحث في LDAP (الحدث 1644). شغّل السكربت مرة واحدة على كل وحدة تحكم من المجلد `C:\Program Files\Hisn\collector` (وانسخه إلى وحدات التحكم التي لا يعمل عليها حصن):

```
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1 -WhatIf   #
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1           #
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1 -Status   #
```

يحفظ السكربت القيم السابقة، ويعيدها الخيار `-Disable`. يمكن إدراج الحسابات والعناوين التي تستعرض AD لغرض مشروع (أدوات الجرد، وحصن نفسه) في *الإعدادات ← المراقبة المباشرة ← استثناءات استطلاع LDAP*.

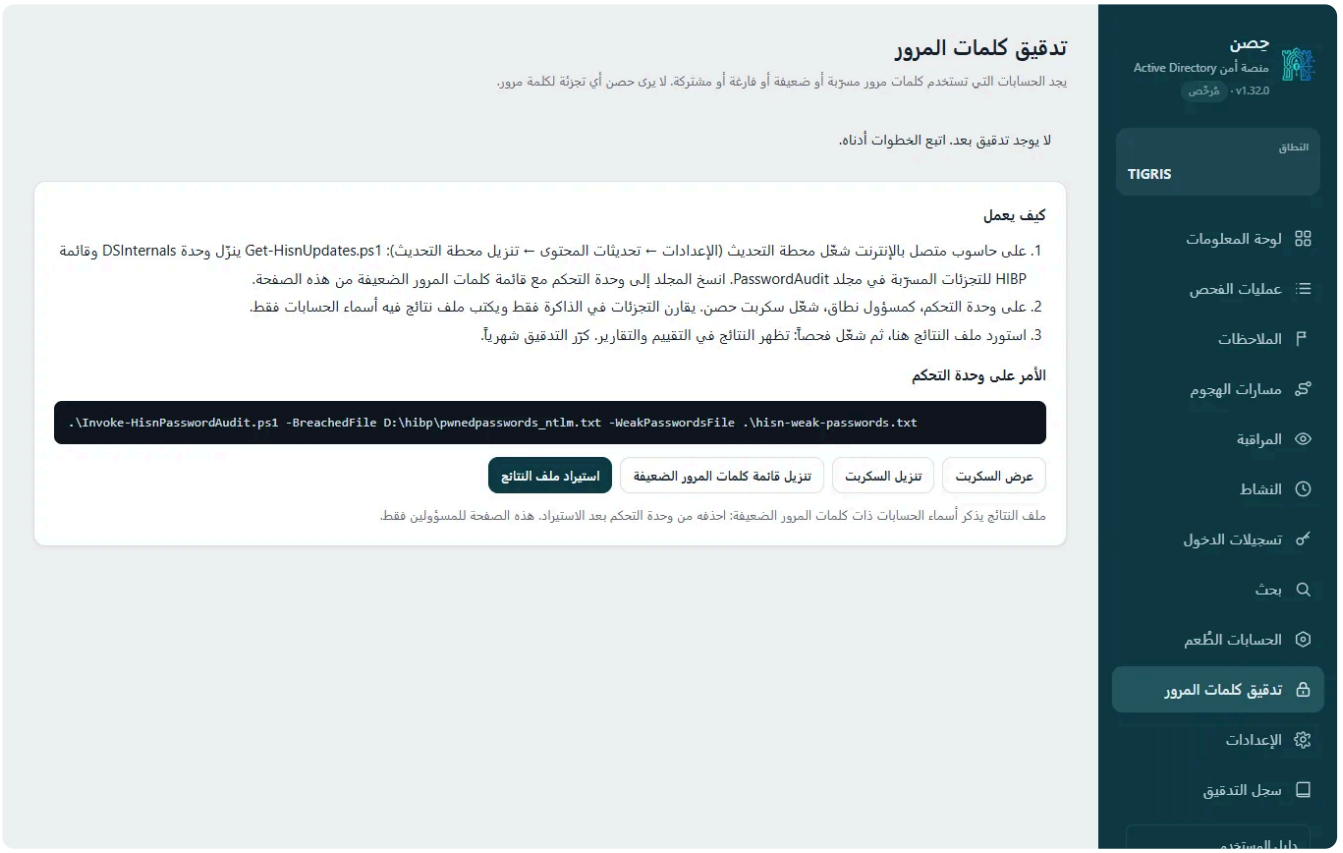
---

17. تدقيق كلمات المرور

يكشف كلمات المرور المسرّبة والضعيفة والفارغة والمشتركة والمخزّنة بصيغة LM (الفحوص من A-014 إلى A-018). شغّله بنفسك بصلاحية Domain Admin على وحدة تحكم؛ يستخدم وحدة DSInternals المجانية ويُبقي قيم التجزئة في الذاكرة فقط.

```
Install-Module DSInternals
.\Invoke-HisnPasswordAudit.ps1 -BreachedFile D:\hibp\pwnedpasswords_ntlm.txt -We
```

استورد ملف `.json` الناتج في صفحة *تدقيق كلمات المرور*. يحتوي أسماء الحسابات فقط، وتستخدمه الفحوص 90 يوماً. وتتيح الصفحة أيضاً تنزيل السكربت وقائمة كلمات المرور الضعيفة.



تدقيق كلمات المرور: شغّله على وحدة تحكم، ثم استورد النتيجة هنا.

18. تحديثات المحتوى (دون اتصال)

تصل قواعد الكشف ومعلومات التهديدات (تحديثات أمان Microsoft حسب الإصدار، وCISA KEV، وEPSS، وتواريخ انتهاء دعم Windows، وقواعد Sigma، وقوائم العناوين الخبيثة، وقوائم كلمات المرور الضعيفة) في حزم موقَّعة بامتداد `.hcb`. استوردها من *الإعدادات ← تحديثات المحتوى*؛ ويُرفض أي ملف معدَّل أو غير موقَّع. على جهاز متصل بالإنترنت، تجلب **محطة التحديث** (تُنزَّل من الصفحة نفسها) الحزم الجديدة لتنقلها أنت. الخادم لا يرسل شيئاً إلى الخارج أبداً.

19. البريد الإلكتروني وSIEM

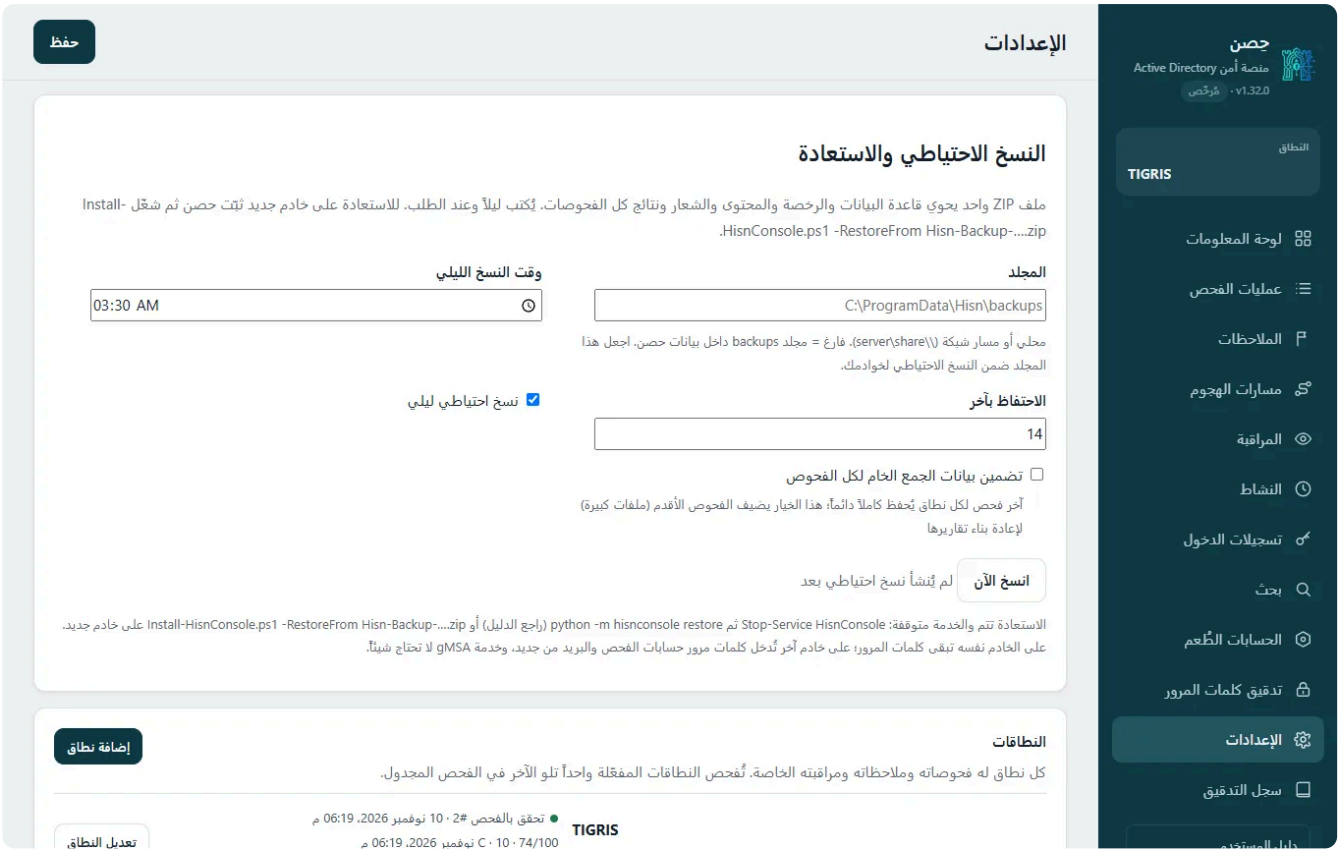
البريد الإلكتروني (*الإعدادات ← البريد الإلكتروني (SMTP)* و*تنبيهات المراقبة*): خادم SMTP والمنفذ والتشفير والمرسِل؛ إرسال تقرير الفحص (باختيار ملف محفوظ) بعد الفحوص المجدولة، وتنبيهات المراقبة فوق حد أدنى من الخطورة. تُرسل التنبيهات في الخلفية، والتنبيهات المتعددة للنطاق نفسه خلال ثوانٍ قليلة تصل في رسالة واحدة بالعربية والإنجليزية.

SIEM (*الإعدادات ← الإرسال إلى Graylog / SIEM*): يرسل التنبيهات وأحداث التدقيق إلى Graylog أو أي مستقبل syslog بصيغة GELF أو CEF أو JSON، عبر UDP أو TCP أو TLS. معطّل افتراضياً.

20. البيانات والنسخ الاحتياطي والاستعادة

الموقع	المحتوى
`C:\Program Files\Hisn`	البرنامج، وسكربتات جامع البيانات، وPython المضمَّن (يُستبدل عند الترقية)
`C:\ProgramData\Hisn`	قاعدة البيانات، ومجلدات الفحوص، والترخيص، والمحتوى، والشعار، والشهادة، والسجلات، والنسخ الاحتياطية (تبقى عند الترقية؛ لا يصل إليها إلا SYSTEM وAdministrators)

النسخ الاحتياطي



الإعدادات ← النسخ الاحتياطي والاستعادة.

كل ليلة في الوقت المحدد (الافتراضي 03:30) تكتب الواجهة ملفاً واحداً `Hisn-Backup-<server>-<date>.zip`، وتحتفظ بأحدث *N* منها (الافتراضي 14). زر **انسخ الآن** يكتب نسخة عند الطلب. يحتوي الملف قاعدة البيانات (نسخة متسقة، آمنة أثناء عمل الخدمة)، و `config.json` ، والترخيص، وحزم المحتوى، والشعار، ونتائج كل الفحوص وتقاريرها. تُضمَّن دائماً البيانات الخام لآخر فحص لكل نطاق، لأن معرّف النطاق وأعداد لوحة المعلومات وإعادة بناء التقارير ومقارنة الفحص التالي تعتمد عليها. أما البيانات الخام للفحوص الأقدم فتُضاف فقط عند تحديد خيار تضمين بيانات الجمع الخام لكل الفحوص.

اجعل المجلد مساراً تشمله النسخ الاحتياطية لخوادمك؛ تصلح مشاركة شبكة مثل `\\backup01\hisn` ، ويحتاج حساب الخدمة إلى صلاحية الكتابة فيها. تركه فارغاً يعني `C:\ProgramData\Hisn\backups` على الخادم نفسه، وهذا يحمي من ترقية فاشلة لكنه لا يحمي من فقدان الخادم.

من سطر الأوامر (للسكربتات والمهام المجدولة): `"C:\Program Files\Hisn\python\python.exe" -m hisnconsole backup --data C:\ProgramData\Hisn --to D:\Backups\Hisn`، مع ضبط `PYTHONPATH` على `C:\Program Files\Hisn\console;C:\Program Files\Hisn\engine` .

الاستعادة

- **على الخادم نفسه من الواجهة:** في *الإعدادات ← النسخ الاحتياطي والاستعادة* انقر **استعادة** بجانب النسخة واكتب `RESTORE`. يعيد حصن تشغيل نفسه، ويحفظ نسخة أمان من الحالة الحالية، ويستعيد النسخة، ثم يعود من تلقاء نفسه؛ سجّل الدخول مجدداً عند إعادة تحميل الصفحة. إن فشل أي شيء يعود إلى نسخة الأمان وتذكر الإعدادات السبب. كل ما هو أحدث من النسخة يُستبدل.
- **على خادم جديد:** شغّل الإعداد واختر النسخة في صفحة الاستعادة من نسخة احتياطية، أو نفّذ `Install-HisnConsole.ps1 -RestoreFrom <zip>`. يستعيد برنامج التثبيت النسخة قبل تشغيل الخدمة.
- **من سطر الأوامر:** `"C:\Program Files\Hisn\HisnConsole.exe" stop`، ثم `python.exe -m hisnconsole restore --data C:\ProgramData\Hisn --from <zip>` (مع `PYTHONPATH` نفسه)، ثم `HisnConsole.exe start`. تُحفظ قاعدة البيانات السابقة باسم `hisn.db.pre-restore`.

بعد الاستعادة على خادم آخر، يذكر تنبيه في الإعدادات كلمات المرور المخزّنة التي أُزيلت: كلمات مرور حسابات الفحص وSMTP وSIEM محمية للخادم القديم (Windows DPAPI) ولا يمكن نقلها. أدخلها من جديد ثم أخفِ التنبيه. الخدمة التي تعمل بحساب **gMSA** لا تحتاج شيئاً. ينتقل الترخيص مع النسخة لأنه مرتبط بمعرّفات نطاقاتك. والنسخة من إصدار أقدم من حصن تُرقّى عند التشغيل الأول (مع نسخة `hisn.db.bak-*` خاصة بها)، أما النسخة من إصدار *أحدث* فتُرفض: ثبّت ذلك الإصدار أولاً.

ما لا تشمله النسخة: شهادة TLS للخادم (تُنشأ شهادة جديدة)، والسجلات، و`config.json` عند الاستعادة إلا مع الخيار `--with-config`. القياس في بيئة الاختبار (3 نطاقات، 15 فحصاً، نسخة بحجم 2.6 ميغابايت): الإيقاف والاستعادة والتشغيل وتسجيل الدخول استغرقت نحو دقيقة.

إلغاء التثبيت: *Hisn AD Security Console* ← Apps ← Settings. يُسأل هل تحتفظ بالبيانات لإعادة تثبيت لاحقة.

21. حل المشكلات

العَرَض	السبب والحل
صفحة فارغة أو رسالة «يحتاج إلى Edge أو Chrome أو Firefox»	المتصفح Internet Explorer. افتح العنوان في Edge أو Chrome أو Firefox.
خطأ WinRM `0x80090322`	وصل Kerberos إلى حساب خاطئ. إما أن اسم وحدة التحكم يُترجم إلى عنوان جهاز آخر (بطاقة شبكة ثانية مسجّلة في DNS: احذف تلك السجلات أو أضف العنوان الصحيح إلى ملف hosts)، وإما أن الاسم `HTTP/<server>` مسجّل على حساب آخر. يعيد حصن المحاولة مع المنفذ في الاسم؛ سجّله مرة واحدة على الخادم: `setspn -S HTTP/<fqdn>:5985 <SERVER>` و`setspn -S HTTP/<short>:5985 <SERVER>`. يذكر اختبار الاتصال الحساب الذي يحمل الاسم.
WinRM «Cannot find the computer» (Kerberos)	غالباً السبب نفسه: حساب gMSA أو حساب خدمة يحمل `HTTP/<server>`. سجّل الأسماء الخاصة بالمنفذ كما سبق.
«رفض الوصول» على خادم عضو	حساب الفحص (أو `DOMAIN\DC$`) ليس في مجموعة Administrators المحلية على الخادم.
فحوص كثيرة «لم يُقيَّم» لنطاق واحد	فشل WinRM إلى وحدة التحكم في ذلك النطاق؛ شغّل اختبار الاتصال وأصلح السبب المذكور، ثم أعد الفحص.
لا يبدأ فحص أو نسخ احتياطي: «المساحة الحرة منخفضة»	المساحة الحرة أقل من الحد الأدنى (2 غيغابايت افتراضياً). أفرغ مساحة، أو اخفض الحد الأدنى في الإعدادات.
صفحة دخول الحسابات المميزة فارغة	المراقبة المباشرة متوقفة، أو لم يُدرج أي فحص حسابات الطبقة صفر بعد. فعّل المراقبة المباشرة وشغّل فحصاً.
سياسة التنفيذ تمنع السكربت	شغّل سكربتات الجمع بالأمر `powershell -ExecutionPolicy Bypass -File <script>`؛ وهذا يسري على ذلك الأمر وحده.

الواجهة لا تفتح	`Get-Service HisnConsole` ؛ والسجلات في `C:\ProgramData\Hisn\logs\console.log` و `C:\ProgramData\Hisn\logs\HisnConsole.err.log` ؛ أو من قائمة ابدأ ← Hisn ← *Hisn health check*.
«قاعدة البيانات من إصدار أحدث من حصن»	ثُبّت إصدار أقدم فوق قاعدة بيانات أحدث. ثبّت الإصدار الأحدث مرة أخرى، أو استعد نسخة احتياطية صُنعت بهذا الإصدار.
المنفذ 8443 مستخدم	شغّل الإعداد مرة أخرى واختر منفذاً آخر.

22. المصطلحات

الطبقة صفر (Tier 0)
الحسابات والمجموعات والأجهزة التي تتحكم بالنطاق كله: وحدات التحكم بالنطاق، وDomain Admins، وEnterprise Admins وما شابهها. من يسيطر على أحدها يسيطر على كل شيء.

ملاحظة
فحص فشل في عملية فحص، مع الكائنات المتأثرة. تحتفظ بحالتها (مفتوحة، مُقَرّ بها، مؤجّلة، استثناء مخاطرة، مُصلحة، عادت للظهور) بين الفحوص.

مسار هجوم
سلسلة من الصلاحيات أو العضويات أو الجلسات تتيح لحساب عادي الوصول إلى الطبقة صفر.

انكشاف
بقاء بيانات اعتماد حساب مميز على جهاز خارج الطبقة صفر، حيث يمكن سرقتها.

جهاز مسموح
محطة إدارة أو خادم قفز أدرجته مكاناً آمناً لدخول حسابات الطبقة صفر.

حساب طُعم
حساب لا يستخدمه أي شيء مشروع، فأي استخدام له تنبيه.

تغيير صامت
تغيير وُجد بمقارنة الفحوص دون حدث مطابق في سجل الأمان: حدث والتدقيق متوقف، أو مُسح السجل.

gMSA

حساب الخدمة المُدار للمجموعات: حساب خدمة ينشئ Windows كلمة مروره ويغيّرها دورياً، ولا تستخدمه إلا الخوادم التي تحددها.

المراقبة المباشرة

قراءة حصن لسجلات الأمان في وحدات التحكم كل دقيقة تقريباً، بين الفحوص.

لم يُقيَّم

فحص تعذّرت قراءة بياناته. لا يُحسب ناجحاً أبداً.

سكربتا الإصلاح والتراجع

أوامر PowerShell يُنشئها حصن ليراجعها المسؤول وينفذها بنفسه؛ حصن لا ينفذها أبداً.