خطة استمرارية الأعمال والتعافي من الكوارث (BCDR) - منصة Kaleem AI

1. المقدمة

1.1. الغرض من الوثيقة

هذه الوثيقة تحدد الإجراءات والاستراتيجيات المتبعة في منصة **Kaleem AI** لضمان استمرارية الأعمال والتعافي السريع والفعال في حالة وقوع حوادث أو كوارث قد تؤثر على تشغيل الخدمات. الهدف الأساسي هو حماية بيانات العملاء، تقليل زمن التوقف، وتوفير مسار واضح للفريق الهندسي للتعامل مع الأزمات.

1.2. نطاق الخطة

تغطي هذه الخطة جميع المكونات الحيوية للبنية التحتية لمنصة Kaleem AI، بما في ذلك: - **الخدمات الأساسية:** API, Workers, Webhooks. - **قواعد البيانات:** MongoDB, Qdrant, Redis. - **أنظمة الرسائل:** RabbitMQ. - **تخزين الملفات:** MinIO. - **خدمات التشغيل:** n8n, Prometheus, Grafana. - **ملفات الإعدادات:** .env files, Docker Compose, Nginx.

1.3. الأهداف الرئيسية (RPO & RTO)

لضمان الحد الأدنى من التأثير على العملاء، تم تحديد الأهداف التالية:

- **هدف نقطة الاستعادة (Recovery Point Objective - RPO):**
- **البيانات الحرجة (الطلبات، العملاء):** ≤ 15 دقيقة.
- **البيانات غير الحرجة (السجلات، التحليلات):** ≤ 24 ساعة. *هذا يعني أن أقصى حجم للبيانات يمكن أن يُفقد في حالة وقوع كارثة هو 15 دقيقة للبيانات الحرجة.*
- **هدف زمن الاستعادة (Recovery Time Objective - RTO):**
- **استعادة خدمة واحدة:** ≤ 1 ساعة.
- **استعادة كاملة للنظام على بنية تحتية جديدة:** ≤ 4 ساعات. *هذا يعني أن أقصى زمن يمكن أن تستغرقه عملية إعادة تشغيل النظام بالكامل هو 4 ساعات.*

2. الأدوار والمسؤوليات

لضمان استجابة منظمة وفعالة، تم تحديد الأدوار والمسؤوليات التالية أثناء حالة الطوارئ:

الدور	المسؤولية الأساسية	المسؤول (الأساسي)	البديل
قائد الحادث (Incident Commander)	- تنسيق جميع جهود الاستجابة. - اتخاذ القرارات النهائية. - التواصل مع أصحاب المصلحة.	قائد الفريق التقني	مدير المنتج
مهندس الاتصالات (Communications Lead)	- إدارة صفحة حالة النظام (Status Page). - إعداد وإرسال التنبيهات للعملاء. - التواصل الداخلي مع الفريق.	مهندس الواجهات الأمامية	مهندس ضمان الجودة
المهندس التقني (Technical Lead)	- تشخيص السبب الجذري للمشكلة. - قيادة جهود الإصلاح والاستعادة التقنية. - توثيق الخطوات المتخذة.	مهندس الواجهات الخلفية (سينيور)	مهندس العمليات (DevOps)
فريق الاستجابة (Response Team)	- تنفيذ المهام التقنية الموكلة إليهم. - مراقبة النظام بعد تطبيق الحلول. - تقديم تقارير مرحلية للقائد التقني.	جميع المهندسين المتاحين	-

3. خطة الاتصالات

التواصل الفعال هو مفتاح إدارة الأزمات بنجاح. سيتم اتباع الخطة التالية:

3.1. الاتصالات الداخلية

- **قناة الطوارئ:** سيتم إنشاء قناة مخصصة على **Slack** باسم `#emergency-room` فور تأكيد الحادث.
- **تحديثات دورية:** سيقوم قائد الحادث بنشر تحديثات كل 30 دقيقة في القناة حول حالة المشكلة والتقدم المحرز.
- **اجتماع الحرب (War Room):** سيتم عقد اجتماع فيديو فوري لجميع أعضاء فريق الاستجابة لتنسيق الجهود.

3.2. الاتصالات الخارجية (العملاء)

- **صفحة حالة النظام (Status Page):** سيتم تحديث صفحة الحالة فورًا لتعكس المشكلة الحالية. يجب أن تكون الرسالة واضحة وموجزة.
- **التنبيهات الأولية:** سيتم إرسال بريد إلكتروني لجميع العملاء المتأثرين في غضون 60 دقيقة من تأكيد الحادث.
- **التحديثات المستمرة:** سيتم نشر تحديثات على صفحة الحالة كل 60 دقيقة أو عند حدوث تطورات مهمة.
- **رسالة الحل:** سيتم إرسال بريد إلكتروني نهائي بعد حل المشكلة وتأكيد استقرار النظام.

4. استراتيجية النسخ الاحتياطي

تعتمد استراتيجيتنا على قاعدة **3-2-1** للنسخ الاحتياطي (3 نسخ، على وسيطين مختلفين، ونسخة واحدة خارج الموقع).

4.1. جدول النسخ الاحتياطي الآلي

يتم تشغيل جميع سكربتات النسخ الاحتياطي عبر (`/etc/cron.d/kaleem-backups`) Cron.

الخدمة	التكرار	الأداة/الطريقة	الموقع الأساسي	الموقع الثانوي
MongoDB	كل 6 ساعات	`mongodump`	`backups/mongo/` (محلي)	`restic` (مشفر)
Qdrant	يوميًا (02:10)	`snapshot` API	`backups/qdrant/` (محلي)	`restic` (مشفر)
RabbitMQ	يوميًا (02:20)	`definitions` JSON	`backups/rabbitmq/` (محلي)	`restic` (مشفر)
n8n (SQLite)	يوميًا (02:30)	`tar`	`backups/n8n/` (محلي)	`restic` (مشفر)
MinIO Bucket	يوميًا (02:50)	`mc mirror`	`backups/minio/` (محلي)	`restic` (مشفر)
Config Files	يوميًا (02:40)	`tar`	`backups/configs/` (محلي)	`restic` (مشفر)
Restic Repo	يوميًا (03:10)	`restic push`	-	S3-Compatible Storage (خارجي)

4.2. النسخ الاحتياطي الخارجي (Off-site)

- **Restic to S3:** يتم دفع مستودع Restic المحلي المشفر إلى خدمة تخزين سحابي متوافقة مع S3 (مثل Backblaze B2 أو AWS S3) يوميًا. هذا يضمن وجود نسخة كاملة من البيانات خارج الموقع الجغرافي للخادم الرئيسي.
- **النسخ اليدوي الطارئ:** في حالة الحاجة، يمكن سحب نسخة يدوية من مجلد `backups/` بالكامل إلى جهاز محلي باستخدام `scp` .

5. إجراءات الاستعادة

مبدأ أساسي: قبل البدء في أي عملية استعادة، يجب أخذ نسخة احتياطية إضافية للحالة الحالية إذا كان ذلك ممكنًا لتجنب فقدان أي بيانات لم يتم نسخها بعد.

5.1. سيناريو 1: فشل خدمة واحدة (Single Service Failure)

الهدف: استعادة خدمة واحدة مع أقل تأثير ممكن على بقية النظام.

استعادة MongoDB:

1. **تحديد النسخة:** اختر أحدث نسخة احتياطية من `backups/mongo/` .
2. **تنفيذ الاستعادة:** `bash mongorestore --uri="${MONGODB_URI}" --gzip --archive=/backups/mongo/mongo-YYYY-MM-DD-HHMM.archive.gz --oplogReplay`
3. **التحقق:** قم بالاتصال بقاعدة البيانات وتحقق من وجود البيانات المستعادة.

استعادة Qdrant:

1. **نسخ الـ Snapshot:** `bash docker cp /backups/qdrant/qdrant-YYYY-MM-DD.snapshot kaleem-qdrant:/qdrant/storage/snapshots`
2. **تفعيل الاستعادة عبر API:** `bash curl -X POST "http://localhost:6333/collections/snapshots/recover" -H "Content-Type: application/json" -d '{ "location": "file:///qdrant/storage/snapshots/qdrant-YYYY-MM-DD.snapshot" }'`
3. **التحقق:** تحقق من الـ Collections عبر واجهة Qdrant أو الـ API.

5.2. سيناريو 2: كارثة كاملة (Total Disaster Recovery)

الهدف: إعادة بناء البنية التحتية بالكامل على خادم جديد (New VPS).

الخطوات: 1. **تجهيز الخادم الجديد:** - قم بإنشاء VPS جديد بنفس مواصفات الخادم القديم. - قم بتثبيت Docker و Docker Compose. - قم بضبط إعدادات جدار الحماية الأساسية (SSH, HTTP, HTTPS).

1. **استعادة ملفات الإعدادات والنسخ الاحتياطي:**
2. قم بتوصيل خدمة التخزين السحابي (S3) بالخادم الجديد.
3. قم باستعادة مستودع Restic بالكامل إلى مجلد `backups`. `bash restic -r s3:your-bucket-name/restic-repo restore latest --target /`
4. **تحقق من وجود جميع ملفات النسخ الاحتياطي والإعدادات في مجلد `backups/` .**
5. **إعادة نشر الخدمات:**
6. انتقل إلى مجلد المشروع (`opt/musaidbot/musad-bot-n8n/`).
7. قم بتشغيل جميع الخدمات باستخدام `bash docker-compose up -d` Docker Compose.
8. **استعادة بيانات الخدمات:**

9. اتبع نفس إجراءات الاستعادة المذكورة في **سيناريو 1** لكل خدمة على حدة (MongoDB, Qdrant, RabbitMQ, n8n, MinIO).

10. **تحديث سجلات DNS:**

11. قم بتوجيه جميع سجلات DNS (A Records) للدومينات والدومينات الفرعية إلى عنوان IP الخاص بالخادم الجديد.

12. **الاختبار الشامل:**

13. قم بإجراء اختبارات E2E شاملة للتأكد من أن جميع أجزاء النظام تعمل بشكل صحيح.
14. راقب سجلات الأخطاء والموارد عن كثب خلال الساعات القليلة الأولى.

6. الصيانة والاختبار

خطة الطوارئ لا قيمة لها بدون اختبار وصيانة دورية.

6.1. اختبار الاستعادة

- **التكرار:** مرة كل ثلاثة أشهر (ربع سنوي).
- **الإجراء:** يتم تنفيذ **سيناريو 2 (كارثة كاملة)** على بيئة اختبار معزولة (Staging Environment).
- **التوثيق:** يتم تسجيل نتائج كل اختبار، بما في ذلك:
- هل نجحت العملية؟ (نعم/لا)
- الزمن الفعلي للاستعادة (Actual RTO).
- أي مشاكل أو تحديات تمت مواجهتها.
- توصيات لتحسين الخطة.

6.2. مراجعة الخطة

- **التكرار:** مرة كل ستة أشهر.
- **الإجراء:** يقوم الفريق بمراجعة هذه الوثيقة بالكامل وتحديثها لتعكس أي تغييرات في البنية التحتية أو الإجراءات.

7. الملحقات

7.1. أوامر Restic المفيدة

```
# تهيئة مستودع Restic (لأول مرة فقط)
# restic -r /path/to/repo init

# عرض جميع النسخ الاحتياطية (Snapshots)
restic -r /path/to/repo snapshots

# مقارنة نسختين
restic -r /path/to/repo diff <snapshot1_id> <snapshot2_id>

# التحقق من سلامة المستودع
restic -r /path/to/repo check
```

7.2. نموذج رسالة للعملاء (تحديث صفحة الحالة)

العنوان: انقطاع جزئي في الخدمة

الحالة: قيد التحقيق

الوصف: نحن نواجه حاليًا انقطاعًا جزئيًا في الخدمة يؤثر على [وصف موجز للميزة المتأثرة، مثل: إرسال واستقبال الرسائل]. فريقنا الهندسي يقوم بالتحقيق في المشكلة على وجه السرعة. سنقوم بتوفير تحديث آخر خلال 60 دقيقة.

نعتذر عن أي إزعاج قد يسببه هذا الأمر.