إسترداد المعلومات في حال حدوث الكوارث

توطأة

لاشك في أن المعلومات الإلكترونية قد استحوذت على إهتمام الناس وطغت على جميع نـــواحي حيـــاتهم فصارت المعلومات الإلكترونية جزءاً مهماً يمثل الأساس في التعاملات المالية والإعلامية والبحثية والثقافيـــة والحكومية وغيرها، ونظراً لهذا الزخم الكبير والكم الهائل من المعلومات ونظراً لما لهذه المعلومات من أهمية فائقة فقد توجهت إهتمامات الخاصة والعامة لحفظ معلوماتهم من الضياع بعمل نســخ إحتياطيـــة للمعلومـــات المهمة.

هذا الإهتمام بحفظ المعلومات والتأكد من سلاماتها لم يقف إلى حد حمايتها في حال حدوث الأعطال فـــي أجهزة الحاسب وإنما نحى منحاً مختلفاً يعنى بحفظ المعلومات في أماكن آمنة تجنباً لضياعها في حال حـــدوث كوارث كبيرة قد تغطي منطقة جغرافية صغيرة أو كبيرة كحدوث الزلازل والحروب والحرائق وغير ذلك.
في هذا البحث سنتحدث إن شاء الله عن أبعاد مشكلة إسترداد المعلومات في حال حدوث الكـــوارث وطـــرق تنفيذها والجدوى منها.

1. المقدمة

لقد أصبحت الأعمال التجارية من مختلف الأحجام تعتمد إعتماداً متزايداً على المعلومات لتحقيق وجودهـــا ولتتمكن من المضي في عملها. إن المخاطر المترتبة على فقدان المعلومات لدى الأعمال التجارية لـــم تعـــد خافية على أحد فقد زاد الوعي بأهمية حفظ المعلومات بطريقة جيدة, يدل علـــى ذلـــك الـــوعي أن الأعمـــال التجارية الصغيرة و المتوسطة (Small and Medium Businesses) (SMB) التي تقوم بتحميـــل نســـخ إحتياطية على الخوادم (Servers) تكاد تصل إلى 100% [1].

إن الوعي لم يقف عند هذا الحد بل تجاوزه ليشمل الإهتمام بإختيار المكان المناسب لحفظ المعلومات.

من المعلوم أن أنظمة المعلومات معرضة للتوقف والخلل لسهولة تعرضها للإعتداء وسرعة تأثرها بذلك, كما يحدث في حال حصول عطب في القرص الصلب أو مايحدث نتيجة للإعتداءت الخارجية. زيادة علـــى ذلك فإن حصول عطل بسيط قد يحدث مشكلة كبيرة إذا لم يكن هناك نسخة إحتياطية مناسبة أو قـــدرة علـــى إسترداد المعلومات. مثال على ذلك أن شركة خاصة واجهتها مشكلة في قاعدة البيانات لديها ممـــا أدى إلـــى إلغاء مئات الرحلات الجوية وتعطل الآف المسافرين. إن هذه المشكلات من الممكن أن تحل أو تقلل بإنشـــاء نظام تقني وإداري قوي, لكن المشكلة تبقى واردة والأعطال ممكنة بما تسببه الكوارث الطبيعية أو التي تحدث بفعل الإنسان والتي لا يمكن التحكم فيها. ما حصل في أكلوهوما عام 1995م وفي نيويـــورك 2001م مـــن تفجيرات أدى إلى دمار المباني المستهدفة بالكلية جعل من الضرورى أن تعاد أنظمة المعلومات بتغيير مكانها إلى مكان آخر [2].

إن كثير من المنظمات و الشركات قد وسعت ميزانياتها لضمان إمكانية تشغيل بنيتها التحتية الحسابية والتخزينية للمعلومات بعد وقوع طوفان أو حريق أو زلزال أو غيرها من الكوارث. من الأشياء الأساسية والتي يجب أن توخذ في الإعتبار في ما يتعلق بإسترجاع المعلومات عنصرين أساسيين:

- حفظ ونسخ البنية التحتية الحسابية.
- حماية وتأمين نسخ حديثة للأشياء المهمة إن لم يكن لجميع المعلومات [3].

يمكن تقسيم الكوارث التي تصيب أنظمة الحاسب والمعلومات على النحو التالي [4]:

1. الدرجة الأولى: وهي أقل الكوارث حدة. كما لو حدث عطل في شبكة الكهرباء أو نحو من ذلك. هذا النوع من الأعطال هو أكثر الأعطال إنتشاراً ومن الممكن أن يكون خطيراً إذا لم يتم الإستعداد له. ثلاث ساعات من التوقف قد يكلف المنشأة الشئ الكثير من الخسائر في الإنتاج والأداء. من حسن الحظ فهذا النوع من الكوارث يمكن تفاديه وتفادي أضراره بإستعمال بطاريات إحتياطية وموالدات محلية.
2. الدرجة الثانية: وهي الكوارث الطبيعية أو الناجمة عن فعل الإنسان مثل الفياضانات والحرائق التي تدمر غرف الحاسب الآلي. هذا النوع يحتاج إلى تخطيط وعمل أكثر من الدرجة الأولى من الكوارث لأن زمن الإنقطاع في هذه الحالة قد يستمر لعدة أيام أو أسابيع. إن حل هذه المشكلة يكمن في التعاقد مع وكيل خارجي ليوفر مركزاً متنقلاً للحاسب يمكن إستخدامه في مثل هذه الحال أو يمكن إنشاء مركز إحتياطي من قبل المنشأة نفسها في مكان آخر ليستفاد منه في وقت حدوث الكوارث.
3. النوع الثالث: الكوارث الطبيعية واسعة الإنتشار. مثال على ذالك الزلازل والفياضانات والأعاصير والتي يحتاج التعمل معها إلى أعلى درجات التخطيط. هذا النوع من الكوارث من أصعب الكوارث ومن أشدها تأثيراً على المنشآت وبدون تخطيط محكم يمكن أن يكون هذا النوع من الكوارث موتاً محققاً لأي منشأة. إن حل هذه المشكلة يكمن في إنشاء مركز للحاسب في مكان آخر سواءً تم ذلك بواسطة المنشأة نفسها أو بواسطة وكيل خارجي كما مر بنا في الحديث عن الدرجة الثانية من الكوارث.

في هذا البحث سنستعرض إسترتيجية إسترجاع المعلومات بعد حصول الكوارث وأنواع المعلومات بحسب أهميتها وآلية حفظ وإسترجاع المعلومات ومن ثم الخاتمة.

2. إستراتيجية إسترجاع المعلومات بعد حصول الكوارث (Data Disaster Recovery Strategy)

إن أبسط الطرق لإسترجاع المعلومات بعد حصول الكوارث (Data Disaster Recovery) (DDR) تكمن في نسخ أقل حسابات البنية التحتية في مكان آخر بعيد عن الموقع الأصلي للأجهزة وبتحديث البيانات بإستمرار للتأكد من صلاحيتها في حال حدث الكوارث لا قدر الله. ومما يجب أن يؤخذ بعين الإعتبار تخفيض تكاليف تأسيس نظام استرجاع المعلومات.

مما يجدر التنبه له فصل البنية التحتية الحسابية لل DDR عن البنية التحتية التخزينية حيث أنهما مختلفين تماماً. إنه لمن السهولة بمكان أن تضيف أجهزة إحتياطية لمعالجة المعلومات ولكنه ليس بالسهل أن تحتفظ بنسخ حديثة للبيانات المهمة والحساسة. لذلك كان من الضروري أن نفصل العمليتين عن بعضهما البعض

بحيث يكون نظام تخزين المعلومات مستقلاً عن نظام ال DDR مما ينتج عنه مرونة في إنشاء نظام ال DDR وبالتالي تقليل التكاليف وأيضاً تبسيط التصميم المطلوب لتوفير نظام ال DDR الحساس. عندما يتم نقل البيانات إلى مكان معدٍ خصيصاً للتخزين فإن توفير الأجهزة القادرة على التعامل مع هذه المعلومات أمر مباشر جداً [3].

3. أهداف المنشأة التجارية في ما يختص بإسترجاع المعلومات [1]

لكل منشأة هدف خاص بما تحتاجه من نظام إسترجاع المعلومات لديها وهذا الهدف ينبني على طبيعة عمل المنشأة وينبني عليه طريقة إنشاء النظام. لتحديد أهداف أي منشأة تجارية في ما يختص بما تطمح فيه من نظام استرجاع المعلومات لديها يمكن تقسيم العمل اللازم لذلك إلى خطوات يسهل تطبيقها واتباعها وهي كالتالي:

1. الخطوة الأولى، تحديد أولويات العمليات: وهذه هي الأولى في طريق بناء نظام لحفظ البيانات والتي تتضمن نظرة فاحصة في المنشأة التجارية وطريقة عملها. إنه لمن المعلوم أنه خلال العقود الثلاثة الماضية والبنية التحتية الحسابية والبيانات التي تديرها أصبحت تمثل جميع العمليات اليومية لمعظم القطاعات التجارية. كم من الوقت تستطيع منشأة العمل بدون بنيتها التحتية الحاسوبية وبدون بياناتها؟ في الجدول (1) يمكننا تقسيم الأعمال التي تقوم بها المنشأة إلى أنواع يمكن من خلالها تقييم أهمية هذه الأعمال ومدى تأثيرها على سير العمل.

الأثر على المنشأة	العمليات	مثال
مصيري وتعتمد عليه أهداف الشركة الرئيسية	جلب العوائد ومقابلة الزبائن	التجارة الإلكترونية وخدمات العملاء
مهم للمنشأة	العمليات داخل المنشأة	البريد الإلكتروني، الحسابات والتصنيع
مهم لسير العمل	الأقسام	قاعدة بيانات الأقسام وخادم الملفات والطابعات

جدول (1) أنواع الأعمال داخل المنشأة

2. الخطوة الثانية، تحديد الأهداف: بعد تحديد ومعرفة أولويات العمليات داخل المنشأة يصبح من الممكن تحديد أهداف استرجاع المعلومات. هنالك ثلاثة مفاهيم رئيسية لا بد من أخذها بعين الإعتبار عند تصميم نظام استرجاع المعلومات:
   - أ- الوقت المستهدف للإسترجاع Recovery Time Objective (RTO): ويمثل الوقت الذي نحتاجه لإعادة النظام إلى العمل بعد وقوع العطل.
   - ب- النقطة المستهدفة للإسترجاع Recovery Point Objective (RPO): والمقصود هنا كمية المعلومات المسموح بفقدها من آخر تحميل إحتياطي ناجح إلى وقوع العطل.

ج- نوع البيانات المفقودة Data Loss Event (DLE): وهو نوع وحجم العطل الذي يسبب فقد البيانات.

هذه المفاهيم تأخذ حيزاً مهماً لدى الشركات الكبيرة وقد بدأت أيضاً الشركات الصغيرة والمتوسطة بالإهتمام بهذه المفاهيم والإعتماد عليها. إن ضبط أهداف ال RTO وال RPO يحتاج من المنشأة إلى التفكير العميق وعمل الحسابات المنطقية الواضحة لتحديد مدى أهمية إي تطبيق وأثره على سير عمل المنشأة، وإليكم بعض الأمثلة الواقعية لتترسخ هذه المفاهيم:

مثال 1:

ينص نظام للمحامين والذي يظم 50 محامياً على أن والوقت المسموح به لعدم الوصول إلى المعلومات (RTO) يساوي 48 ساعة ولكن بمجرد دخول المعلومات للنظام فلا مجال لفقد أي شئ منها، مما يعني أن ال (RPO) في هذه الحالة يساوي صفراً.

مثال 2:

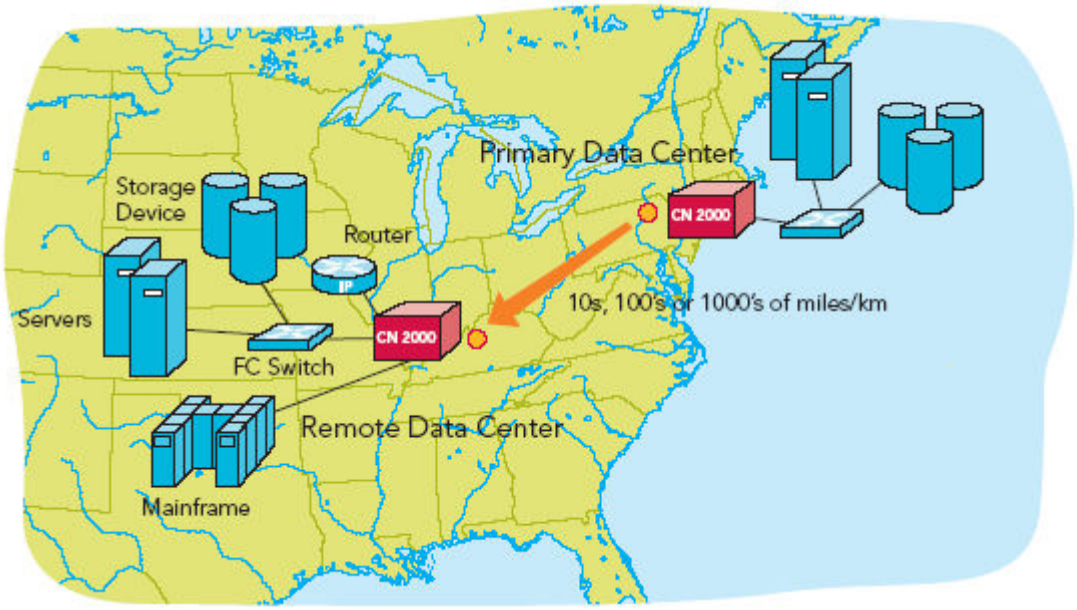
شركة تأمين تحرص على إمكانية وصول زبائنها إلى أنظمتها في حال حدوث الكوارث تنص على أن ال (RTO) يجب أن لا يزيد عن 4 ساعات ولكن لا بأس بفقد المعلومات المدخلة في آخر ساعتين قبل وقوع الكارثة لسهولة إمكانية إدخالها مرة أخرى مما يعني أن ال (RPO) يساوي ساعتين

3. الخطوة الثالثة، تحديد حالات فقد البيانات: من المعلوم أن الحالات التي تفقد فيها المعلومات تحدث بأشكال مختلفة. وجد بالتتبع أن فقد المعلومات يحصل في الغالب بسبب الأخطاء البشرية وذلك يمثل 83 % من مجمل فقد المعلومات، يلي ذلك في كثرة الحدوث ما يحصل من فساد للملفات داخل الأجهزة الحاسوبية بسبب الفيروسات وغيرها وهذا يمثل 10 %، ثم يكون ما يمثل 5 % من فقد المعلومات بسبب الأعطال التي تحدث في أجهزة تخزين المعلومات، أما ال 3 % المتبقية فهي ما يحصل بسبب الكوارث التي تدمر المنشآت أو ما يحصل من عطل لأجهزة الحاسب أو سرقتها. من هذه الإحصائيات يتبين لنا أهمية معرفة النوع الذي نتعامل معه لنتمكن من عمل الإستعدادات اللازمة وليس هذا فحسب بل لتحديد حجم الميزانية التي يجب أن تنفق في هذا الخصوص.
4. الخطوة الرابعة، وضع الأشياء مع بعضها البعض: بعد معرفة أولويات الشركة أو المنشأة وبعد تحديد الزمن المستهدف لإسترجاع المعلومات (RTO) لكل تطبيق ومقدار الفقد المسموح به (RPO) والحالات التي يتم فيها فقد المعلومات، يمكننا أن نضع هذا الأشياء مجتمعة ونرسم جدولاً يبين كل المعلومات التي نحتاج إليها لكل تطبيق على حدة.

4. طريقة إنشاء مركز إضافي لتخزين المعلومات [5]

كما ناقشنا في الفقرات التالية فإن النتيجة النهائية والحل الكلي يكمن في إنشاء مركز لتخزين نسخ إحتياطية للمعلومات بحسب أهميتها وبالطريقة التي تتناسب مع أهداف المنشأة صاحبة العمل. الشكل (1) يبين كيفية إنشاء مركز بيانات بعيد عن مركز البيانات الأساسي بعشرات أو مئات أو الآف الكيلومترات. إن إنشاء مثل هذه الشبكة يتم بواسطة أجهزة شبكات الحاسب من خادمات ومحولات ومبدلات وأهم من ذلك كله

قناة إتصال ذات موثوقية عالية تلبي الحاجة المطلوبة في نقل البيانات من المركز الأساس إلى المركز الثانوي البعيد.



شكل (1) نسخ البيانات بين مراكز المعلومات البعيدة عن بعض

يتطلب الحصول على نظام لتخزين البيانات توفير خطوط إتصال غير مكلفة في الدرجة الأولى وتتوفر فيها الخصائص الرئسة التالية:

- سرعة نقل المعلومات (High Throughput): فتطبيقات تخزين البيانات هي أكثر التطبيقات إستهلاكاً للشبكات.
- قلة التأخير (Low Latency): فتطبيقات تخزين البيانات تحتاج إلى وقت إستجابة قصير وإلا حدث ضرر بأدائها.
- عدم فقد أي من المعلومات أو تقليل المفقود منها (Zero or Minimal Data Loss): وهذا يعتمد على نوع التطبيق، ففي بعض الأحيان لا يقبل فقد أي شئ من المعلومات ولكن في جميع الأحوال تقليل الفقد أمر مطلوب في جميع تطبيقات التخزين. إن إعادة إرسال المعلومات أمر مكلف يؤثر بقوة على أداء التخزين.

الجدول رقم (2) يبين بعض الطرق المستخدمة في التخزين – والتي لا يتسع المجال للإسهاب في الحديث عنها – وما تحتاجه من سرعة ومدى التأخير المسموح به ومدى الفقد المسموح به. SAN تعني Storage Area Network.

Application	Typical Throughput	Latency Requirement	Loss Tolerance
Synchronous Disk Mirroring	10 to 40 MB/s	Low, fixed latency	Zero loss
Asynchronous Disk Mirroring	10 to 40 MB/s	Low latency	Zero loss
Remote Backup	10 to 40 MB/s	Low latency	Low loss
Clustering	5 to 20 MB/s	Low, fixed latency	Zero loss
SAN extension	10 to 40 MB/s	Low latency	Zero loss

جدول (2) إحتياجات تطبيقات التخزين

إن الأعمال التجارية الكبيرة والحكومية تحتاج إلى خيارات ذات موثوقية عالية في الإتصال والتي يمكن من خلالها نسخ البنية التحتية لمراكز البيانات الموجودة وفي نفس الوقت تكون إقتصادية للغاية حيث أن إحتياجاتهم التخزينية تزداد يوماً بعد يوم.

في نهاية هذا البحث يجب التعريج بسرعة على أنواع الشبكات الممكن إستخدامها لإنشاء مراكز بعيدة لتخزين المعلومات. من أشهر التقنيات المستخدمة في شبكات الحاسب ما يلي:

- IP Virtual Private Networks (IP VPN): وهذه التقنية تعتمد على بروتوكول TCP/IP وتعاني من مشاكل كثيرة نظراً لتقادمها، فأداءها في ما يتعلق بالتأخير والفقد لا يناسب تطبيقات تخزين المعلومات.
- ATM-Based Networked Remote Storage: ومن مشكلات هذه التقنية التكلفة العالية والتأخير الناتج عن معالجة البيانات داخل الخلايا التي تعتمد عليها هذه التقنية وكذلك عدم القدرة على توفير السرعة المطلوبة في تطبيقات التخزين.
- SONET/SDH: وهذه من الحلول الممتازة لتطبيقات التخزين والتي تتمتع بسرعات عالية وقلة التأخير وقلة فقد البيانات داخل خطوط النقل.
- WDM: وهذه التقنية الرائعة تلبي الحاجة إلى السرعات الكبيرة جداً لنقل أكبر كم من المعلومات مع قلة التأخير الفائقة والتي تعتمد على الألياف البصرية في عملها. ومن ميزات هذه التقنية المرونة في إعطاء السرعات للمشتركين والتي تصل إلى 10 Gbps. ومما يجدر التنبيه عليه أن هذه التقنية إقتصادية أكثر من سابقاتها.

5. خاتمة

إن مسألة حفظ المعلومات لتفادي فقدانها في حال حدوث كوارث طبيعية أو ناتجة عن فعل الإنسان ولتوفير القدرة على إسترجاعها متى ما أحتيج لذلك، إن هذه القضية من القضايا التي أصبحت تؤرق إدارات المنشآت التجارية والحكومية. عند التفكير بعمل نظام لتخزين المعلومات لحفظها من الكوارث فلا بد من حفظها في أماكن متفرقة وفي أماكن جغرافية متباعدة. لتصميم نظام إسترجاع المعلومات في حال حدوث الكوارث يتطلب ذلك أن يكون هنالك إسترتيجية واضحة ودراسة وافية لنوع المعلومات المراد حفظها وأهداف الشركة في ما يتعلق بطريقة إسترجاع المعلومات من وقت وكمٍ وغير ذلك، وأخيراً تنفيذ ذلك على أرض الواقع بإستخدام تقنيات الشبكات المعروفة.

مما يجب أن يدرس بعمق وبتقصي كبير، أهمية المعلومات المراد حفظها والتكاليف المترتبة على حفظها. فلا بد من التوفيق بين جودة وكمية الحفظ والتكاليف المترتبة على التأسيس والصيانة. في هذا البحث تم الحديث بشئ من التفصيل غير المسهب في ما يتعلق بأنواع المعلومات وأهداف استرجاع المعلومات والتقنيات المتوفرة للتنفيذ يرجى أن تكون قد وصلت بالقارئ إلى شاطئ من المعرفة بالموضوع تفتح له آفاقاً جديده وتيسر له فهمه وتصوره.

6. المراجع

1) Data Disaster Recovery for Small to Mid-Sized Businesses, White Paper, U.S. Data Trust, 2002-2004 Live Vault Corporation.