بسم اللّٰه الرحمن الرحيم

ماورد في المحاضره:

س- ماالفرق بين user management and hardware management ؟

جـ/ user management يمكن أن يدير أكثر من نظام.

اما hardware management لايدير الا نظام واحد.

Removable storage:

1- Floppy disk
2- H.W disk
3- CDsبجميع انواعه وأحجامه.
4- standard of type USBs

System monitor:

تحليل مصادر النظام.

Layers of IT system:

1- Software
2- App/ services
3- OS

تعريف المراقبه: هي المراقبه المستمره لأي بنيه تحتيه.

أنواع المراقبه:

1- تقنيه.
2- وظيفيه.
3- مراقبة عمليه تجارية.

أهمية المراقبه:

1- إنذار مبكر واستجابة استباقيه.

2- حماية البيانات.

3- جمع بيانات.

- الأدوات إما أن تكون:

1- server مثل: mainframe.

2- Software مثل: sole worms.

3- Website مثل: Aero.

س- كيف نصنف الأداة الأفضل؟

1- الأداة التي تدعم الشبكات المعقده.

2- الأداة التي تعطي تنبيهات مستمره (حسب ظبطها).

3- التي لديها مستوى عالي من الأتمته.

4- الأداة التي تساعد في إخراج تقارير.

إدارة النظام والصيانة

المقدمة

1. **ما هي إدارة النظام؟**
2. **تاريخ إدارة النظام.**
3. **إدارة المستخدمين وإدارة الأجهزة.**
4. **النسخ الاحتياطي للبيانات.**

إدارة النظام

- تشير إدارة النظم إلى عملية إدارة نظام أو أكثر من أنظمة الأجهزة والبرامج.
- يقوم بهذه المهمة مسؤول النظام الذي:
  - يراقب صحة النظام.
  - يراقب ويخصص موارد النظام مثل مساحة القرص، ويقوم بإجراء النسخ الاحتياطي، ويوفر وصول المستخدم، ويدير حسابات المستخدمين.
  - يراقب أمان النظام وينفذ العديد من الوظائف الأخرى.

مسؤول النظام

- مسؤول النظام (System Administrator) أو(SA) مسؤول عن إدارة والإشراف على بيئة الحوسبة متعددة المستخدمين، مثل شبكة محلية (LAN) .
- تختلف مسؤوليات مسؤول النظام بناءً على متطلبات المؤسسة. يجب أن يمتلك مسؤول النظام معرفة تقنية قوية ومهارات، بالإضافة إلى خبرة في إدارة الأفراد.
- يُعرف مسؤول النظام أيضًا باسم مسؤول الأنظمة أو مدير النظام .(SysAdmin) قد يكون لدى مؤسسة صغيرة مسؤول نظام واحد فقط، بينما تمتلك المؤسسات الكبيرة فريقًا كاملًا لإدارة النظام.

أنواع مسؤولي النظام بناءً على أدوارهم ومسؤولياتهم:

1. **مسؤولو قواعد البيانات:**
   - إعداد وصيانة قواعد البيانات المستخدمة في المؤسسة، قد يُطلب منهم دمج البيانات من قاعدة بيانات قديمة إلى قاعدة جديدة أو حتى إنشاء قاعدة بيانات من الصفر.
2. **مسؤولو الشبكات:**

- إدارة البنية التحتية للشبكات بالكامل في المؤسسة، وتصميم وتثبيت أنظمة الحاسوب، أجهزة التوجيه(Routers) ، المحولات(Switches) ، الشبكات المحلية(LAN) ، الشبكات الواسعة(WAN) ، وأنظمة الإنترانت.

3. **مسؤولو أنظمة الأمان:**

- مراقبة وصيانة أنظمة الأمان في المؤسسة، تطوير إجراءات الأمان المؤسسية وإجراء فحوصات بيانات دورية، إعداد، حذف، وصيانة حسابات المستخدمين.

تاريخ إدارة الأنظمة:

1940 - 1979

- الحواسيب العملاقة.(Supercomputers)
- الحواسيب المركزية.(Mainframes)
- الحواسيب الصغيرة والمتوسطة.(Minis & Micros)

1980 - 1990

- الشبكات.(Networks)
- أنظمة العميل/الخادم.(Client/Server)
- المبرمجون.(Programmers)
- المشغلون.(Operators)

2000وما بعدها:

حوسبه.

إدارة المستخدمين

- القدرة على إدارة :
  - الأجهزة.
  - الأنظمة.
  - التطبيقات.
  - أنظمة التخزين.
  - الشبكات.
  - خدمات البرمجيات كخدمة.(SaaS)
  - وصول المستخدم إلى موارد تقنية المعلومات الأخرى.

إدارة الأجهزة

- نظام إدارة الأجهزة يوفر معلومات مفصلة عن جميع أصول الأجهزة الحاسوبية المستخدمة.

المهام:

1. عرض وفحص تكوين كل جهاز كمبيوتر، خادم، أو جهاز حاسوب محمول على الشبكة.
2. وضع علامات على كل أصل وتخصيصه للموظفين.
3. تتبع البرامج المثبتة على كل جهاز.

الفوائد:

- تتبع الأجهزة في أنظمة الموظفين.
- تحديد السرقات والخسائر.
- التخلص من الإنفاق على الأجهزة غير المستخدمة.
- تتبع والإبلاغ عن جميع مشتريات الأجهزة.

- إدارة مخزون الأجهزة.
- تقليل تكاليف الصيانة.
- مراقبة الإصلاحات ضمن الضمان(أي أن ضمن الضمان يشير إلى دور نظام إدارة الأجهزة في تتبع الإصلاحات التي تتم للأجهزة التي لا تزال ضمن فترة الضمان الخاص بها.

النسخ الاحتياطي للبيانات:

- النسخ الاحتياطي هو ممارسة نسخ البيانات من الموقع الأساسي إلى موقع ثانوي لحمايتها في حالة وقوع كارثة، حادث أو عمل خبيث.
- يشير النسخ الاحتياطي إلى نسخ الملفات أو قواعد البيانات الفعلية أو الافتراضية إلى موقع ثانوي للحفاظ عليها في حالة فشل المعدات أو حدوث كارثة.

خيارات النسخ الاحتياطي:

1. الوسائط القابلة للإزالة.(Removable Media)
2. النسخ الاحتياطي المكرر.(Redundancy)
3. الأقراص الصلبة الخارجية.(External Hard Drives)
4. أجهزة النسخ الاحتياطي.(Hardware Appliances)
5. برامج النسخ الاحتياطي.(Backup Software)
6. خدمات النسخ الاحتياطي السحابية.(Cloud Backup Services)

المحاضره الثانيه

ماورد بالمحاضره:

س- ماهو الفرق بين الـ server and Desktop؟

من حيث التعريف:

Desktop:إدارة كل الكمبيبوترات داخل المنظمه.

Server:إدارة كل السيرفرات داخل المنظمه.

من حيث الأهميه:

Desktop

1- تحسين أداء الشركه.
2- أمان عالي للشركه.
3- زيادة إنتاج الشركه.

Server

1- تقليل تباطئ الخادم وقت التعطيل.

س-ماذا نعني بالمراقبه في الوقت الفعلي؟

جـ/ عملية تجميع وتخزين مقاييس حركة البيانات

س- لماذا المنظمات تحتاج real time؟

1- تعقب أداء الشركه.
2- تعقب نشاط الشركه.
3- تعقب أمنية الشبكه.
4- تحديد المشاكل بمجرد ظهورها.
5- زيادة أداء الشركه.
6- حفظ التكاليف (من خلال تجنب الشركه شراء أدوات للمراقبه).

المحتويات

مراقبة النظام

- يعد مراقبة الأنظمة جزءاً أساسيًا لإدارة بيئات تقنية المعلومات المعقدة اليوم، يتضمن مراقبة صحة التطبيقات والخدمات المختلفة لضمان عملها بشكل جيد.

- **برمجية مراقبة النظام: هي أداة تتيح مراقبه وتسجيل وتحليل مصادر النظام**

مستويات مراقبة النظام:

1. **الطبقة العليا :**
   - البرامج المستخدمة من قِبل المستخدمين.
2. **الطبقة المتوسطة :**
   - التطبيقات والخدمات.
3. **الطبقة السفلى :**
   - الأنظمة التشغيلية والبرامج الثابتة(التي تأتي مثبته بـال ROM).

ما الذي يتم مراقبته؟

- وحدة المعالجة المركزية.(CPU)
- ذاكرة الخادم.
- أجهزة التوجيه.(Routers)
- المحولات.(Switches)
- عرض النطاق الترددي.(Bandwidth)
- التطبيقات.
- أداء وتوافر الأجهزة الهامة.

- تشمل المراقبه المستمره للبنية التحتيه كما تعرف بـ نظام تكنولوجيا المعلومات وتدار بواسطة مدراء تكنولوجيا المعلومات.

أنواع مراقبة النظام

1. **المراقبة الوظيفية:**
   - تركز على الوظائف التي تقدمها تطبيقات محددة أو الأنظمة الموزعة، الهدف هو تقييم الأداء وتوافر حالات الاستخدام على النظام.
2. **المراقبة التقنية:**
   - تهتم بصحة المعدات أو البرامج الفردية، تركز على وظائف الكائن قيد المراجعة بدلاً من دوره في النظام.
3. **مراقبة العمليات التجارية:**
   - تعد الهدف النهائي لإدارة الأنظمة، تقدم جميع الشركات الكبيرة حلولها كأداة مراقبة العمليات التجارية.

أهمية مراقبة أنظمة الكمبيوتر

- مراقبة أنظمة الكمبيوتر مهمة مثل الأنظمة نفسها.

- تتيح المراقبة :

1. **الاستجابة الاستباقية.**
2. **أمن البيانات.**
3. **جمع البيانات.**
4. **ضمان الصحة العامة للنظام.**

- لا تقوم المراقبة بإصلاح المشكلات، لكنها تجعل الأنظمة أكثر استقرارًا وموثوقية.

أفضل أدوات مراقبة النظام

1- مراقب Sematext

مراقبة Sematext هي برنامج قوي لمراقبة الأنظمة يوفر رؤية شاملة وفورية لجميع عمليات النشر سواء على الخوادم المحلية أو السحابة .يمكنك الحصول على نظرة سريعة حول حالة صحة النظام من خلال مراقبة مركزية لـ التطبيقات، الخوادم، الحاويات، الأحداث، حزم البرمجيات، صور الحاويات، قواعد البيانات، العمليات، والمزيد.

المميزات

- **وكيل Sematext Agent خفيف جدًا، مما يجعله مناسبًا لأي بيئة تشغيل.**
- **يدعم أكثر من 100 تكامل مع إطارات العمل الشائعة مثل :**
  - **Apache Cassandra، MySQL، PostgreSQL، JVM، Elasticsearch، Solr، MongoDB وغيرها.**

التسعير

- **يوفر Sematext فترة تجريبية مجانية لمدة 14 يومًا.**
- **تتوفر ثلاث خطط تسعير:**
  - **الخطة الأساسية (Basic): مراقبة مجانية للبنية التحتية لما يصل إلى 3 خوادم.**

- الخطة القياسية :(Standard) بسعر 3.6دولار لكل خادم شهريًا.
- الخطة الاحترافية :(Pro) بسعر 5.76دولار لكل خادم شهريًا.

2- SolarWinds Server & Application Monitor

توفر SolarWindsمجموعة من أدوات إدارة الأنظمة التي تراقب التطبيقات، تجربة مستخدمي تطبيقات الويب، المضيفين الافتراضيين، الخوادم، أداء التخزين والموارد الأخرى، مما يمنح رؤية شاملة حول حالة وأداء النظام في كل من البيئات المحلية والسحابية.

الميزات

- لوحة تحكم موحدة لمراقبة التطبيقات والخوادم.
- تسريع وقت حل المشكلات من خلال تجميع البيانات المتنوعة وعرضها في رسوم بيانية.
- رؤية شاملة عبر جميع الطبقات التقنية لمراقبة الأداء، وقت التشغيل، السعة، واستهلاك الموارد.
- مراقبة مؤشرات الأداء ووقت التشغيل لضمان استقرار الأنظمة.

التسعير

- توفر SolarWindsنسخة تجريبية مجانية لمدة 30 يومًا مع جميع الميزات.
- تبدأ أسعار الاشتراك والترخيص الدائم من :
  - 1,622دولارًا لاشتراك يصل إلى 10عقد.
  - 2,995دولارًا للترخيص الدائم حتى 10عقد.

3- Atera

Ateraهي أداة مراقبة متاحة ضمن نظامين :SaaS

1. أتمتة الخدمات الاحترافية(PSA)
2. المراقبة والإدارة عن بُعد(RMM)

يستخدم مزودو الخدمات الإداريه (MSPs) وفرق تكنولوجيا المعلومات الحل المستند إلى الوكيل من Atera لمراقبة عدد غير محدود من الأجهزة والبرمجيات واستكشاف المشكلات وإصلاحها.

تتيح برمجيات RMM مراقبة الاتصالات البعيدة، إدارة التحديثات، تثبيت البرامج، تنظيم الاستجابة للحوادث، والمزيد.

المميزات

- مراقبة وتنبيهات فورية لموارد النظام، سلوك المستخدم، وتدفق حركة الشبكةIP/
- التعرف الفوري على الأجهزة غير المدارة
- تحديثات تلقائية للبرامج والتصحيحات الأمنية
- مهام إدارة وصيانة مضبوطة مسبقًا، بالإضافة إلى دعم البرمجة النصية المخصصة

التسعير

- توفر Ateraنسخة تجريبية مجانية لمدة 30 يومًا لجميع خطط الاشتراك.
- يتم تحديد الأسعار بناءً على عدد الفنيين وليس عدد الأجهزة، مما يوفر تكلفة ثابتة لكل فني شهريًا.
- أسعار الاشتراك السنوي (مع الخصومات) :
  - Pro: 79 دولارًا لكل فني شهريًا.
  - Growth: 119 دولارًا لكل فني شهريًا.
  - Power: 149 دولارًا لكل فني شهريًا.

- هناك بعض المتطلبات التي يجب مراعاتها عند اختيار برنامج مراقبة النظام:

1- دعم البيئات المعقدة.

2- الإشعارات والتنبيهات.

3- مستويات عالية من الأتمتة

4- إعداد التقارير

إدارة سطح المكتب

- طريقة لإدارة جميع أجهزة الحاسوب في المؤسسة بما في ذلك الحواسيب المكتبية والمحمولة والأجهزة اللوحية. **وغيرها من أجهزة الحوسبة للمستخدم النهائي.**

تعد إدارة أجهزة سطح المكتب جزءًا من المجال الأوسع **لإدارة الأنظمة**، والذي يشمل جميع أنظمة وخدمات تكنولوجيا المعلومات المستخدمة داخل المؤسسة.

- العمل:

مراقبة وصيانة ال، H.W and S.W.

- عند تنفيذها بشكل صحيح، تؤدي إلى:
  - **زيادة الإنتاجية**
  - **تحسين الأمان**
  - **مساعدة مسؤولي تكنولوجيا المعلومات في دعم الأجهزة، التطبيقات، والخدمات**

إدارة الخوادم

نهج لإدارة جميع عمليات المراقبة والصيانة المطلوبة لضمان تشغيل الخوادم بشكل موثوق وبأداء مثالي.

تشمل **إدارة الخوادم** أيضًا إدارة **الأجهزة، البرامج، الأمان، والنسخ الاحتياطي**، بهدف الحفاظ على **بيئة تكنولوجيا المعلومات فعالة وقيد التشغيل باستمرار.**

- العمل:

مراقبة وصيانة السيرفرات.

عند تنفيذها بشكل صحيح، تؤدي إلى:

- **تقليل تباطؤ وتعطل الخوادم مع زيادة موثوقيتها**

- **تأمين وحماية بيئات الخوادم**

الإدارة عن بُعد

الإدارة عن بُعد تشير إلى أي طريقة للتحكم في جهاز كمبيوتر من موقع بعيد. أصبحت **البرمجيات التي تتيح الإدارة عن بُعد** شائعة بشكل متزايد، وغالبًا ما تُستخدم عندما يكون من الصعب أو غير العملي التواجد **فعليًا** بالقرب من النظام لاستخدامه.

- **الإدارة عن بُعد** هي نهج يُستخدم للتحكم في **نظام كمبيوتر أو شبكة أو تطبيق أو جميعها** من موقع بعيد.
- ببساطة، تعني **الإدارة عن بُعد** أي طريقة للتحكم في **جهاز كمبيوتر من مكان بعيد**.
- قد يكون الموقع البعيد **جهاز كمبيوتر في الغرفة المجاورة أو على الجانب الآخر من العالم**.

المتطلبات اللازمة لتنفيذ الإدارة عن بُعد:

1. **اتصال بالإنترنت**
2. **اتصال بالشبكة**
3. **عنوانIP**
4. **مودم الاتصال الهاتفي(Dial-up Modem)**

المحاضرة الثالثه

مراقبة النظام

&

الاختبار الشامل (من البداية إلى النهاية)

ماورد بالمحاضره:

أداة مراقبه:real time environment monitoring and alarm system.

هي منهجية لتطوير البرمجيات،End-to-end System:

- فوائد الصيانه:

1- فحص البرامج داخل النظام.

2- للتحقق من صحة النظام.

3- للتحقق من الأنظمة الفرعيه أنها تعمل بالشكل المُتوقع.

4- إكتشاف الأخطاء وإصلاحها.

5- تقليل التكاليف.

Process of end to end Testing:

1- End-to-end design

2- End-to-end component (objective)

3- End-to-end development

إما أن يكون يدوي أو أو آلي:

يدوي: عن طريق كتابة أكواد.

آلي: عن طريق أدوات.

المحتويات

المراقبة الفورية

- ما هي المراقبة الفورية؟
- فوائد المراقبة الفورية
- البرامج المستخدمة في المراقبة الفورية

الاختبار الشامل (من البداية إلى النهاية)

- **ما هو الاختبار الشامل؟**
- **فوائد الاختبار الشامل**
- **تحديات الاختبار الشامل**
- **عملية الاختبار الشامل**
- **خطوات الاختبار الشامل**
- **أدوات الاختبار الشامل**

المراقبة الفورية(في الوقت):

يمكن أن تلعب أمان الشبكة وأداؤها دورًا مهمًا في النجاح العام لشركتك. لهذا السبب، يجب على كل شركة، خاصة تلك التي تعمل في التجارة الإلكترونية، مراقبة شبكاتها بشكل متكرر لضمان أن كل شيء يعمل بسلاسة.

المراقبة الفورية

- **المراقبة الفورية هي عملية جمع وتخزين مقاييس الأداء للبيانات أثناء انتقالها عبر شبكتك، تتضمن الاستقصاء (Polling) وتدفق البيانات من أجهزة البنية التحتية بحيث تعرف كيف تعمل شبكاتك، تطبيقاتك، وخدماتك.**
- **المراقبة الفورية هي استخدام التطبيقات والأدوات التي تتبع وتسجل لقطات مستمرة لأداء شبكتك العام.**
- **تستخدم المؤسسات المراقبة الفورية لتتبع نشاط الشبكة، تحسين أمان الشبكة، وتحديد المشكلات المحتملة فور ظهورها.**
- **يمكن لكل شركة، بغض النظر عن حجمها، الاستفادة من مراقبة شبكتها في الوقت الفعلي.**

تستخدم المؤسسات المراقبة الفورية لـ:

- **تتبع نشاط الشبكة**
- **تحسين أمان الشبكة**

- تحديد المشكلات المحتملة فور ظهورها

فوائد المراقبة الفورية

1- أمان الشبكة

- يجب أن يكون أمان الشبكة أولوية قصوى لأي شركة. إن مراقبة شبكتك في الوقت الفعلي هي طريقة رائعة لدعم الامتثال الأمني.
- يمكن أن تساعد المراقبة الفورية قسم تكنولوجيا المعلومات لديك في تحديد وحل المشكلات الأمنية فور ظهورها.
- تشمل هذه المشكلات حركة المرور غير العادية أو المشبوهة، الطلبات أو الأجهزة غير المصرح بها، التهديدات الإلكترونية، أو أي سلوك ضار آخر على شبكتك.

2- أداء الشبكة

- يمكن أن يكون أداء شبكتك مرتبطًا مباشرة بنجاح عملك.
- على سبيل المثال، إذا كنت تدير نشاطًا تجاريًا في التجارة الإلكترونية، فستحتاج إلى تحسين خوادمك لتجنب مشكلات مثل التوقف، التحميل الزائد على النطاق الترددي، وأوقات التحميل الطويلة، يمكن أن تكشف مراقبة شبكتك في الوقت الفعلي عن رؤى قابلة للتنفيذ حول الأعطال وعدم كفاءة الأداء التي تحتاج إلى معالجتها.

عناصر أداء الشبكة التي يمكن مراقبتها:

- استخدام النطاق الترددي :إذا كنت ترسل أو تستقبل بيانات أكثر مما خططت له، فقد يتعرض خط الشبكة لديك للتحميل الزائد، مما قد يؤثر على الأداء العام.
- التأخير :هذا هو الوقت بين الطلب واستجابة البيانات. التأخير أكثر أهمية في بعض الحالات عن غيرها؛ على سبيل المثال، يكون ذا أهمية كبيرة عند لعب لعبة في الوقت الفعلي.
- توفر الشبكة/الوقت الفعلي :(Uptime) معرفة الوقت الفعلي الذي تكون فيه شبكتك متاحة يسمح لك بالإعلان عن اتفاقية مستوى الخدمة (SLA) بثقة

- السرعة :ستختلف سرعة شبكتك في أي وقت معين. تعد الرؤية في السرعة التي تتلقاها مقابل السرعة المتوقعة أمرًا مهمًا للحفاظ على أداء شبكة جيد.

3- إنتاجية الموظفين

- يمكن أن تؤدي مراقبة شبكتك إلى زيادة إنتاجية الموظفين.
- على سبيل المثال، يمكن أن يساعد استخدام المراقبة الفورية لتحسين أداء الشبكة مما يتيح لفريقك في إرسال رسائل البريد الإلكتروني الخاصة بالشركة، العمل على المشاريع، والتعاون مع الزملاء بكفاءة أكبر.
- يمكنك أيضًا استخدام المراقبة الفورية لتتبع نقل بيانات الموظفين وحماية أي معلومات حساسة قد يعملون عليها.

4- توفير التكاليف

- يمكن أن توفر لك المعرفة الحديثة بكيفية استخدام شبكتك لحفظ المال في نهاية المطاف.
- بدلاً من الإنفاق الزائد على البرامج المتقدمة أو سرعات الموقع غير الضرورية، يمكنك الحصول على رؤية شاملة للتكنولوجيا والدعم الذي تحتاجه بالضبط.
- يمكن أن تساعدك الشبكة المحسنة أيضًا في تحقيق الأرباح، خاصةً إذا كنت تعمل في التجارة الإلكترونية.

البرنامج المستخدم في المراقبة الفورية:

- REMAS أنظمة المراقبة البيئية والتنبيه في الوقت الفعلي.
- يعد REMAS نظامًا قويًا لإدارة البيانات البيئية في الوقت الفعلي يقيس ويسجل ويحلل البيانات مع التنبيه والعرض على الموقع أو عبر الويب.

الاختبار الشامل(End-to-End Testing)

ما هو الاختبار الشامل؟

- الاختبار الشامل (E2E) هو طريقة اختبار برمجية تتضمن اختبار سير عمل التطبيق من البداية إلى النهاية، يهدف هذا الأسلوب إلى تكرار سيناريوهات المستخدم الحقيقية للتحقق من تكامل النظام وسلامة البيانات.

- يُستخدم الاختبار الشامل في دورة حياة تطوير البرمجيات (SDLC) لاختبار وظائف وأداء التطبيق في ظروف شبيهة بالمنتج الفعلي، الهدف هو محاكاة سيناريو المستخدم الحقيقي من البداية إلى النهاية.
- لا يقتصر اكتمال هذا الاختبار على التحقق من النظام قيد الاختبار فقط، بل يضمن أيضًا أن الأنظمة الفرعية تعمل وتتفاعل كما هو متوقع.

فوائد الاختبار الشامل:

- اختبار وظائف وأداء التطبيق.
- التحقق من سلامة النظام.
- ضمان عمل الأنظمة الفرعية كما هو متوقع.
- اكتشاف المشكلات وإصلاحها بشكل أسرع.
- تقليل جهود وتكاليف الاختبار.
- اكتشاف الأخطاء وزيادة إنتاجية التطبيق.

تحديات الاختبار الشامل:

الوصول إلى بيئة الاختبار: من السهل اختبار التطبيقات في بيئات التطوير. ومع ذلك، يجب اختبار كل تطبيق في بيئات العملاء أو الإنتاج. من المحتمل أن تكون بيئات الإنتاج غير متاحة دائمًا للاختبار. يجب على المختبرين تثبيت الوكلاء المحليين وتسجيل الدخول إلى الأجهزة الافتراضية حتى عندما تكون متاحة. كما يجب عليهم الاستعداد للمشكلات مثل تحديثات النظام التي قد تعيق تنفيذ الاختبار ومنع حدوثها.

إنشاء سير العمل: لفحص سير عمل التطبيق، يجب تشغيل حالات الاختبار في مجموعة اختبار E2E بتسلسل معين. يجب أن يتطابق هذا التسلسل مع مسار المستخدم النهائي أثناء تنقله داخل التطبيق. يمكن أن يكون إنشاء مجموعات اختبار تتوافق مع هذا المسار أمرًا مرهقًا، خاصةً لأنها تتطلب عادةً إنشاء وتشغيل آلاف الاختبارات.

- يستغرق وقتًا طويلاً.
- يتطلب فهمًا جيدًا لأهداف المستخدم.

عملية الاختبار من البداية إلى النهاية

- هنا نظرة عامة على عملية الاختبار من البداية إلى النهاية.

1. المتطلبات
    - التقاط المتطلبات
    - التوثيق
2. تصميم الاختبار من البداية إلى النهاية(E2E Design)
    - تصميم المكونات
    - تصميمE2E
3. تصميم المكونات
    - تصميم المكونات والاختبار
4. التطوير
    - ترميز التطوير والتصميم
5. اختبارE2E
    - إعداد البيئة للاختبار من البداية إلى النهاية
    - تصميم الاختبار والتنفيذ

خطوات تنفيذ الاختبار الشامل:

1. تحليل المتطلبات وفهم كيفية عمل التطبيق في كل جانب.
2. إعداد بيئة اختبار تتماشى مع جميع المتطلبات.
3. تحليل متطلبات البرامج والأجهزة.
4. تحديد كيفية استجابة كل نظام.

5. تحديد طرق الاختبار المطلوبة لاختبار هذه الاستجابات، بما في ذلك الأوصاف الواضحة للمعايير (اللغة، الأدوات، إلخ).
6. تصميم حالات الاختبار.
7. تشغيل الاختبارات، ودراسة النتائج وحفظها.

أدوات الاختبار الشامل:

- testRigor:
  - رائدة في مجال الاختبار الشامل.
  - تتيح إنشاء اختبارات بدون كود عبر واجهات الويب، التطبيقات الأصلية والهجينة، المتصفحات المحمولة، وواجهات API.
  - تدعم اختبار رسائل البريد الإلكتروني والرسائل النصية، بالإضافة إلى اختبار الملفات مثل XLS. و DOC. و PDF. بسهولة.
- خصائص testRigor:
  - تدعم كتابة الاختبارات بلغة إنجليزية بسيطة.
  - توفر تغطية عبر الويب، الجوال، وواجهات البرمجة.
  - تقلل من صيانة الاختبار بنسبة تصل إلى 99.5٪.
  - آمنة.
  - يمكنها تشغيل آلاف الاختبارات والحصول على النتائج في أقل من 30 دقيقة.

المحاضرة الرابعه

تشغيل وإيقاف تشغيل النظام والإقلاع الذاتي

المحتويات

- تشغيل النظام
- إيقاف تشغيل النظام

الإقلاع الذاتي (Bootstrapping)

- الإقلاع الذاتي
- تسلسل الإقلاع الذاتي في نظام التشغيل (خطوات الإقلاع الذاتي)
- عمليات الإقلاع الذاتي
- عمليات الإقلاع الذاتي في لينكس
- إعادة التشغيل

تشغيل وإيقاف تشغيل النظام

يصف هذا الفصل إجراءات تشغيل وإيقاف تشغيل النظام، وإدخال النظام إلى المستويات الافتراضية المختلفة للتشغيل، وكيفية إنشاء مستويات تشغيل مخصصة.

في لينكس، تحدد مستويات التشغيل (Runlevels) كيفية بدء تشغيل النظام. بعد الإقلاع، يبدأ النظام كما هو محدد في الملف /etc/inittab في السطر initdefault. كبديل، يمكن تحديد مستوى التشغيل أثناء التمهيد (على سبيل المثال، في موجه الإقلاع الذاتي). أي معلمات لا يتم تقييمها مباشرةً بواسطة النواة يتم تمريرها إلى init.

لتغيير مستويات التشغيل أثناء تشغيل النظام، أدخل init متبوعًا بالرقم المناسب كمُعامل. يُسمح فقط لمسؤول النظام بتنفيذ هذا الإجراء.

- init 1) أو shutdown now) يؤدي إلى تحويل النظام إلى وضع المستخدم الفردي(Single User Mode) ، والذي يُستخدم للصيانة والإدارة.
- بعد الانتهاء من العمل، يمكن للمسؤول العودة إلى مستوى التشغيل العادي بإدخال init 3، مما يؤدي إلى تشغيل جميع البرامج الأساسية والسماح للمستخدمين العاديين بتسجيل الدخول واستخدام النظام.

- init 0 أو shutdown -h now يؤدي إلى إيقاف تشغيل النظام
- init 6 أو shutdown -r now يؤدي إلى إيقاف تشغيل النظام مع إعادة تشغيله.

تشغيل النظام:

تشغيل النظام يشير إلى الإجراء الخاص ببدء تشغيل برامج الكمبيوتر، وتحديدًا نظام التشغيل والبرامج الأخرى. لا يشير تشغيل النظام إلى تثبيت النظام لأول مرة.

إيقاف تشغيل النظام:

إيقاف التشغيل يشير إلى إغلاق جميع البرامج استعدادًا لإيقاف تشغيل الكمبيوتر .يكون نظام التشغيل هو آخر برنامج يتم إغلاقه كجزء من عملية إيقاف التشغيل.

الإقلاع الذاتي(Bootstrapping) :

- يشير مصطلح الإقلاع الذاتي (bootstrap) إلى تحميل وتشغيل برنامج داخل الكمبيوتر باستخدام برنامج أولي أصغر لتحميل البرنامج المطلوب، والذي يكون عادةً نظام التشغيل.
- عملية الإقلاع الذاتي (Booting) هي العملية التي يتم فيها تشغيل الكمبيوتر، وخاصة تشغيل البرمجيات.
- تتضمن هذه العملية عدة مراحل متسلسلة، حيث يقوم كل برنامج أصغر بتحميل وتشغيل برنامج أكبر وأكثر تعقيدًا في المرحلة التالية.

تسلسل الإقلاع الذاتي في نظام التشغيل (خطوات الإقلاع الذاتي)

عند تشغيل الكمبيوتر، يتم تزويد جميع مكونات الأجهزة بالطاقة ويتم تهيئتها. بعد ذلك، يمر النظام بسلسلة من 6 خطوات:

1. تحميل الBIOS : يتم تحميل مجموعة صغيرة من التعليمات المخزنة في ذاكرة ROM إلى ذاكرة الكمبيوتر، ثم يقوم المعالج بتنفيذ هذه التعليمات.

2. اختبار التشغيل الذاتي (POST): يقوم BIOS بفحص جميع الأجهزة المتصلة بالنظام للتأكد من أنها تعمل بشكل صحيح. إذا تم اكتشاف مشكلة، يتم تنبيه المستخدم عن طريق إشارات صوتية (POST Beeps) أو رسائل خطأ على الشاشة.

3. تحميل نظام التشغيل:

   - بعد نجاح POST، يقرأ BIOS تسلسل الإقلاع المخزن في CMOS.
   - بناءً على هذا التسلسل، يبحث عن سجل التمهيد الرئيسي (MBR) في أحد أجهزة الإقلاع مثل القرص الصلب أو الفلاشة أو الـCD-ROM.
   - إذا لم يتم العثور على MBR، يتوقف النظام ويعرض رسالة "لا يوجد جهاز إقلاع." (No Boot Device Found)
   - إذا تم العثور على MBR، يقوم BIOS بتحميل محمل الإقلاع (Boot Loader) ، الذي يقوم في النهاية بتحميل نظام التشغيل.

4. تهيئة النظام: بعد تحميل نظام التشغيل، يتم تحميل برامج تشغيل الأجهزة إلى الذاكرة لضمان عمل الأجهزة بشكل صحيح.

5. تحميل أدوات النظام: يتم تحميل أدوات النظام مثل مكافحات الفيروسات، التحكم في الأقراص، إلخ.

6. مصادقة المستخدم: إذا كان هناك نظام مصادقة، يطلب النظام من المستخدم إدخال بيانات الاعتماد. عند إدخالها بشكل صحيح، يتم تشغيل واجهة المستخدم الرسومية (GUI) أو واجهة الأوامر النصية (CLI).

عمليات الإقلاع الذاتي:

1. البحث عن كود الإقلاع الذاتي (Bootstrapping Code) وتحميله وتشغيله.
2. البحث عن نواة نظام التشغيل (Kernel) وتحميلها وتشغيلها.
3. تشغيل سكربتات بدء التشغيل.
4. إدارة عمليات النظام والانتقالات بين الحالات المختلفة.

عمليات الأقلاع في لينكس

1. تشغيل الجهاز.

2. تحميل الـ BIOS من ذاكرة NVRAM ذاكرة غير متطايرة تحتفظ بالبيانات حتى عند انقطاع الطاقة.

3. فحص الأجهزة(Hardware Probe)

4. اختيار جهاز الإقلاع (قرص صلب، شبكة، إلخ)

5. تحميل النواة :(Kernel Loading)

   - النواة هي المكون المركزي لنظام التشغيل الذي يدير عمليات الكمبيوتر والأجهزة.
   - يتم تحميل النواة كملف صورة مضغوط zImage) أو (bzImage إلى ذاكرة RAM.
   - يتم تحديد النواة من خلال الأمر uname -r في لينكس.

6. تحديد نوع النواة التي سيتم تشغيلها :

   - النواة الأحادية :(Monolithic Kernel) تتضمن عددًا كبيرًا من الأكواد وتتميز بأداء عال.
   - النواة الصغيرة :(Micro Kernel) تحتوي على ذاكرة افتراضية، تحتاج إلى مساحة أقل، وأكثر استقرارًا.
   - النواة الهجينة :(Hybrid Kernel) مزيج بين النواة الأحادية والصغيرة، وتتميز بالسرعة.

7. تحميل محمل الإقلاع :(Boot Loader)

   - برنامج صغير مسؤول عن تحميل نظام التشغيل.
   - أمثلة على أوامر الإقلاع /boot/Vmli :، .root=/dev/sdx

8. التعرف على نظام :EFI نظام مستقل عن نظام التشغيل، ويعمل كمساحة تخزين لمحملات الإقلاع والتطبيقات والتعريفات.

9. إنشاء بنية بيانات النواة.

10. بدء تشغيل initأو :systemd

    - systemdهو مدير أنظمة وخدمات لأنظمة لينكس.
    - يعمل كأول عملية عند الإقلاع، ويتولى تشغيل الخدمات والمساحات الخاصة بالمستخدمين.

11. تنفيذ سكربتات بدء التشغيل.

12. تشغيل النظام بالكامل.

إعادة التشغيل(Rebooting)

إعادة التشغيل تعني تشغيل الكمبيوتر مرة أخرى باستخدام الأجهزة (مثل زر الطاقة) بدلاً من البرمجيات .قد يكون ذلك ضروريًا بعد تثبيت برامج جديدة أو تحديثات نظام التشغيل، أو لاستعادة التشغيل بعد خطأ ما، أو إعادة تهيئة الأجهزة والتعريفات.

المحاضرة الخامسه

حسابات المستخدم

المحتويات

- حسابات المستخدم
- إنشاء / إزالة حسابات المستخدم(Windows)
- إنشاء / إزالة حسابات المستخدم(Linux)
- إدارة حسابات المستخدم
- وظائف إدارة حسابات المستخدم
- أدوات إدارة حسابات المستخدم

حسابات المستخدم

- حساب المستخدم هو هوية يتم إنشاؤها لشخص في جهاز كمبيوتر أو نظام حوسبة.
- يمكن أيضًا إنشاء حسابات المستخدم للكيانات الآلية، مثل :
  - حسابات الخدمات لتشغيل البرامج.
  - حسابات النظام لتخزين ملفات النظام والعمليات.

- حسابات المسؤول لإدارة النظام

- أقرب مثال على حساب المستخدم هو حساب الإنترنت أو البريد الإلكتروني الخاص بك.

تخزين معلومات الحساب:

- يتم استخدام حساب المستخدم كموقع على خادم الشبكة لتخزين :
  - اسم مستخدم الكمبيوتر.
  - كلمة المرور.
  - معلومات أخرى.
- يسمح حساب المستخدم أو يمنع المستخدم من :
  - الاتصال بالشبكة.
  - الوصول إلى كمبيوتر آخر.
  - مشاركة الملفات والموارد.

أنواع حسابات المستخدم:

- الحسابات العادية(Standard accounts) :
  - تستخدم للمهام اليومية العادية.
  - يمكن للمستخدم تشغيل البرامج وتخصيص سطح المكتب.
- حسابات المسؤول(Administrator accounts) :
  - حسابات خاصة تُستخدم لتغيير إعدادات النظام أو إدارة حسابات المستخدمين الآخرين.
  - تمتلك صلاحيات كاملة للتحكم في النظام.
  - يجب أن يحتوي كل جهاز كمبيوتر على حساب مسؤول واحد على الأقل.

إنشاء حسابات المستخدم(Windows)

إنشاء حساب مستخدم محلي

1. حدد ابدأ <الإعدادات <الحسابات ثم العائلة والمستخدمون الآخرون.
2. بجانب إضافة مستخدم آخر، حدد إضافة حساب.
3. حدد ليس لدي معلومات تسجيل دخول لهذا الشخص، ثم إضافة مستخدم بدون حساب Microsoft.
4. أدخل اسم المستخدم وكلمة المرور أو استخدم أسئلة الأمان، ثم اضغط التالي.

إنشاء حساب مسؤول

1. حدد ابدأ <الإعدادات <الحسابات.
2. ضمن العائلة والمستخدمون الآخرون، اختر اسم الحساب ثم تغيير نوع الحساب.
3. حدد مسؤول ثم اضغط موافق.
4. قم بتسجيل الدخول باستخدام حساب المسؤول الجديد.

إنشاء حسابات مستخدمين متعددة

1. حدد ابدأ <الإعدادات <الحسابات.
2. ضمن العائلة والمستخدمون الآخرون، اختر إدارة حساب آخر.
3. حدد إضافة مستخدم جديد في إعدادات الكمبيوتر.

إزالة حساب مستخدم

1. حدد ابدأ <الإعدادات <الحسابات <العائلة والمستخدمون الآخرون.
2. اختر الحساب المطلوب إزالته ثم اضغط على إزالة.
3. لاحظ أن هذا لا يحذف حساب Microsoft الخاص بالمستخدم، بل يزيل فقط بيانات تسجيل الدخول من جهاز الكمبيوتر.

إنشاء حسابات المستخدم(Linux)

ملفات الحسابات في لينكس

- ملف /etc/shadow: يخزن كلمات المرور المشفرة مع خصائص إضافية لكلمات المرور.
- ملف /etc/passwd: يخزن معلومات الحساب الضرورية لتسجيل الدخول، مثل :
  - معرف المستخدم(UID)
  - معرف المجموعة(GID)
  - الدليل الرئيسي(Home Directory)
  - واجهه تقوم بتفسير الاوامر من المستخدم وتحويلها الى أوامر قابله للتنفيذ بواسطة نواة النظام(Shell)

إنشاء حساب مستخدم محلي

1. لإنشاء حساب جديد، استخدم الأمر useradd متبوعًا باسم المستخدم.
2. على سبيل المثال، لإنشاء مستخدم باسم Mohammed، استخدم :
3. sudo useradd Mohammed
4. يضيف هذا الأمر إدخالًا في الملفات /etc/passwd و/etc/shadow.
5. لضبط كلمة مرور المستخدم الجديد :
6. sudo passwd Mohammed

إنشاء حساب مسؤول

1. لا يوجد فرق تقني بين المستخدمين العاديين ومستخدمي النظام، مستخدمي النظام تنشأ عند تثبيت النظام.
2. لإنشاء حساب نظام، استخدم الخيار r-:
3. sudo useradd -r Mohammed

إنشاء حسابات مستخدمين متعددة

1. عند إنشاء مستخدم جديد باستخدام useradd، لا يتم إنشاء الدليل الرئيسي تلقائيًا.

2. نستخدم m- لانشاء مستخدم دليل رئيسي:

3. sudo useradd -m Mohammed

إزالة حساب مستخدم

1. لحذف حساب مستخدم، استخدم الأمر :userdel

2. sudo userdel Mohammed

3. لحذف الحساب وجميع ملفاته، استخدم الخيار :r-

4. sudo userdel -r Mohammed

إدارة حسابات المستخدم

- **يصف إدارة المستخدم قدرة المسؤولين على إدارة :**
  - الأجهزة والأنظمة.
  - التطبيقات وأنظمة التخزين.
  - الشبكات وخدمات الحوسبة السحابية
  - وصول المستخدمين إلى الموارد المختلفة.
- **تشمل إدارة الحسابات :**
  - تحديد المستخدمين الذين يمكنهم الوصول إلى الملفات والمجلدات.
  - منح بيانات الاعتماد المناسبة لكل مستخدم.

وظائف إدارة حسابات المستخدم

- منع الوصول غير المصرح به إلى البنية التحتية، التطبيقات، والبيانات.
- تخزين تفاصيل المستخدم.

- توفير آلية تسجيل دخول مناسبة للمستخدمين.
- السماح للمستخدمين بإعادة تعيين كلمات المرور.

أدوات إدارة حسابات المستخدم

Access Rights Manager (ARM)

- يعمل على أتمتة إدارة حسابات المستخدم، مما يساعد في تحسين عمليات تكنولوجيا المعلومات وتوفير الموارد من خلال :
  - إنشاء حسابات المستخدم.
  - تعديل حسابات المستخدم.
  - حذف حسابات المستخدم.

المحاضره السادسه

تصحيح الأخطاء(Debugging)

المحتويات

1. معنى تصحيح الأخطاء.
2. خطوات تصحيح الأخطاء.
3. استراتيجيات تصحيح الأخطاء.
4. أنواع تصحيح الأخطاء.

معنى تصحيح الأخطاء:

- هو عملية العثور على الأخطاء وإصلاحها في كود المصدر لأي برنامج.

- تصحيح الأخطاء هو تقنية مراقبة كود البرمجيات واكتشاف وإزالة الأخطاء المحتملة، الثغرات، أو العيوب التي قد تتسبب في سلوك غير متوقع أو تعطل التطبيق.
- يلعب تصحيح الأخطاء دورًا حاسمًا في دورة حياة تطوير البرمجيات.

تصحيح الأخطاء في تطوير البرمجيات:

- تبدأ عملية تصحيح الأخطاء عندما يحدد المطور خطأ في الكود البرمجي ويكون قادرًا على إعادة إنتاجه.
- يعد تصحيح الأخطاء جزءًا من عملية اختبار البرمجيات وجزءًا أساسيًا من دورة حياة تطوير البرمجيات بالكامل.

تصحيح الأخطاء في تطوير الأجهزة:

- تتضمن عملية تصحيح الأخطاء في الأجهزة البحث عن المكونات غير المثبتة أو غير المهيأة بشكل صحيح.
- على سبيل المثال، قد يقوم المهندس بتشغيل اختبار اتصال JTAG لتصحيح الأخطاء في دائرة متكاملة.

خطوات تصحيح الأخطاء:

1. تحديد الخطأ.
2. عزل مصدر الخطأ.
3. تحديد الحل لإصلاح الخطأ.
4. تطبيق الحل واختباره.

لماذا يعد تصحيح الأخطاء مهمًا؟

- تصحيح الأخطاء أمر ضروري لفهم سبب سوء سلوك نظام التشغيل، التطبيق أو البرنامج.
- حتى مع اتباع معايير ترميز موحدة، من المحتمل أن يحتوي أي برنامج جديد على أخطاء.

- في كثير من الحالات، قد يستغرق تصحيح الأخطاء وقتًا أطول من كتابة البرنامج نفسه.
- عادةً، يتم العثور على الأخطاء في مكونات البرامج الأكثر استخدامًا وإصلاحها أولاً.

تصحيح الأخطاء & الاختبار:

- الاختبار وتصحيح الأخطاء عمليتان مكملتان لبعضهما البعض.
- الغرض من الاختبار هو تحديد ما يحدث عندما يكون هناك خطأ في كود المصدر.
- الغرض من تصحيح الأخطاء هو تحديد موقع الخطأ وإصلاحه.
- عملية الاختبار لا تساعد المطور في معرفة الخطأ البرمجي بالتحديد، لكنها تكشف فقط تأثير الخطأ على البرنامج.
- بمجرد تحديد الخطأ، يساعد تصحيح الأخطاء في تحديد سببه حتى يمكن إصلاحه.

استراتيجيات تصحيح الأخطاء:

تشمل استراتيجيات تصحيح الأخطاء ما يلي:

- التحليل الثابت :(Static Analysis) يقوم المطور بفحص الكود دون تشغيل البرنامج.
- تصحيح الأخطاء عبر الطباعة :(Print Debugging) يراقب المطور المخرجات الفورية أو المسجلة لمعرفة تدفق التنفيذ.
- التصحيح عن بُعد :(Remote Debugging) يتم تشغيل أداة التصحيح على نظام مختلف عن النظام الذي يتم تصحيحه.
- التصحيح بعد التوقف :(Post-mortem Debugging) يتوقف المطور لتصحيح الأخطاء فقط عند حدوث استثناءات قاتلة

أدوات تصحيح الأخطاء:

- المصحح البرمجي (Debugger) هو أداة برمجية تساعد في عملية تطوير البرمجيات من خلال تحديد أخطاء الكود البرمجي في مراحل مختلفة من تطوير نظام التشغيل أو التطبيق.

- بعض المصححات البرمجية تقوم بتحليل عملية الاختبار لمعرفة :
  - ما هي الأسطر البرمجية التي لم يتم تنفيذها
  - توفير أدوات محاكاة تسمح للمبرمج بمحاكاة سلوك التطبيق على نظام تشغيل أو جهاز معين.

أنواع الأخطاء:

1- أخطاء البناء والتجميع(Build and Compile-Time Errors)

- تحدث في مرحلة التطوير عندما يتم بناء الكود البرمجي.
- يتم اكتشاف هذه الأخطاء بواسطة المترجم أو المفسر أثناء تحويل الكود المصدر إلى ملف تنفيذي.
- تمنع هذه الأخطاء تشغيل التطبيق.
- غالبًا ما تكون بسبب أخطاء في بناء الجملة(Syntax Errors) ، مثل :
  - نسيان الفاصلة المنقوطة(;)
  - عدم العثور على الفئة أو المكتبة المطلوبة

2- أخطاء وقت التشغيل(Runtime Errors)

- لا يمكن اكتشافها إلا أثناء تشغيل التطبيق.
- تحدث عندما يكون الكود البرمجي خاليًا من الأخطاء أثناء التجميع، لكن يحتوي على مشاكل تؤثر على التشغيل.
- غالبًا ما تعتمد على :
  - مدخلات المستخدم.
  - البيئة التشغيلية.
- يمكن معالجتها باستخدام كتل try-catch وتسجيل رسائل الخطأ بشكل صحيح.

3- أخطاء المنطق(Logic Errors)

- تحدث بعد نجاح تجميع البرنامج وتشغيله.
- لا تؤدي إلى تعطل البرنامج، لكنها تعطي نتائج غير صحيحة.
- لا يمكن اكتشاف هذه الأخطاء باستخدام كتلtry-catch.
- تُعرف أيضًا بـ الأخطاء الدلالية(Semantic Errors) ، وتحدث بسبب منطق برمجي غير صحيح أثناء تطوير التطبيق.

أنواع تصحيح الأخطاء:

1- التصحيح التفاعلي(Reactive Debugging)

- يشير إلى أي عملية تصحيح تتم بعد ظهور الخطأ.
- يتم استخدامه لتقليل أخطاء وقت التشغيل والأخطاء المنطقية.

2- التصحيح الاستباقي(Preemptive Debugging)

- يتضمن كتابة كود برمجي إضافي لا يؤثر على وظيفة البرنامج ولكنه يساعد المطورين في اكتشاف الأخطاء مبكرًا أو تصحيحها بسهولة عند حدوثها.

التعافي من الكوارث(Disaster Recovery - DR)

- التعافي من الكوارث (DR) هو عملية حاسمة تساعد المؤسسات في النجاة والتعافي في حالة حدوث كارثة مثل :
  - كارثة طبيعية.
  - فقدان البيانات غير المقصود.
  - هجوم إلكتروني ضار.

خطة التعافي من الكوارث:

- تساعد خطة التعافي من الكوارث المؤسسة في الاستجابة للكوارث واتخاذ التدابير اللازمة لمنع الأضرار واستعادة العمليات بسرعة.

- يشمل التعافي من الكوارث في تكنولوجيا المعلومات (IT DR) التركيز على :
  - تقليل وقت تعطل الخوادم.
  - استعادة قواعد البيانات وأجهزة الموظفين.
  - إعادة تشغيل الأنظمة الحيوية بسرعة.

المحاضرة السابعة

التعافي من الكوارث(Disaster Recovery - DR)

المحتويات

1. التعافي من الكوارث(DR)
2. خطة التعافي من الكوارث
3. أهمية التعافي من الكوارث
4. طرق التعافي من الكوارث

التعافي من الكوارث(DR)

- التعافي من الكوارث (DR) هو عملية حيوية تساعد المؤسسات على البقاء والتعافي في حالة وقوع كارثة، سواء كانت:
  - كارثة طبيعية.
  - فقدان البيانات عن طريق الخطأ.
  - هجوم إلكتروني خبيث.
- تتيح خطة التعافي من كوارث تكنولوجيا المعلومات (IT DR Plan) للمؤسسة:
  - تحديد الأولويات والتركيز على الأصول والمخاطر.

- وضع استراتيجية لحماية البيانات.
- تحديد أفضل الطرق لاستعادة العمليات الطبيعية.

خطة التعافي من الكوارث(Disaster Recovery Plan - DRP)

- خطة التعافي من الكوارث هي وثيقة تساعد المؤسسة على الاستجابة للكوارث واتخاذ إجراءات للحد من الأضرار واستعادة العمليات بسرعة.
- يركز التعافي من كوارث تكنولوجيا المعلومات على الجوانب التقنية، مثل :
  - تقليل وقت تعطل الخوادم.
  - استعادة قواعد البيانات وأجهزة العمل.
  - إعادة تشغيل الأنظمة الحيوية.

الهيكل النموذجي لخطةDR :

1. الأهداف :تحديد الحد الأقصى للوقت المسموح لتعطل الأنظمة الحيوية، والحد الأقصى لخسارة البيانات المقبولة.
2. الموظفون المسؤولون :تحديد من المسؤول عن تنفيذ خطة التعافي من الكوارث.
3. جرد الأصول التقنية :يشمل الأجهزة والبرمجيات، وأهميتها، وما إذا كانت مملوكة أو مستأجرة أو جزءًا من خدمة.
4. إجراءات النسخ الاحتياطي :تحديد كيفية ومكان تخزين البيانات الاحتياطية، وكيفية استعادتها عند الحاجة.
5. إجراءات الاستجابة للطوارئ :تشمل الاستجابة الفورية للحد من الأضرار، وتنفيذ نسخ احتياطية أخيرة، والتعامل مع تهديدات الأمن السيبراني.
6. مواقع التعافي من الكوارث :يجب أن تتضمن خطة DR القوية موقع استرداد كوارث ساخن(Hot DR Site) ، وهو مركز بيانات بديل في موقع بعيد يحتوي على نُسخ مكررة من الأنظمة الحيوية والبيانات المحدثة بانتظام.

الهيكل النموذجي لخطة استعادة الكوارث

1. تجميع الخطة (Assemble Plan)
   - إعداد وتجميع خطة استعادة الكوارث.
2. تحديد النطاق (Identify Scope)
   - تحديد نطاق الخطة، مثل الأنظمة والبيانات والخدمات التي تشملها.
3. تعيين جهات الاتصال الطارئة (Appoint Emergency Contacts)
   - تحديد وتسجيل جهات الاتصال الضرورية في حالة الطوارئ.
4. تعيين فريق استعادة الكوارث (Designate Disaster Recovery Team)
   - اختيار الفريق المسؤول عن تنفيذ الخطة أثناء الطوارئ.
5. تحديد الأدوار والمسؤوليات (Assign Roles & Responsibilities)
   - توزيع المهام بين أعضاء الفريق وفقًا لخبراتهم.
6. استعادة وظائف التكنولوجيا (Restore Technology Functionality)
   - إعادة تشغيل واستعادة الأنظمة التقنية المتضررة.
7. تحديد مواقع البيانات والنسخ الاحتياطية (Data & Back Ups Location)
   - معرفة أماكن تخزين النسخ الاحتياطية وضمان توفرها عند الحاجة.
8. الاختبار والصيانة (Testing & Maintenance)
   - إجراء اختبارات دورية على الخطة لضمان فعاليتها وتحديثها حسب الحاجة.

(توضيح):

- Disaster Recovery Plan خطة استعادة الكوارث: هي خطة موثقة تضمن استعادة العمليات والأنظمة بعد وقوع حادث طارئ مثل الكوارث الطبيعية أو الهجمات الإلكترونية.
- Scope النطاق: يشير إلى الحدود التي تغطيها الخطة، مثل أنواع البيانات أو الأنظمة المشمولة بها.

- Emergency Contacts جهات الاتصال الطارئة :تشمل الأشخاص أو الفرق التي يتم التواصل معها أثناء الأزمة لضمان استجابة سريعة.

أهمية التعافي من الكوارث:

- ضمان استمرارية الأعمال.
- تعزيز أمان النظام.
- تحسين رضا العملاء والاحتفاظ بهم.
- تقليل تكاليف التعافي.
- تقليل الانقطاع :في حالة وقوع كارثة، حتى لو كانت غير متوقعة تمامًا، يمكن للأعمال الاستمرار بأقل قدر من التعطيل.
- تحديد الأضرار :يمكن السيطرة على مدى الضرر الناجم عن الكارثة
- التدريب والاستعداد :يساعد وجود برنامج تعافي من الكوارث في تدريب الموظفين على كيفية التصرف أثناء الكوارث، مما يقلل التوتر ويوفر خطة عمل واضحة
- استعادة الخدمات الحيوية : تتيح خطة DR إعادة تشغيل الخدمات الحرجة في وقت قصير .يعتمد وقت استعادة الخدمة (RTO)على أقصى فترة انتظار مقبولة حتى تتم استعادة الخدمة بالكامل.

طرق التعافي من الكوارث:

1- النسخ الاحتياطي(Backup)

- النسخ الاحتياطي هو أسهل طريقة للتعافي من الكوارث والتي تعتمدها جميع الشركات.
- يتضمن تخزين البيانات في مواقع خارجية أو في السحابة أو على وسائط قابلة للإزالة.
- يجب إجراء النسخ الاحتياطي بانتظام لضمان تحديث البيانات.

2- التعافي من كوارث مراكز البيانات(Data Center Disaster Recovery)

- في بعض أنواع الكوارث الطبيعية، يمكن للمعدات المناسبة حماية مراكز البيانات وتسريع عملية الاسترداد.
- على سبيل المثال :
  - أدوات إطفاء الحرائق تحمي المعدات والبيانات من التلف الناتج عن الحرائق.
  - مصادر الطاقة الاحتياطية تدعم استمرارية العمل في حالة انقطاع التيار الكهربائي.

3- المحاكاة الافتراضية(Virtualization)

- تعتمد الشركات على الآلات الافتراضية (VMs) لتخزين بياناتها وعملياتها في مواقع بعيدة غير معرضة للكوارث المادية.
- عند تضمين المحاكاة الافتراضية كجزء من خطة التعافي من الكوارث، يتم أتمتة بعض العمليات، مما يسرّع استعادة الأنظمة بعد الكوارث الطبيعية.

4- التعافي من الكوارث كخدمة(Disaster Recovery as a Service - DRaaS)

- نقل عمليات معالجة البيانات والأنشطة التجارية الأساسية إلى خدمات السحابة الخاصة بالشركة في حالة وقوع كارثة.

إن أصبت فذلك توفيق اللّه، وإن أخطأت فمن نفسي.

محمد بن عبدالرحمن العماري

أي سهو، تقدروا تلقوني.