Lernziele 3. ZW (ZP, MainQuest) Modul 231

Inhalt

Prüfungsvorbereitung

1. Worin zeichnet sich ein differenzielles Back-Up aus

Ein differenzielles Backup zeichnet sich dadurch aus, dass es im Vergleich zu einem inkrementellen Backup und einem vollständigen (auch als Vollbackup bezeichneten) Backup eine spezifische Methode der Datensicherung darstellt. Hier sind die wichtigsten Merkmale eines differenziellen Backups:

1. Vollbackup-Referenzpunkt: Ein differenzielles Backup basiert auf einem vorherigen Vollbackup. Dieses Vollbackup dient als Ausgangspunkt, von dem aus die Unterschiede (Differenzen) zwischen den Daten in diesem Vollbackup und den aktuellen Daten erfasst werden.

2. Speichert nur Änderungen seit dem letzten Vollbackup: Anders als inkrementelle Backups, die nur die Änderungen seit dem letzten Backup (egal, ob es sich um ein Vollbackup oder ein inkrementelles Backup handelt) speichern, speichert ein differenzielles Backup alle Änderungen, die seit dem letzten Vollbackup aufgetreten sind. Dies bedeutet, dass es im Laufe der Zeit größer werden kann, da es alle seit dem Vollbackup hinzugefügten oder geänderten Daten enthält.

3. Einfachere Wiederherstellung: Die Wiederherstellung eines Systems oder einer Datei aus einem differenziellen Backup ist einfacher als aus einer Abfolge von inkrementellen Backups, da nur das letzte Vollbackup und das differenzielle Backup benötigt werden. Im Falle eines inkrementellen Backups müssten alle inkrementellen Backups seit dem letzten Vollbackup wiederhergestellt werden, was zeitaufwendiger sein kann.

4. Geringerer Speicherplatzbedarf als Vollbackups: Im Vergleich zu regelmäßigen Vollbackups benötigen differenzielle Backups in der Regel weniger Speicherplatz, da sie nur die Änderungen seit dem letzten Vollbackup speichern. Allerdings kann der Speicherplatzbedarf im Laufe der Zeit steigen, da sich die Menge der gespeicherten Daten erhöht.

5. Schnellere Wiederherstellung als inkrementelle Backups: Im Vergleich zu inkrementellen Backups bietet ein differenzielles Backup in der Regel schnellere Wiederherstellungsgeschwindigkeiten, da weniger Backups durchlaufen werden müssen, um den gewünschten Stand der Daten wiederherzustellen.

Es ist wichtig zu beachten, dass differenzielle Backups zwar einige Vorteile bieten, aber auch Nachteile haben, wie einen potenziell steigenden Speicherplatzbedarf im Vergleich zu inkrementellen Backups. Die Wahl des besten Backup-Typs hängt von den spezifischen Anforderungen und Zielen für die Datensicherung ab.

2. Was ist der Unterschied zwischen Back-Up und Archivierung

Backup und Archivierung sind zwei unterschiedliche Konzepte, die in der Datenverwaltung und Datensicherheit eine wichtige Rolle spielen. Hier sind die Hauptunterschiede zwischen Backup und Archivierung:

1. Zweck:

- Backup: Das Hauptziel eines Backups besteht darin, Daten zu sichern, um im Falle eines Datenverlusts, sei es aufgrund von Hardwareausfällen, unbeabsichtigtem Löschen oder anderen Katastrophen, eine Wiederherstellung der Daten zu ermöglichen. Backups dienen der Wiederherstellung von aktuellen oder kürzlich bearbeiteten Daten.

- Archivierung: Archivierung ist ein langfristiger Prozess, bei dem Daten gespeichert und aufbewahrt werden, um sicherzustellen, dass sie langfristig zugänglich und unverändert bleiben. Archivierung ist in der Regel auf die Aufbewahrung von historischen oder rechtlich relevanten Daten ausgerichtet.

2. Datenretention:

- Backup: Backups haben in der Regel eine begrenzte Aufbewahrungsfrist und werden regelmäßig überschrieben oder gelöscht, sobald sie nicht mehr benötigt werden. Sie konzentrieren sich auf aktuelle oder kürzlich bearbeitete Daten.

- Archivierung: Daten, die archiviert werden, werden über lange Zeiträume hinweg aufbewahrt und sind normalerweise vor Änderungen geschützt. Sie können über Jahre oder sogar Jahrzehnte aufbewahrt werden, um beispielsweise gesetzlichen Anforderungen gerecht zu werden.

3. Datenstruktur:

- Backup: Backups können in verschiedenen Formaten erstellt werden, einschließlich vollständiger Kopien von Dateien, inkrementeller Backups und differenzieller Backups. Die Struktur der Daten im Backup ist darauf ausgelegt, die schnelle Wiederherstellung aktueller Daten zu ermöglichen.

- Archivierung: Bei der Archivierung werden Daten oft in speziellen Archivformaten gespeichert, die sicherstellen, dass die Daten unverändert bleiben und gut dokumentiert sind. Dies ermöglicht die langfristige Wiederherstellung und Suchbarkeit der archivierten Informationen.

4. Häufigkeit der Aktualisierung:

- Backup: Backups werden regelmäßig aktualisiert und überschrieben, um die aktuellsten Daten zu sichern. Sie sind auf kurzfristige Datensicherheit ausgerichtet.

- Archivierung: Daten in Archiven werden normalerweise selten aktualisiert und sind darauf ausgerichtet, historische Aufzeichnungen oder Referenzmaterial zu speichern.

5. Suchbarkeit und Zugriff:

- Backup: Backups sind in der Regel darauf ausgelegt, eine schnelle Wiederherstellung der Daten zu ermöglichen. Die Suche nach spezifischen Informationen in Backups kann herausfordernder sein.

- Archivierung: Archivierte Daten werden oft sorgfältig indexiert und dokumentiert, um eine einfache Suche und den Zugriff auf historische Informationen zu ermöglichen.

Insgesamt dienen Backups dazu, Datenverluste zu verhindern und die Wiederherstellbarkeit von aktuellen Daten sicherzustellen, während die Archivierung dazu dient, historische und rechtlich relevante Informationen langfristig aufzubewahren und leicht zugänglich zu machen. Beide Konzepte sind wichtige Bestandteile der Datenverwaltung in Unternehmen und Organisationen.

3. In welchen Fällen ist die Rede von redundanter Datenhaltung (Daten müssen zweimal erhalten werden wie macht man das, wurde vor den Ferien besprochen)

RAID-0 ist nicht redundant, all der Rest wie RAID-10 ist redundanter Datenerhaltung

Die redundante Datenhaltung tritt auf, wenn Daten in einem System, einer Datenbank oder einem Speicherort mehrfach und in mehreren Kopien vorhanden sind. Dies kann aus verschiedenen Gründen erfolgen und in verschiedenen Kontexten auftreten:

1. **Sicherung und Redundanz**: Redundante Datenhaltung kann als Teil einer Sicherungsstrategie eingesetzt werden. Daten werden in mehreren Kopien gespeichert, um sicherzustellen, dass sie im Falle eines Datenverlusts wiederhergestellt werden können. Dies kann in Form von regelmäßigen Backups erfolgen.

2. **Fehlertoleranz und Hochverfügbarkeit**: In Systemen, in denen Hochverfügbarkeit und Fehlertoleranz entscheidend sind, werden Daten redundant gespeichert. Dies ermöglicht es, dass das System weiterhin funktioniert, selbst wenn eine Kopie der Daten beschädigt wird oder ein Server ausfällt. Hierbei handelt es sich oft um Cluster- und Failover-Systeme.

3. **Skalierbarkeit und Lastenausgleich**: In großen Anwendungen und Datenbanken kann die Datenbankreplikation genutzt werden, um die Last auf verschiedene Server zu verteilen. Daten werden auf mehreren Servern redundant gespeichert, um die Abfragegeschwindigkeit zu erhöhen und die Skalierbarkeit zu verbessern.

4. **Historische Aufzeichnungen**: In einigen Fällen ist die redundante Speicherung von Daten Teil der Archivierung. Historische Daten werden in separaten Archivsystemen redundant gespeichert, um sicherzustellen, dass sie langfristig verfügbar sind.

5. **Datenintegration und Datentransformation**: In Data-Warehouses und Data-Marts können Daten aus verschiedenen Quellen zusammengeführt und redundant gespeichert werden, um effiziente Abfrage- und Analysemöglichkeiten zu bieten, ohne die Quellsysteme zu belasten.

6. **Datensynchronisation**: In verteilten Systemen oder bei der Zusammenarbeit von mehreren Benutzern können Daten in mehreren Kopien redundant gespeichert werden, um sicherzustellen, dass alle Benutzer mit den aktuellsten Informationen arbeiten.

Es ist wichtig zu beachten, dass redundante Datenhaltung nicht immer wünschenswert ist, da sie zusätzlichen Speicherplatz und Verwaltungsaufwand erfordern kann. Die sorgfältige Planung und Verwaltung von redundanten Daten sind entscheidend, um sicherzustellen, dass Datenintegrität und Konsistenz gewährleistet sind. In einigen Fällen können auch Datenschutz- und Compliance-Anforderungen die Art und Weise beeinflussen, wie redundante Daten gespeichert und verwaltet werden.

4. In welchen Datenschutzniveaus (Datenübermittlung ins Ausland) werden die Länder eingeteilt

Zur letzten, der vierten Frage gibt es so ein Ranking

Die Einteilung der Länder in Datenschutzniveaus, wenn es um die Übermittlung personenbezogener Daten ins Ausland geht, kann je nach Region oder Gesetzgebung variieren. Im Allgemeinen werden Länder in Datenschutzniveaus wie folgt eingeteilt:

1. **Angemessenheitsbeschlüsse**: Einige Länder oder Regionen werden als "angemessen" eingestuft, was bedeutet, dass sie ein Datenschutzniveau bieten, das mit den Datenschutzstandards des Ursprungslandes oder der Region vergleichbar ist. Datenübermittlungen in Länder mit einem Angemessenheitsbeschluss sind normalerweise ohne zusätzliche rechtliche Anforderungen erlaubt. Ein bekanntes Beispiel für einen solchen Beschluss ist die EU-US-Datenschutzschildvereinbarung.

2. **Standardvertragsklauseln**: Wenn ein Land nicht als angemessen eingestuft ist, können Organisationen Standardvertragsklauseln verwenden. Dies sind von der Europäischen Kommission genehmigte Vertragsmuster, die zwischen Datenexporteuren und Datenimporteuren in verschiedenen Ländern geschlossen werden, um den Schutz personenbezogener Daten sicherzustellen.

3. **Binding Corporate Rules (BCR)**: Große multinationale Unternehmen können Binding Corporate Rules erstellen, die von den Datenschutzbehörden genehmigt werden, um die Übermittlung von Daten innerhalb des Unternehmens in Länder mit unterschiedlichen Datenschutzstandards zu ermöglichen.

4. **Einwilligung**: Personen können der Übermittlung ihrer Daten ins Ausland zustimmen. Dies ist jedoch in einigen Regionen, insbesondere in der Europäischen Union, mit bestimmten Einschränkungen und Informationsanforderungen verbunden.

5. **Adequate Schutzmaßnahmen**: Organisationen können zusätzliche Sicherheitsmaßnahmen ergreifen, um sicherzustellen, dass die übermittelten Daten angemessen geschützt werden, selbst wenn das Zielland nicht als angemessen eingestuft ist. Dazu gehören Verschlüsselung, Pseudonymisierung und andere technische und organisatorische Maßnahmen.

6. **Notfälle und öffentliche Interessen**: In einigen Fällen kann die Übermittlung personenbezogener Daten ins Ausland aus dringenden Gründen des öffentlichen Interesses oder zur Abwehr von Gefahren gestattet sein.

Es ist wichtig zu beachten, dass die Datenschutzregelungen in verschiedenen Ländern und Regionen unterschiedlich sein können. Die Einhaltung der geltenden Datenschutzgesetze und die Berücksichtigung der erforderlichen Schritte zur sicheren Übermittlung von Daten ins Ausland sind entscheidend, um Datenschutzverletzungen und rechtliche Konsequenzen zu vermeiden. Daher sollten Organisationen, die personenbezogene Daten ins Ausland übertragen, die jeweiligen Gesetze und Bestimmungen sorgfältig prüfen und gegebenenfalls Rechtsberatung in Anspruch nehmen.