DEVOPS

5. forduló

<epam>

A kategória támogatója: EPAM

RENDELKEZÉSRE ÁLLÓ IDŐ:

15:00

Ismertető a feladathoz

Felhasznált idő: 02:07/15:00 **Elért pontszám:** 0/25

1. feladat 0/5 pont

Hogyan orvosolod a cloudban, ha a Linux gépeden a steal time (%st) értéke nem 0?

Válaszok

- [ ] Megnövelem a másodpercenként elvégezhető Input/Output műveletek számát
- [x] Másik régióba vagy zónába mozgatom a gépet
- [ ] Ürítem a Pagecache-t a szerveren
- [x] Nagyobb teljesítményű virtuális gépet indítok

Magyarázat

A CPU steal time az a százalékban kifejezett idő, amikor a virtuális CPU a valós CPU-ra vár, miközben a hypervisor egy másik virtuális CPU-t szolgál ki. Ha ez az állapot előáll a virtuális gépben a folyamat ugyanúgy futó státuszban van, de CPU időt nem kap a feladatának végrehajtására.

Mozgatással és új gép indításával új fizikai gépre kerül a virtuális gép ahol jó eséllyel kedvezőbb lesz a CPU steal time értéke.

2. feladat 0/5 pont

Melyik két funkció tartozik a Kubernetes cluster-ek „Cloud Controller Manager” (többnyire alap) komponens felelősségi körébe?

Válaszok

- [x] Automatikus loadbalancer létrehozás és konfigurálás a felhőszolgáltatónál, ahol fut a cluster
- [x] Node-ok automatikus törlése amennyiben a felhőszolgáltatónál már nem létezik a node-hoz tartozó virtuális gép
- [ ] A Node-okhoz tartozó DNS bejegyzések automatikus létrehozása, frissítése (amennyiben a felhőszolgáltató támogat ilyen funkciót)
- [ ] Új node-ok automatikus indítása, amennyiben a cluster nem képes elegendő erőforrást lefoglalni a beütemzendő Pod-ok számára

Magyarázat

Node DNS létrehozás/frissítás: ez a funkció csak külső komponens által elérhető: pl. external-dns

Új nodeok automata indítás: ez a funkció csak külső komponens által elérhető: pl. cluster-autoscaler

3. feladat 0/5 pont

Egy cég folyamatos integráció (CI) megvalósításában a verziókezelő rendszer főágába (main/master) kizárólag akkor kerülhet be (merge) új fejlesztéshez tartozó kód, amennyiben az sikeresen átment a szükséges ellenőrzési/tesztelési lépéseken. Miután ez megtörtént újra lefutnak az ellenőrzések a főágban tárolt kódra is. Az alábbiak közül, melyik indokolja az ellenőrzések újrafuttatását a főágon?

Válasz

- ( ) Az automatikus tesztelés instabil, ezért nem árt többször lefuttatni
- ( ) A fejlesztési ágon lévő kód nem feltétlenül egyezik meg azzal a kódállapottal, ami közvetlenül a beküldés (merge) után jön létre a főágon, így eltérő eredményt hozhat
- ( ) A fejlesztők azután is tudnak módosítani a fejlesztési ágon, miután az bekerült a főágba
- ( ) A főágba történő beolvasztáskor (merge) karakterkódolási hibák léphetnek fel, melyek hibát okozhatnak a főágon

Magyarázat

Az automatikus tesztek esetleges instabilitását nem a CI processz szintjén kell megoldani, hanem az instabilitás okát megkeresni vagy a tesztekbe építeni az újrapróbálkozást.

A fejlesztési ágon történt későbbi változtatások nincsenek hatással a főágra, ha azt szeretnénk, hogy az is be kerüljön meg kell ismételni az ellenőrzési folyamatot.

A karakterkódolásból adódó hibákat nem a merge okozza, azokat a fejlesztői ág ellenőrzése is felfedezné.

4. feladat 0/5 pont

Milyen előnyei lehetnek a Terraform “plan” parancs használatának?

Válaszok

- [ ] Felhőszolgáltatások esetén költségtervet készít az elvégzendő infrastrutúraváltozásokról
- [x] A segítségével ellenőrizni lehet a végrehajtandó változásokat, mielőtt ténylegesen végrehajtjuk őket
- [ ] Optimalizálási javaslatokat tesz az infrastruktúra leírókódunkhoz
- [x] Folyamatos telepítési folyamatba építhető, hogy kiszűrje a szabályzatba ütköző változtatásokat

Magyarázat

Az optimalizálás és költség terv készítés nem tartozik a Terraform alap funkciói közé.

5. feladat 0/5 pont

Az alábbiak közül melyek hordozzák lehetséges ”Ellátási lánc” (Supply chain) támadás kockázatát?

Válaszok

- [ ] Az alkalmazás titkosítatlan adatbázis kapcsolaton keresztül fogad adatokat egy általunk üzemeltetett másik adatközpontból
- [x] Alkalmazásépítéskor mindig egy közösségi fejlesztés alatt álló nyílt forráskódú fordítóprogram legfrissebb verzóját használjuk
- [x] Az alkalmazásunk Docker konténerét egy DockerHub-os image “stable” tag-gel ellátott változatára alapozzuk
- [ ] Egy webes alkalmazás nem ellenőrzi a bemenő adatait

Magyarázat

Az adatok továbbítás közbeni titkosítása, valamint a bemendő adatok ellenőrzése nincs összefüggésben az Ellátásilánc támadások definíciójával: „Közvetett kibertámadás egy szervezet ellen, egy az ellátási láncában található másik szervezeten keresztül.”

KÉSZÍTETTE

Megjelenés

Világos