- **Vendor:** Microsoft
- **Exam Code:** AZ-400
- **Exam Name:** Implementing and Operating Cisco Data Center Core Technologies (DCCOR)
- **New Updated Questions from Braindump2go (Updated in Oct./2020)**

QUESTION 219
You need to configure GitHub to use Azure Active Directory (Azure AD) for authentication.
What should you do first?

A. Create a conditional access policy in Azure AD.
B. Register GitHub in Azure AD.
C. Create an Azure Active Directory B2C (Azure AD B2C) tenant.
D. Modify the Security settings of the GitHub organization.

Answer: B
Explanation:
When you connect to a Git repository from your Git client for the first time, the credential manager prompts for credentials. Provide your Microsoft account or Azure AD credentials.
Note: Git Credential Managers simplify authentication with your Azure Repos Git repositories. Credential managers let you use the same credentials that you use for the Azure DevOps Services web portal.
Credential managers support multi-factor authentication through Microsoft account or Azure Active Directory (Azure AD). Besides supporting multi-factor authentication with Azure Repos, credential managers also support two-factor authentication with GitHub repositories.
Reference:
https://docs.microsoft.com/en-us/azure/devops/repos/git/set-up-credential-managers

QUESTION 220
You have a project in Azure DevOps named Project1. Project1 contains a pipeline that builds a container image named Image1 and pushes Image1 to an Azure container registry named ACR1. Image1 uses a base image stored in Docker Hub.
You need to ensure that Image1 is updated automatically whenever the base image is updated.
What should you do?

A. Enable the Azure Event Grid resource provider and subscribe to registry events.
B. Add a Docker Hub service connection to Azure Pipelines.
C. Create and run an Azure Container Registry task.
D. Create a service hook in Project1.

Answer: C
Explanation:
ACR Tasks supports automated container image builds when a container's base image is updated, such as when you patch the OS or application framework in one of your base images.
Reference:
https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tutorial-base-image-update

QUESTION 221

You have a free tier of an Azure DevOps organization named Contoso. Contoso contains 10 private projects. Each project has multiple jobs with no dependencies.
You frequently run the jobs on five self-hosted agents but experience long build times and frequently queued builds.
You need to minimize the number of queued builds and the time it takes to run the builds.
What should you do?

A. Configure the pipelines to use the Microsoft-hosted agents.
B. Register additional self-hosted agents.
C. Purchase self-hosted parallel jobs.
D. Purchase Microsoft-hosted parallel jobs.

Answer: D
Explanation:
When the free tier is no longer sufficient, you can pay for additional capacity per parallel job.
Note: Microsoft-hosted CI/CD
If you want to run your jobs on machines that Microsoft manages, use Microsoft-hosted parallel jobs. Your jobs run on our pool of Microsoft-hosted agents.
We provide a free tier of service by default in every organization.
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/licensing/concurrent-jobs

QUESTION 222
You have an Azure DevOps project that contains a build pipeline. The build pipeline uses approximately 50 open source libraries.
You need to ensure that all the open source libraries comply with your company's licensing standards.
Which service should you use?

A. Ansible
B. Maven
C. WhiteSource Bolt
D. Helm

Answer: C
Explanation:
WhiteSource provides WhiteSource Bolt, a lightweight open source security and management solution developed specifically for integration with Azure DevOps and Azure DevOps Server.
Note: WhiteSource is the leader in continuous open source software security and compliance management. WhiteSource integrates into your build process, irrespective of your programming languages, build tools, or development environments. It works automatically, continuously, and silently in the background, checking the security, licensing, and quality of your open source components against WhiteSource constantly-updated definitive database of open source repositories.
Note: Blackduck would also be a good answer, but it is not an option here.
Reference:
https://www.azuredevopslabs.com/labs/vstsextend/whitesource/

QUESTION 223
Your company develops an application named App1 that is deployed in production.
As part of an application update, a new service is being added to App1. The new service requires access to an application named App2 that is currently in development.
You need to ensure that you can deploy the update to App1 before App2 becomes available. You must be able to enable the service in App1 once App2 is deployed.
What should you do?

A. Implement a feature flag.
B. Create a fork in the build.
C. Create a branch in the build.

D. Implement a branch policy.

Answer: A
Explanation:
Feature flags support a customer-first DevOps mindset, to enable (expose) and disable (hide) features in a solution, even before they are complete and ready for release.
Incorrect Answers:
C: Branch policies are an important part of the Git workflow and enable you to:
Isolate work in progress from the completed work in your master branch
Guarantee changes build before they get to master
Reference:
https://docs.microsoft.com/en-us/azure/devops/migrate/phase-features-with-feature-flags

QUESTION 224
You are designing the security validation strategy for a project in Azure DevOps.
You need to identify package dependencies that have known security issues and can be resolved by an update.
What should you use?

A. Octopus Deploy
B. Jenkins
C. Gradle
D. SonarQube

Answer: A
Explanation:
Incorrect Answers:
B: Jenkins is a popular open-source automation server used to set up continuous integration and delivery (CI/CD) for your software projects.
D: SonarQube is a set of static analyzers that can be used to identify areas of improvement in your code. It allows you to analyze the technical debt in your project and keep track of it in the future.
Reference:
https://octopus.com/docs/packaging-applications

QUESTION 225
You have a private distribution group that contains provisioned and unprovisioned devices.
You need to distribute a new iOS application to the distribution group by using Microsoft Visual Studio App Center.
What should you do?

A. Generate a new .p12 file for each device.
B. Create an unsigned build.
C. Register the devices on the Apple Developer portal.
D. Create an active subscription in App Center Test.

Answer: C
Explanation:
When releasing an iOS app signed with an ad-hoc or development provisioning profile, you must obtain tester's device IDs (UDIDs), and add them to the provisioning profile before compiling a release. When you enable the distribution group's Automatically manage devices setting, App Center automates the before mentioned operations and removes the constraint for you to perform any manual tasks. As part of automating the workflow, you must provide the user name and password for your Apple ID and your production certificate in a .p12 format.
App Center starts the automated tasks when you distribute a new release or one of your testers registers a new device. First, all devices from the target distribution group will be registered, using your Apple ID, in your developer portal and all provisioning profiles used in the app will be generated with both new and existing device ID. Afterward, the newly generated provisioning profiles are downloaded to App Center servers.
Reference:
https://docs.microsoft.com/en-us/appcenter/distribution/groups

QUESTION 226
Your company uses the following resources:

```
- Windows Server 2019 container images hosted in an Azure Container Registry.
- Azure virtual machines that run the latest version of Ubuntu
- An Azure Log Analytics workspace
- Azure Active Directory (Azure AD)
- An Azure key vault
```

For which two resources can you receive vulnerability assessments in Azure Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Azure Log Analytics workspace
B. the Azure key vault
C. the Azure virtual machines that run the latest version of Ubuntu
D. Azure Active Directory (Azure AD)
E. The Windows Server 2019 container images hosted in the Azure Container Registry.

Answer: BC
Explanation:
B: Azure Security Center includes Azure-native, advanced threat protection for Azure Key Vault, providing an additional layer of security intelligence.
C: When Security Center discovers a connected VM without a vulnerability assessment solution deployed, it provides the security recommendation "A vulnerability assessment solution should be enabled on your virtual machines".
Ubuntu supported versions: 12.04 LTS, 14.04 LTS, 15.x, 16.04 LTS, 18.04 LTS Reference:
https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm

QUESTION 227
You have a private project in Azure DevOps.
You need to ensure that a project manager can create custom work item queries to report on the project's progress. The solution must use the principle of least privilege.
To which security group should you add the project manager?

A. Reader
B. Project Collection Administrators
C. Project Administrators
D. Contributor

Answer: D
Explanation:
Contributors have permissions to contribute fully to the project code base and work item tracking. The main permissions they don't have or those that manage or administer resources.
Reference:
https://docs.microsoft.com/en-us/azure/devops/organizations/security/permissions

QUESTION 228
You use Azure Pipelines to manage build pipelines, GitHub to store source code, and Dependabot to manage dependencies.
You have an app named App1.
Dependabot detects a dependency in App1 that requires an update.
What should you do first to apply the update?

A. Create a pull request.
B. Approve the pull request.
C. Create a branch.
D. Perform a commit.

Answer: B

Explanation:

DependaBot is a useful tool to regularly check for dependency updates. By helping to keep your project up to date, DependaBot can reduce technical debt and immediately apply security vulnerabilities when patches are released. How does DependaBot work?

1. DependaBot regularly checks dependencies for updates
2. If an update is found, DependaBot creates a new branch with this upgrade and Pull Request for approval
3. You review the new Pull Request, ensure the tests passed, review the code, and decide if you can merge the change

Reference:
https://samlearnsazure.blog/2019/12/20/github-using-dependabot/

QUESTION 229

You are integrating Azure Pipelines and Microsoft Teams.
You install the Azure Pipelines app in Microsoft Teams.
You have an Azure DevOps organization named Contoso that contains a project name Project1.
You subscribe to Project1 in Microsoft Teams.
You need to ensure that you only receive events about failed builds in Microsoft Teams.
What should you do first?

A. From Microsoft Teams, run @azure pipelines subscribe https://dev.azure.com/Contoso/Project1.
B. From Azure Pipelines, add a Publish Build Artifacts task to Project1.
C. From Microsoft Teams, run @azure pipelines subscriptions.
D. From Azure Pipelines, enable continuous integration for Project1.

Answer: A

Explanation:

To start monitoring all pipelines in a project, use the following command inside a channel:
@azure pipelines subscribe [project url]
The project URL can be to any page within your project (except URLs to pipelines).
For example:
@azure pipelines subscribe https://dev.azure.com/myorg/myproject/
Reference:
https://docs.microsoft.com/en-us/azure/devops/pipelines/integrations/microsoft-teams