Answer Sheet

Q1) What restricts the release of packages in development if a single feed releases multiple builds of each package which are to be shared and were written, tested, validated, and deployed by using Azure Artifacts?

✅ Upstream sources

Explanation:-Upstream sources enable you to manage all of your product's dependencies in a single feed. We recommend publishing all of the packages for a given product to that product's feed, and managing that product's dependencies from remote feeds in the same feed, via upstream sources. This setup has a few benefits:

• Simplicity: your NuGet.config, .npmrc, or settings.xml contains exactly one feed (your feed).

• Determinism: your feed resolves package requests in order, so rebuilding the same codebase at the same commit or changeset uses the same set of packages

• Provenance: your feed knows the provenance of packages it saved via upstream sources, so you can verify that you're using the original package, not a custom or malicious copy published to your feed

• Peace of mind: packages used via upstream sources are guaranteed to be saved in the feed on first use; if the upstream source is disabled/removed, or the remote feed goes down or deletes a package you depend on, you can continue to develop and build

- None of these
- Views
- Global symbols
- Local symbols

Q2) Which of the following should be used to collect crash reports for issue analysis, distribute beta releases to testers and obtain user feedback on the functionality of new apps, when developing a mobile app for Android and iOS devices using Azure DevOps for work items and release cycles?

- Azure Application insights widgets
- Microsoft Visual Studio App Center integration

✅ the Microsoft Test & Feedback extension

Explanation:-The "Exploratory Testing" extension is now "Test & Feedback" and is now Generally Available.

Anyone can now test web apps and give feedback, all directly from the browser on any platform: Windows, Mac, or Linux. Available for Google Chrome and Mozilla Firefox (required version 50.0 or above) currently. Support for Microsoft Edge is in the pipeline and will be enabled once Edge moves to a Chromium-compatible web platform.

- Jenkins integration
- None of these

Q3)

You manage build pipelines and deployment pipelines by using Azure DevOps.

Your company has a team of 500 developers. New members are added continually to the team.

You need to automate the management of users and licenses whenever possible.

Which task must you perform manually?

- assigning entitlements
- adding users
- modifying group memberships

✅ procuring licenses

Q4)

You are developing a multi-tier application. The application will use Azure App Service web apps as the front end and an Azure SQL database as the back end. The application will use Azure functions to write some data to Azure Storage.

You need to send the Azure DevOps team an email message when the front end fails to return a status code of 200.

Which feature should you use?

- Service Map in Azure Log Analytics
- Availability tests in Azure Application Insights
- Profiler in Azure Application Insights

✅ Application Map in Azure Application Insights

Explanation:-Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status.

Q5)

During a code review, you discover many quality issues. Many modules contain unused variables and empty catch blocks.

You need to recommend a solution to improve the quality of the code.

What should you recommend?

- In a Xcode build task, select Use xcpretty from Advanced.

✅ In a Maven build task, select Run PMD.

Explanation:-PMD is a source code analyzer. It finds common programming flaws like unused variables, empty catch blocks, unnecessary object creation, and so forth.

There is an Apache Maven PMD Plugin which allows you to automatically run the PMD code analysis tool on your project's source code and generate a site report with its results.

- In a Grunt build task, select Enabled from Control Options.
- In a Gradle build task, select Run Checkstyle.

Q6)

Your company plans to use an agile approach to software development.

You need to recommend an application to provide communication between members of the development team who work in locations around the world. The applications must meet the following requirements:

Provide the ability to isolate the members of different project teams into separate communication channels and to keep a history of the chats within those channels.
Be available on Windows 10, Mac OS, iOS, and Android operating systems.
Provide the ability to add external contractors and suppliers to projects.
Integrate directly with Azure DevOps.

What should you recommend?

- Microsoft Project
- Bamboo
- Octopus
- ✅ Slack

Explanation:-Slack is a popular team collaboration service that helps teams be more productive by keeping all communications in one place and easily searchable from virtually anywhere. All your messages, your files, and everything from Twitter, Dropbox, Google Docs, Azure DevOps, and more all together. Slack also has fully native apps for iOS and Android to give you the full functionality of Slack wherever you go.
Integrated with Azure DevOps
This integration keeps your team informed of activity happening in its Azure DevOps projects. With this integration, code check-ins, pull requests, work item updates, and build events show up directly in your team's Slack channel.

Q7)

Your development team is building a new web solution by using the Microsoft Visual Studio integrated development environment (IDE).

You need to make a custom package available to all the developers. The package must be managed centrally, and the latest version must be available for consumption in Visual Studio automatically.

Which three actions should you perform?

- ✅ Create a new feed in Azure Artifacts.

Explanation:-By using your custom NuGet package feed within your Azure DevOps (previously VSTS) instance, you'll be able to distribute your packages within your organization with ease.
Start by creating a new feed.

- Upload a package to a Git repository.
- Add the package URL to the Environment settings in Visual Studio.
- ✅ Add the package URL to the NuGet Package Manager settings in Visual Studio.

Explanation:-Consume your private NuGet Feed
Go back to the Packages area in Azure DevOps, select your feed and hit "Connect to feed". You'll see some instructions for your feed, but it's fairly simple to set up.
Just copy your package source URL, go to Visual Studio, open the NuGet Package Manager, go to its settings and add a new source. Choose a fancy name, insert the source URL. Done.
Search for your package in the NuGet Package Manager and it should appear there, ready for installation. Make sure to select the appropriate feed (or just all feeds) from the top right select box.

- ✅ Publish the package to a feed.

Explanation:-We can publish, pack and push the built project to our NuGet feed.

- Create a Git repository in Azure Repos.

Q8)

Your company uses a Git repository in Azure Repos to manage the source code of a web application. The master branch is protected from direct updates.

Developers work on new features in the topic branches.

Because of the high volume of requested features, it is difficult to follow the history of the changes to the master branch.

You need to enforce a pull request merge strategy. The strategy must meet the following requirements:

Consolidate commit histories.
Merge the changes into a single commit.

Which merge strategy should you use in the branch policy?

- no-fast-forward merge
- Git fetch
- fast-forward merge
- ✅ squash merge

Explanation:-Squash merging is a merge option that allows you to condense the Git history of topic branches when you complete a pull request. Instead of each commit on the topic branch being added to the history of the default branch, a squash merge takes all the file changes and adds them to a single new commit on the default branch.
A simple way to think about this is that squash merge gives you just the file changes, and a regular merge gives you the file changes and the commit history.

Q9)

Your company uses cloud-hosted Jenkins for builds.

You need to ensure that Jenkins can retrieve source code from Azure Repos.

Which three actions should you perform?

✅ Create a service hook in Azure DevOps.
Explanation:-For those who need tighter integration, Team Services provides two additional ways to achieve it: 1) the Jenkins Service Hook, and 2) Jenkins build and release tasks.)
⚪ Add a domain to your Jenkins account.
✅ Create a personal access token in your Azure DevOps account.
Explanation:-Use Azure DevOps/ Visual Studio Team Services to create an access token, and use th
⚪ Create a webhook in Jenkins.
✅ Add the Team Foundation Server (TFS) plug-in to Jenkins.
Explanation:-Jenkins' built-in Git Plugin or Team Foundation Server Plugin can poll a Team Services repository every few minutes and queue a job when changes are detected.

Q10)

You have an Azure Resource Manager template that deploys a multi-tier application.

You need to prevent the user who performs the deployment from viewing the account credentials and connection strings used by the application.

What should you use?

⚪ an Azure Storage table
⚪ an Appsettings.json file
⚪ a Web.config file
✅ Azure Key Vault
Explanation:-When you need to pass a secure value (like a password) as a parameter during deployment, you can retrieve the value from an Azure Key Vault. You retrieve the value by referencing the key vault and secret in your parameter file. The value is never exposed because you only reference its key vault ID. The key vault can exist in a different subscription than the resource group you are deploying to.
⚪ an Azure Resource Manager parameter file

Q11)

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create an email subscription to an Azure DevOps notification.

Does this meet the goal?

⚪ Correct
✅ Incorrect
Explanation:-You can create a service hook for Azure DevOps Services and TFS with Jenkins.

Q12)

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You create a service hook subscription that uses the code pushed event.

Does this meet the goal?

⚪ Incorrect
✅ Correct
Explanation:-You can create a service hook for Azure DevOps Services and TFS with Jenkins.

Q13)

You integrate a cloud-hosted Jenkins server and a new Azure DevOps deployment.

You need Azure DevOps to send a notification to Jenkins when a developer commits changes to a branch in Azure Repos.

Solution: You add a trigger to the build pipeline.

Does this meet the goal?

⚪ Correct
✅ Incorrect
Explanation:-You can create a service hook for Azure DevOps Services and TFS with Jenkins.

Q14)

You are automating the build process for a Java-based application by using Azure DevOps.

You need to add code coverage testing and publish the outcomes to the pipeline.

What should you use?

- NUnit
- Coverlet
- MSTest
- Bullseye Coverage
- ✅ Cobertura

Explanation:-Use Publish Code Coverage Results task in a build pipeline to publish code coverage results to Azure Pipelines or TFS, which were produced by a build in Cobertura or JaCoCo format.

- Coverage.py

Q15)

Your company uses Azure DevOps.

Only users who have accounts in Azure Active Directory can access the Azure DevOps environment.

You need to ensure that only devices that are connected to the on-premises network can access the Azure DevOps environment.

What should you do?

- Assign the Stakeholder access level all users.
- In Azure Active Directory, configure risky sign-ins.
- In Azure DevOps, configure Security in Project Settings.
- ✅ In Azure Active Directory, configure conditional access.

Explanation:-Conditional Access is a capability of Azure Active Directory. With Conditional Access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.
Conditional Access policies are enforced after the first-factor authentication has been completed.

Q16)

You are automating the testing process for your company.

You need to automate UI testing of a web application.

Which framework should you use?

- Microsoft.CodeAnalysis
- Xamarin.UITest
- ✅ Selenium

Explanation:-Performing user interface (UI) testing as part of the release pipeline is a great way of detecting unexpected changes, and need not be difficult. Selenium can be used to test your website during a continuous deployment release and test automation.

- JaCoco

Q17)

You have an Azure DevOps organization named Contoso, an Azure DevOps project named Project1, an Azure subscription named Sub1, and an Azure key vault named vault1.

You need to ensure that you can reference the values of the secrets stored in vault1 in all the pipelines of Project1. The solution must prevent the values from being stored in the pipelines.

What should you do?

- Modify the security settings of the pipelines.
- Add a secure file to Project1.
- ✅ Create a variable group in Project1.

Explanation:-Use a variable group to store values that you want to control and make available across multiple pipelines.

- Configure the security policy of Contoso.

Q18)

Your team uses an agile development approach.

You need to recommend a branching strategy for the team's Git repository. The strategy must meet the following requirements.

Provide the ability to work on multiple independent tasks in parallel.
Ensure that checked-in code remains in a releasable state always.
Ensure that new features can be abandoned at any time.
Encourage experimentation.

What should you recommend?

- a single long-running branch
- multiple long-running branches
- a single fork per team member
- ✅ a single-running branch with multiple short-lived topic branches

Explanation:-Topic branches, however, are useful in projects of any size. A topic branch is a short-lived branch that you create and use for a single particular feature or related work. This is something you've likely never done with a VCS before because it's generally too expensive to create and merge branches. But in Git it's common to create, work on, merge, and delete branches several times a day

---

Q19)

Your company has a project in Azure DevOps for a new web application.

The company identifies security as one of the highest priorities.

You need to recommend a solution to minimize the likelihood that infrastructure credentials will be leaked.

What should you recommend?

- Add Azure Key Vault references to Azure Resource Manger templates.
- Add a Azurre Key Vault task to the pipeline.
- ✅ Add a PowerShell task to the pipeline and run Set-AzureKeyVaultSecret.

Explanation:-Azure Key Vault provides a way to securely store credentials and other keys and secrets.
The Set-AzureKeyVaultSecret cmdlet creates or updates a secret in a key vault in Azure Key Vault.

- Add a Run Inline Azure PowerShell task to the pipeline.

Q20)

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure an Octopus Tentacle on an on-premises machine. Use the Package Application task in the build pipeline.

Does this meet the goal?

- Incorrect
- ✅ Correct

Explanation:-Octopus Deploy is an automated deployment server that makes it easy to automate deployment of ASP.NET web applications, Java applications, NodeJS application and custom scripts to multiple environments.
Octopus can be installed on various platforms including Windows, Mac and Linux. It can also be integrated with most version control tools including VSTS and GIT.
When you deploy software to Windows servers, you need to install Tentacle, a lightweight agent service, on your Windows servers so they can communicate with the Octopus server.
When defining your deployment process, the most common step type will be a package step. This step deploys your packaged application onto one or more deployment targets.
When deploying a package you will need to select the machine role that the package will be deployed to.

Q21)

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.

Solution: Install and configure a self-hosted build agent on an on-premises machine. Configure the build pipeline to use the Default agent pool. Include the Java

Tool Installer task in the build pipeline.

Does this meet the goal?

- ✅ Incorrect
- Correct

Q22)

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted VS 2017 agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

- ✅ Incorrect
- Correct

Q23)

You are designing the development process for your company.

You need to recommend a solution for continuous inspection of the company's code base to locate common code patterns that are known to be problematic.

What should you include in the recommendation?

- Gradle wrapper scripts
- ✅ SonarCloud analysis

Explanation:-SonarCloud is a cloud service offered by SonarSource and based on SonarQube. SonarQube is a widely adopted open source platform to inspect continuously the quality of source code and detect bugs, vulnerabilities and code smells in more than 20 different languages.

- Microsoft Visual Studio test plans
- the JavaScript task runner

Q24)

Your company builds a multi-tier web application.

You use Azure DevOps and host the production application on Azure virtual machines.

Your team prepares an Azure Resource Manager template of the virtual machine that you will use to test new features.

You need to create a staging environment in Azure that meets the following requirements:

Minimizes the cost of Azure hosting
Provisions the virtual machines automatically
Uses the custom Azure Resource Manager template to provision the virtual machines

What should you do?

- In Azure Cloud Shell, run Azure CLI commands to create and delete the new virtual machines in a staging resource group.
- In Azure DevOps, configure new tasks in the release pipeline to deploy to Azure Cloud Services.
- From Azure Cloud Shell, run Azure PowerShell commands to create and delete the new virtual machines in a staging resource group.
- ✅ In Azure DevOps, configure new tasks in the release pipeline to create and delete the virtual machines in Azure DevTest Labs.

Explanation:-You can use the Azure DevTest Labs Tasks extension that's installed in Azure DevOps to easily integrate your CI/CD build-and-release pipeline with Azure DevTest Labs. The extension installs three tasks:
• Create a VM
• Create a custom image from a VM
• Delete a VM
The process makes it easy to, for example, quickly deploy a "golden image" for a specific test task and then delete it when the test is finished.

Q25)

You need to recommend an integration strategy for the build process of a Java application. The solution must meet the following requirements:

The builds must access an on-premises dependency management system.
The build outputs must be stored as Server artifacts in Azure DevOps.
The source code must be stored in a Git repository in Azure DevOps.

Solution: Configure the build pipeline to use a Hosted Ubuntu agent pool. Include the Java Tool Installer task in the build pipeline.

Does this meet the goal?

- ✅ Incorrect

Explanation:-Instead use Octopus Tentacle.

- Correct

Q26)

You have 50 Node.js-based projects that you scan by using WhiteSource. Each project includes Package.json, Package-lock.json, and Npm-shrinkwrap.json files.

You need to minimize the number of libraries reports by WhiteSource to only the libraries that you explicitly reference.

What should you do?

- Delete Package-lock.json.
- Configure the Artifactory plug-in.
- ✅ Add a devDependencies section to Package-lock.json.

Explanation:-Separate Your Dependencies
Within your package.json file be sure you split out your npm dependencies between devDependencies and (production) dependencies. The key part is that you must then make use of the --production flag when installing the npm packages. The --production flag will exclude all packages defined in the devDependencies section.

- Configure the File System Agent plug-in.

Q27)

You have an approval process that contains a condition. The condition requires that releases be approved by a team leader before they are deployed.

You have a policy stating that approvals must occur within eight hours.

You discover that deployment fail if the approvals take longer than two hours.

You need to ensure that the deployments only fail if the approvals take longer than eight hours.

Solution: From Post-deployment conditions, you modify the Time between re-evaluation of gates option.

Does this meet the goal?

- ✅ Incorrect
- Correct

Q28) Correct or incorrect: You need to use the Azure CLI to create an Azure Spring Cloud cluster.

- [x] Incorrect
- [ ] Correct

Q29) Correct or incorrect: The name of an Azure Spring Cloud cluster should be unique across all of Azure.

- [ ] Incorrect
- [x] Correct

Q30) On Azure Spring Cloud, which security mechanisms do Spring Cloud Config Server support?

- [ ] Only publicly available (unsecured) Git repositories
- [ ] Secured by SSH, or secured using HTTP basic authentication
- [x] Public, secured by SSH or secured using HTTP basic authentication
- [ ] Only HTTP basic authentication

Q31) Using Spring Cloud Config is a great solution as:

- [x] All of these.
- [ ] It allows storing sensitive parameters (like your database password) outside of your application.
- [ ] It provides a centralized place to store all your configuration data, for all your microservices.
- [ ] Configuration is stored in a specific Git repository, which can be secured separately.
- [ ] It uses Git, so your configuration data can be tagged or rolled back.

Q32) To deploy a Spring Boot microservice to Azure Spring Cloud, what do you need to change in your application?

- [ ] You need to set up some specific environment variables
- [x] You need to add a specific Maven dependency
- [ ] You need to code a specific Spring bean

Q33) By default, how can you access your microservice once it is deployed?

- [ ] The endpoint is not available at all on the Internet, you must use a private network to access it
- [ ] There is a publicly-available endpoint
- [x] There is a specific, secured endpoint, where the application is published

Q34) How do you configure distributed tracing for an application deployed to Azure Spring Cloud?

- [x] Add a Spring Boot starter, in the Maven pom.xml file
- [ ] Configure a specific Spring bean
- [ ] Add some specific Spring Boot configuration properties

Q35) Once your telemetry data is ingested by Azure Monitor, what will you be able to do?
I. You'll have access to an automatically generated map of all your microservices
II. You'll be able to launch a debugger, and hot replace code in production
III. You'll have access to a search engine, to find your performance bottlenecks

- [x] I and III
- [ ] I, II and III
- [ ] I and II

Q36) Using Azure Spring Cloud and CI/CD together is a recommended practice as:

- [x] All of these
- [ ] It can automatically deploy an application to production
- [ ] It allows testing the application automatically
- [ ] It allows building the application automatically