# AZ-400 Q&As

Designing and Implementing Microsoft DevOps Solutions

## Pass Microsoft AZ-400 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.leads4pass.com/az-400.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

**QUESTION 1**

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

Correct Answer: C

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 2**

You use WhiteSource Bolt to scan a Node.js application.

The WhiteSource Bolt scan identifies numerous libraries that have invalid licenses. The libraries are used only during development and are not part of a production deployment.

You need to ensure that WhiteSource Bolt only scans production dependencies.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Run npm install and specify the --production flag.

B. Modify the WhiteSource Bolt policy and set the action for the licenses used by the development tools to Reassign.

C. Modify the devDependencies section of the project\\'s Package.json file.

D. Configure WhiteSource Bolt to scan the node_modules directory only.

Correct Answer: AD

Reference: https://whitesource.atlassian.net/wiki/spaces/WD/pages/34209870/NPM+Plugin

https://nodejs.org/en/knowledge/getting-started/npm/what-is-the-file-package-json

**QUESTION 3**

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure DevOps organization named Contoso and an Azure subscription. The subscription contains an Azure virtual machine scale set named VMSS1 that is configured for autoscaling.

You have a project in Azure DevOps named Project1. Project1 is used to build a web app named App1 and deploy App1 to VMSS1.

You need to ensure that an email alert is generated whenever VMSS1 scales in or out.

Solution: From Azure Monitor, configure the autoscale settings.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead create an action group.

Note: An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor, Service Health and Azure Advisor alerts use action groups to notify users that an alert has been triggered.

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups

**QUESTION 4**

You use Azure Pipelines to build and test code projects.

You notice an increase in cycle times.

You need to identify whether agent pool exhaustion is causing the issue.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Query the PipelineRun/PipelineRuns endpoint.

B. Query the TaskAgentPoolSizeSnapshots endpoint.

C. View the Pipeline duration report.

D. View the pool consumption report at the organization level.

Correct Answer: BD

**QUESTION 5**

You have a GitHub repository that is integrated with Azure Boards. Azure Boards has a work item that has the number 715.

You need to ensure that when you commit source code in GitHub, the work item is updated automatically.

What should you include in the commit comments?

A. the URL of the work item

B. AB#715

C. @715

D. #715

Correct Answer: B

Link GitHub commits, pull requests, and issues to work items in Azure Boards

Use AB# mention to link from GitHub to Azure Boards work items

From a GitHub commit, pull request or issue, use the following syntax to create a link to your Azure Boards work item. Enter the AB#ID within the text of a commit message. Or, for a pull request or issue, enter the AB#ID within the title or

description (not a comment).

AB#{ID}

For example, AB#125 will link to work item ID 125.

Reference:

https://learn.microsoft.com/en-us/azure/devops/boards/github/link-to-from-github

**QUESTION 6**

You manage a project by using Azure Board, and you manage the project code by using Azure Repos.

You have a bug work item that has an ID of 123.

You need to set the work item state to Resolved.

What should you add to the commit message?

A. #123 completes

B. Resolves #AB-123

C. Verifies #123

D. Fixes #123

Correct Answer: D

Resolve work items on commit

Close work items by mentioning keywords in commit messages. When you mention a work item in a commit that makes it to the default branch via one of the supported workflows, we will attempt to resolve that work item.

Keywords

The three supported keywords to trigger a resolution mention are fix, fixes, and fixed (case insensitive). Optionally, a colon can follow the keyword. Most forms of punctuation can precede or proceed the resolution mention, excluding another

pound sign (#).

Examples

Fixes #123

This fixed #123!

Change behavior to fix: #123

Fixes #123 and fixes #124

Reference:

https://learn.microsoft.com/en-us/azure/devops/repos/git/resolution-mentions

---

**QUESTION 7**

You have an Azure key vault named KV1 and three web servers.

You plan to deploy an app named App1 to the web servers.

You need to ensure that App1 can retrieve a secret from KV1. The solution must meet the following requirements:

1.

Minimize the number of permission grants required.

2.

Follow the principle of least privilege. What should you include in the solution?

A. role-based access control (RBAC) permission

B. a system-assigned managed identity

C. a user-assigned managed identity

D. a service principal

Correct Answer: C

Grant yourself data plane access to the Key Vault

Step 1: Set access policy.

Set access policy.

1.

Go to the Azure Portal and log in using your Azure account

2.

Search for your Key Vault in Search Resources dialog box

3.

Select Overview > Access policies

4.

Click on Add Access Policy > Secret permissions > Get

5.

Click on Select Principal, add your account and pre created system-assigned identity

6.

Click on "OK" to add the new Access Policy, then click "Save" to save the Access Policy

Etc.

Note: You can use a managed identity to connect Key Vault to an Azure web app in .NET.

Azure Key Vault provides a way to store credentials and other secrets with increased security. But your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources help to solve this problem by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having to display credentials in your code.

A managed identity automatically manages application credentials.

While developers can securely store the secrets in Azure Key Vault, services need a way to access Azure Key Vault. Managed identities provide an automatically managed identity in Microsoft Entra ID for applications to use when connecting

to resources that support Microsoft Entra authentication. Applications can use managed identities to obtain Microsoft Entra tokens without having to manage any credentials.

Managed identity types

There are two types of managed identities:

System-assigned. Some Azure resources, such as virtual machines allow you to enable a managed identity directly on the resource.

User-assigned. You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more Azure Resources.

Reference:

https://learn.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app
https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

---

**QUESTION 8**

You have a project in Azure DevOps named Project1 that references an Azure Artifacts feed named Feed1. You have a package named Package1 that has the versions shown in the following table.

| Version | Description |
|---|---|
| 1.0.3 | Manually pushed to Feed1 |
| 1.4.0 | Manually pushed to Feed1 |
| 2.0.0 | Available from an upstream source |
| 2.3.1 | Saved from an upstream source |

You need to perform a build of Project1.

Which version of Package1 will be used?

A. 1.0.3

B. 1.4.0

C. 2.0.0

D. 2.3.1

Correct Answer: C

Reference: https://learn.microsoft.com/en-us/azure/devops/artifacts/concepts/upstream-sources

---

**QUESTION 9**

You have been tasked with strengthening the security of your team\\'s development process.

You need to suggest a security tool type for the Continuous Integration (CI) phase of the development process.

Which of the following is the option you would suggest?

A. Penetration testing

B. Static code analysis

C. Threat modeling

D. Dynamic code analysis

Correct Answer: B

Validation in the CI/CD begins before the developer commits his or her code. Static code analysis tools in the IDE provide the first line of defense to help ensure that security vulnerabilities are not introduced into the CI/CD process.

Reference: https://docs.microsoft.com/en-us/azure/devops/articles/security-validation-cicd-pipeline?view=vsts

**QUESTION 10**

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to use an Azure Pipelines pipeline to test an app. The solution meet the following requirements:

1.

The pipeline must fail if any tests fail.

2.

The test results must be published to the pipeline.

3.

The test for every pipeline run must be triggered unless the pipeline is cancelled. Solution: You include the following elements in the YAML definition of the pipeline.

```
...
- task: PublishTestResults@2
displayName: 'Publish Unit Test Results'
condition: succeededOrFailed()
inputs:
testResultsFormat: 'JUnit'
testResultsFiles: '**/junit.xml'
failTaskOnFailureToPublishResults: true
testRunTitle: 'App Test'
...
```

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

**QUESTION 11**

You have an Azure subscription that contains four Azure virtual machines

You need to configure the virtual machines to use a single identity. The solution must meet the following requirements:

Ensure that the credentials for the identity are managed automatically. Support granting privileges to the identity.

Which type of identity should you use?

A. a service principal

B. a user-assigned managed identity

C. a system-assigned managed identity

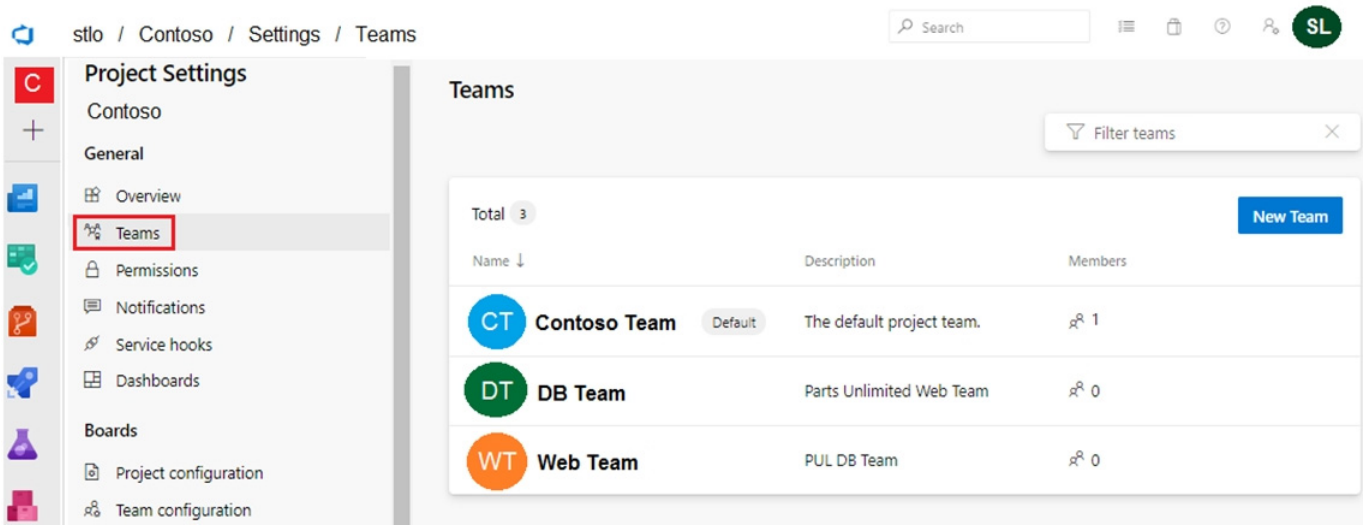
D. a user account

Correct Answer: B

**QUESTION 12**

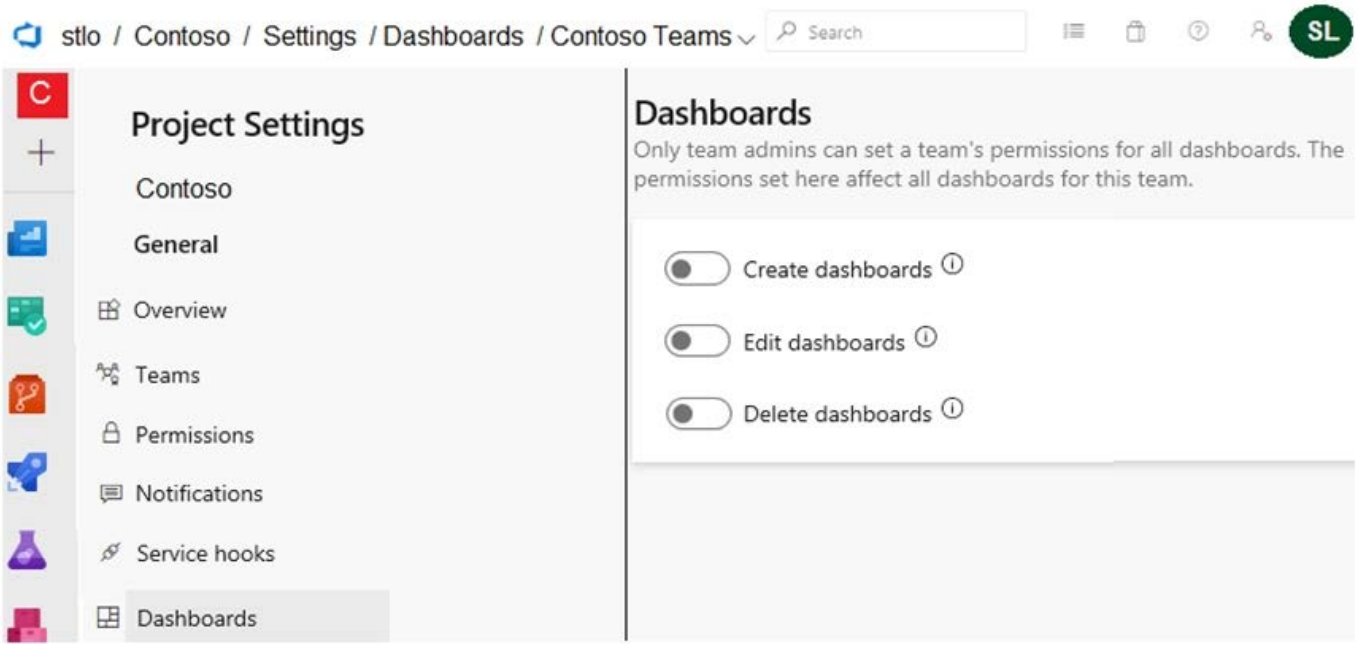
HOTSPOT

You have a project in Azure DevOps that has three teams as shown in the Teams exhibit. (Click the Teams tab.)




You create a new dashboard named Dash1.

You configure the dashboard permissions for the Control project as shown in the Permissions exhibit. (Click the Permissions tab.)




All other permissions have the default values set.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

| Statements | Yes | No |
|---|---|---|
| Web Team can delete Dash1. | ○ | ○ |
| Contoso Team can view Dash1. | ○ | ○ |
| Project administrators can create new dashboards. | ○ | ○ |

Correct Answer:

## Answer Area

| Statements | Yes | No |
|---|---|---|
| Web Team can delete Dash1. | ○ | ● |
| Contoso Team can view Dash1. | ● | ○ |
| Project administrators can create new dashboards. | ● | ○ |

Reference: https://docs.microsoft.com/en-us/azure/devops/report/dashboards/charts-dashboard-permissions-access

**QUESTION 13**

You use Azure Artifacts to host NuGet packages that you create.

You need to make one of the packages available to anonymous users outside your organization. The solution must minimize the number of publication points.

What should you do?

A. Change the feed URL of the package

B. Create a new feed for the package

C. Promote the package to a release view.

D. Publish the package to a public NuGet repository.

Correct Answer: B

Azure Artifacts introduces the concept of multiple feeds that you can use to organize and control access to your packages.

Packages you host in Azure Artifacts are stored in a feed. Setting permissions on the feed allows you to share your packages with as many or as few people as your scenario requires.

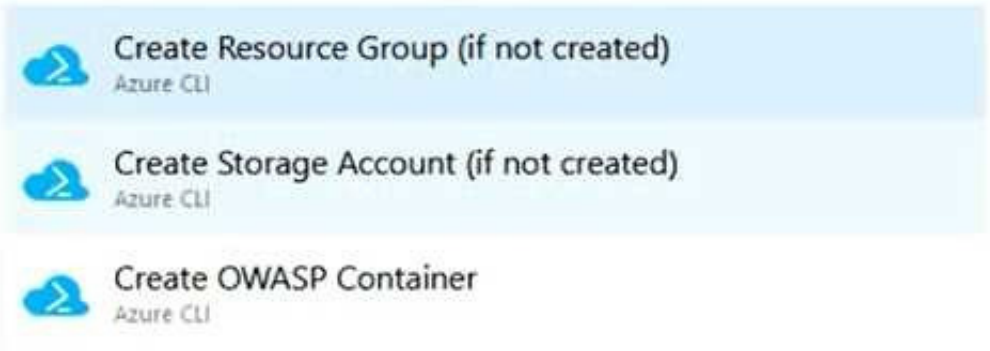
Feeds have four levels of access: Owners, Contributors, Collaborators, and Readers.

References: https://docs.microsoft.com/en-us/azure/devops/artifacts/feeds/feed-permissions?view=vstsandtabs=new-nav

**QUESTION 14**

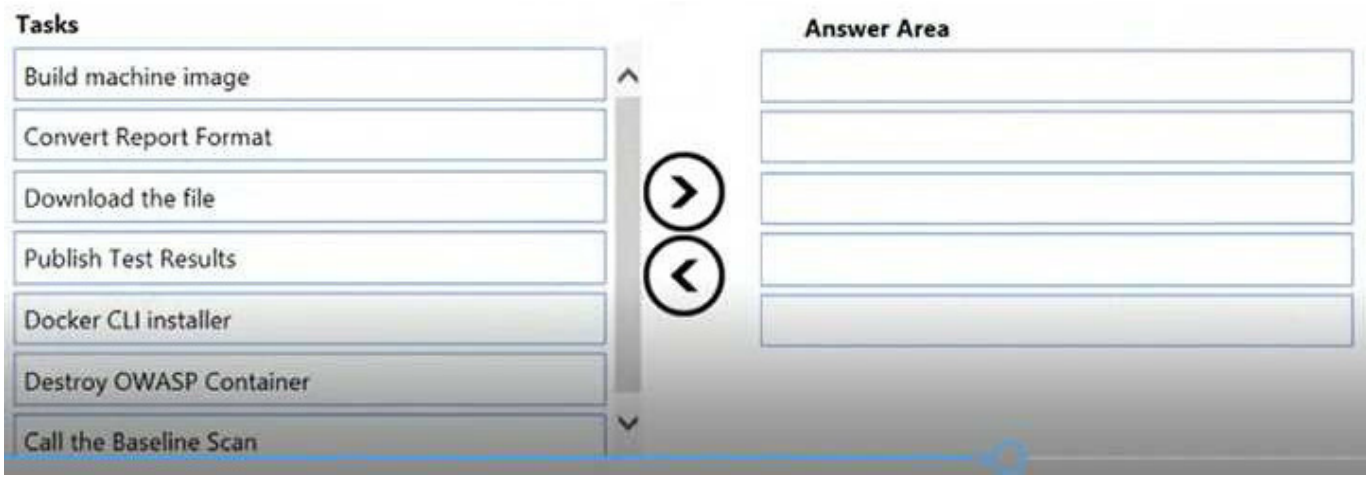
DRAG DROP

You have an Azure DevOps release pipeline as shown in the following exhibit.

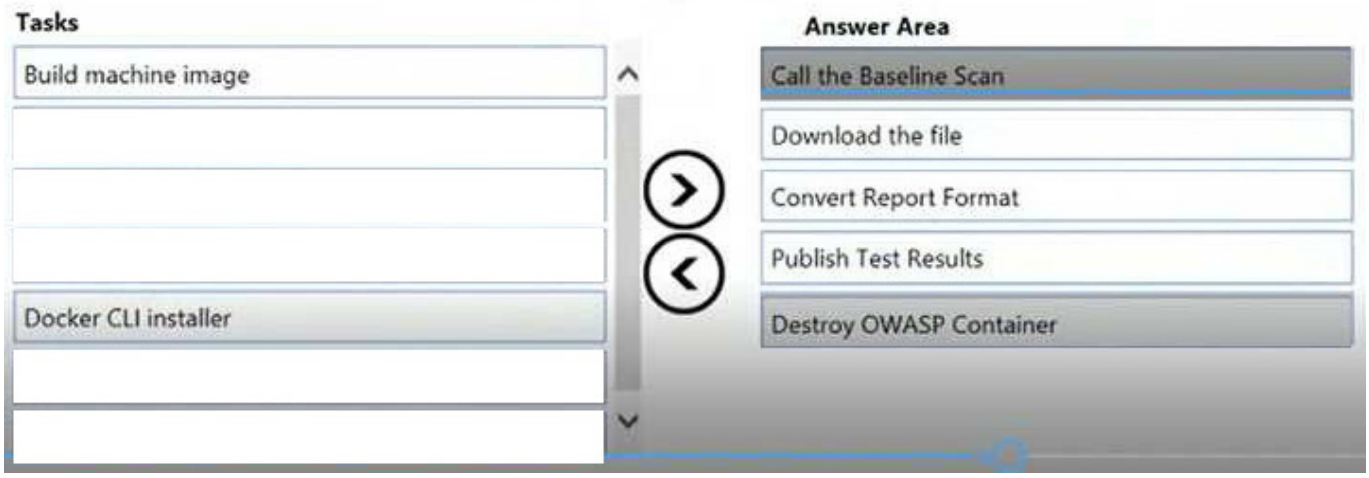


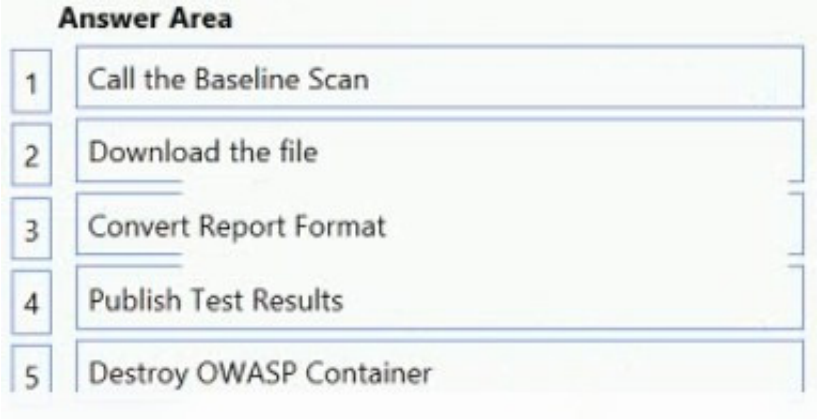

You need to complete the pipeline to configure OWASP ZAP for security testing. Which five Azure CLI tasks should you add in sequence? To answer, move the tasks from the list of tasks to the answer area and arrange them in the correct order.

Select and Place:



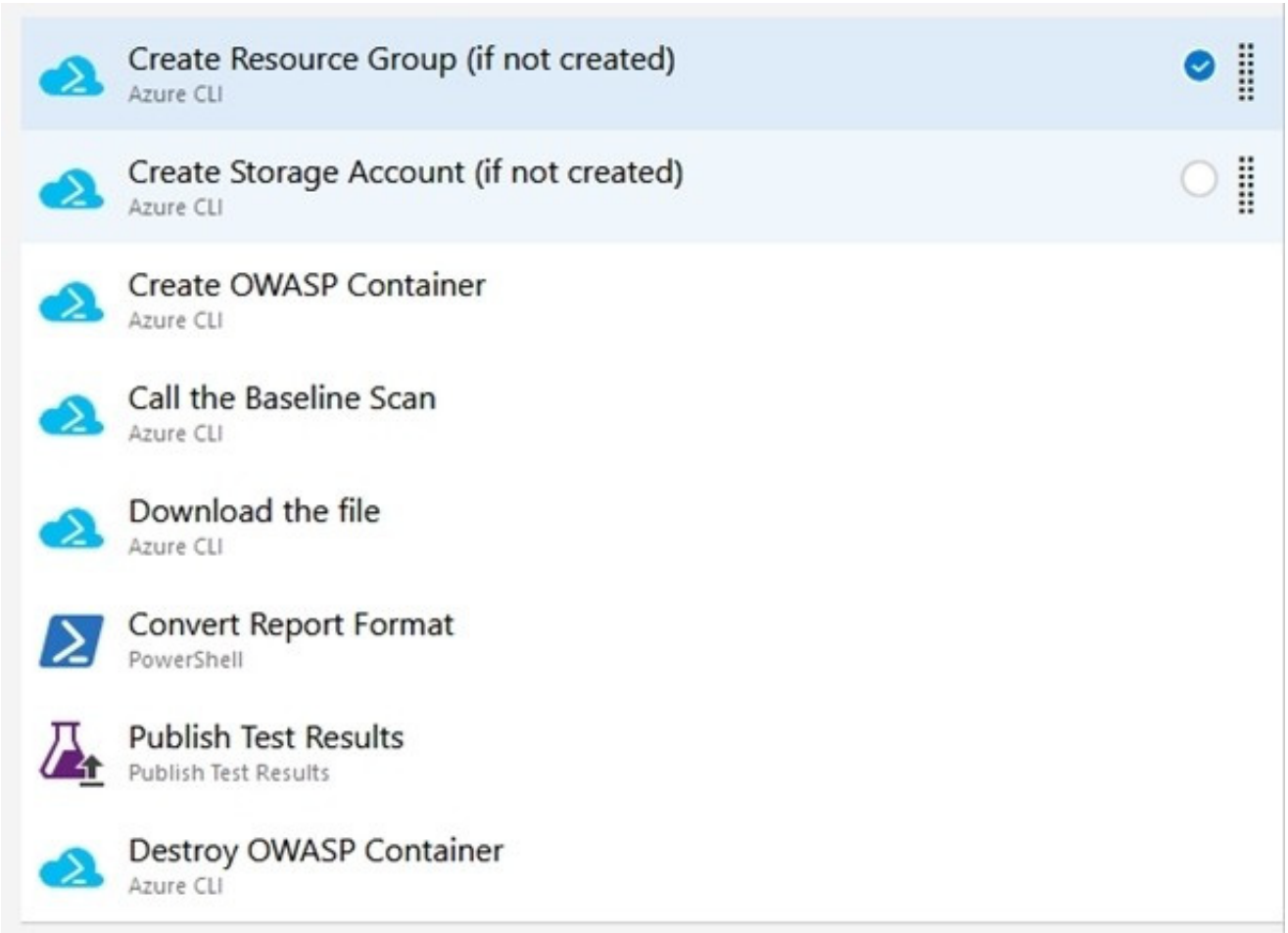

Correct Answer:






Defining the Release Pipeline Once the application portion of the Release pipeline has been configured, the security scan portion can be defined. In our example, this consists of 8 tasks, primarily using the Azure CLI task to create and use the ACI instance (and supporting structures).

Otherwise specified, all the Azure CLI tasks are Inline tasks, using the default configuration options.




**QUESTION 15**

You add the virtual machines as managed nodes in Azure Automation State Configuration.

You need to configure the computers in Pool7.

What should you do?

A. Modify the RefreshMode property of the Local Configuration Manager (LCM).

B. Run the Register-AzureRmAutomationDscNode Azure Powershell cmdlet.

C. Modify the ConfigurationMode property of the Local Configuration Manager (LCM)

D. Install PowerShell Core.

Correct Answer: C