Correct Answer: D
Explanation:
Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

▪ Role Assignments
▪ Policy Assignments
▪ Azure Resource Manager templates
▪ Resource Groups

Reference:
https://docs.microsoft.com/en-us/azure/governance/blueprints/overview

QUESTION 35
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 have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Explanation:
Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.

Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the

shared access signatures associated with it.

References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

QUESTION 36
DRAG DROP
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

Correct Answer:

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

QUESTION 37
HOTSPOT
You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

How should you configure the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and  [        ▼]  ==4625
                                      ActivityID
                                      DataType
                                      EventID
                                      QuantityUnit

| Summarie failed_login_attempts=  [        ▼]
                                    Count(),
                                    Countif(),
                                    Makeset(),
                                    Split(),

    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

Correct Answer:

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and  [        ▼]  ==4625
                                      ActivityID
                                      DataType
                                      EventID
                                      QuantityUnit

| Summarie failed_login_attempts=  [        ▼]
                                    Count(),
                                    Countif(),
                                    Makeset(),
                                    Split(),

    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

QUESTION 38
Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.
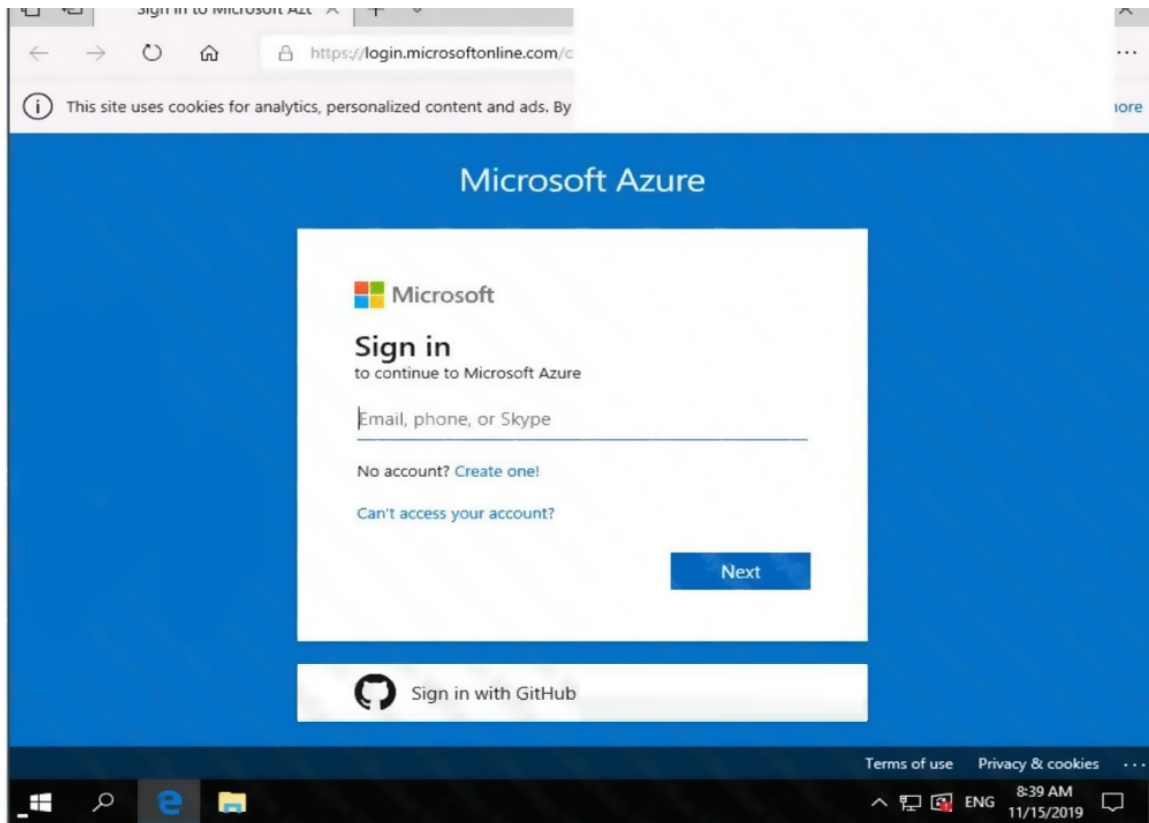
To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168