AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.passapply.com/az-500.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 subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

A. Azure DevOps

B. Azure Application Insights

C. Azure Monitor

D. Azure Logic Apps Designer

Correct Answer: D

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References: https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

---

QUESTION 2

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You plan to enable passwordless authentication for the tenant.

You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security administrator

B. Privileged role administrator

C. Authentication administrator

D. Global administrator

Correct Answer: C

Authentication Administrator.

Users with this role can set or reset any authentication method (including passwords) for non-administrators and some roles. Authentication Administrators can require users who are non-administrators or assigned to some roles to re-

register

against existing non-password credentials (for example, MFA or FIDO), and can also revoke remember MFA on the device, which prompts for MFA on the next sign-in.

Note: Before combined registration, users registered authentication methods for Azure AD Multi-Factor Authentication and self-service password reset (SSPR) separately. People were confused that similar methods were used for Azure AD

Multi-Factor Authentication and SSPR but they had to register for both features. Now, with combined registration, users can register once and get the benefits of both Azure AD Multi-Factor Authentication and SSPR.

Azure Active Directory role enable the combined registration experience

Incorrect:

Privileged Role Administrator.

Users with this role can manage role assignments in Azure Active Directory, as well as within Azure AD Privileged Identity Management. They can create and manage groups that can be assigned to Azure AD roles. In addition, this role

allows management of all aspects of Privileged Identity Management and administrative units.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#privileged-role-administrator

---

QUESTION 3

SIMULATION

You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

To complete this task, sign in to the Azure portal.

A. See the explanation below.

Correct Answer: A

Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment

1.

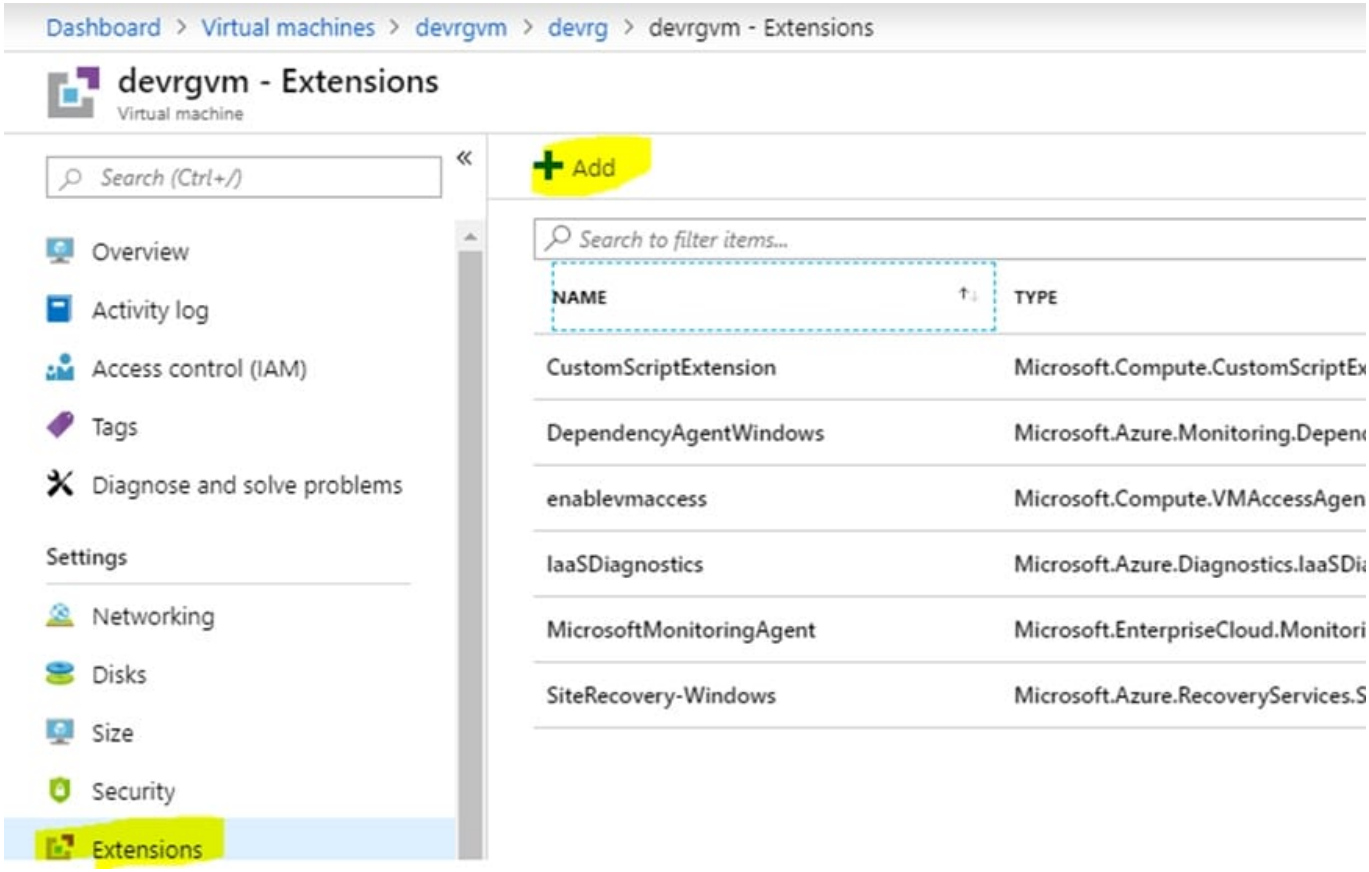
In Azure Portal, go to the Azure VM1\\'s blade, navigate to the Extensions section and press Add.

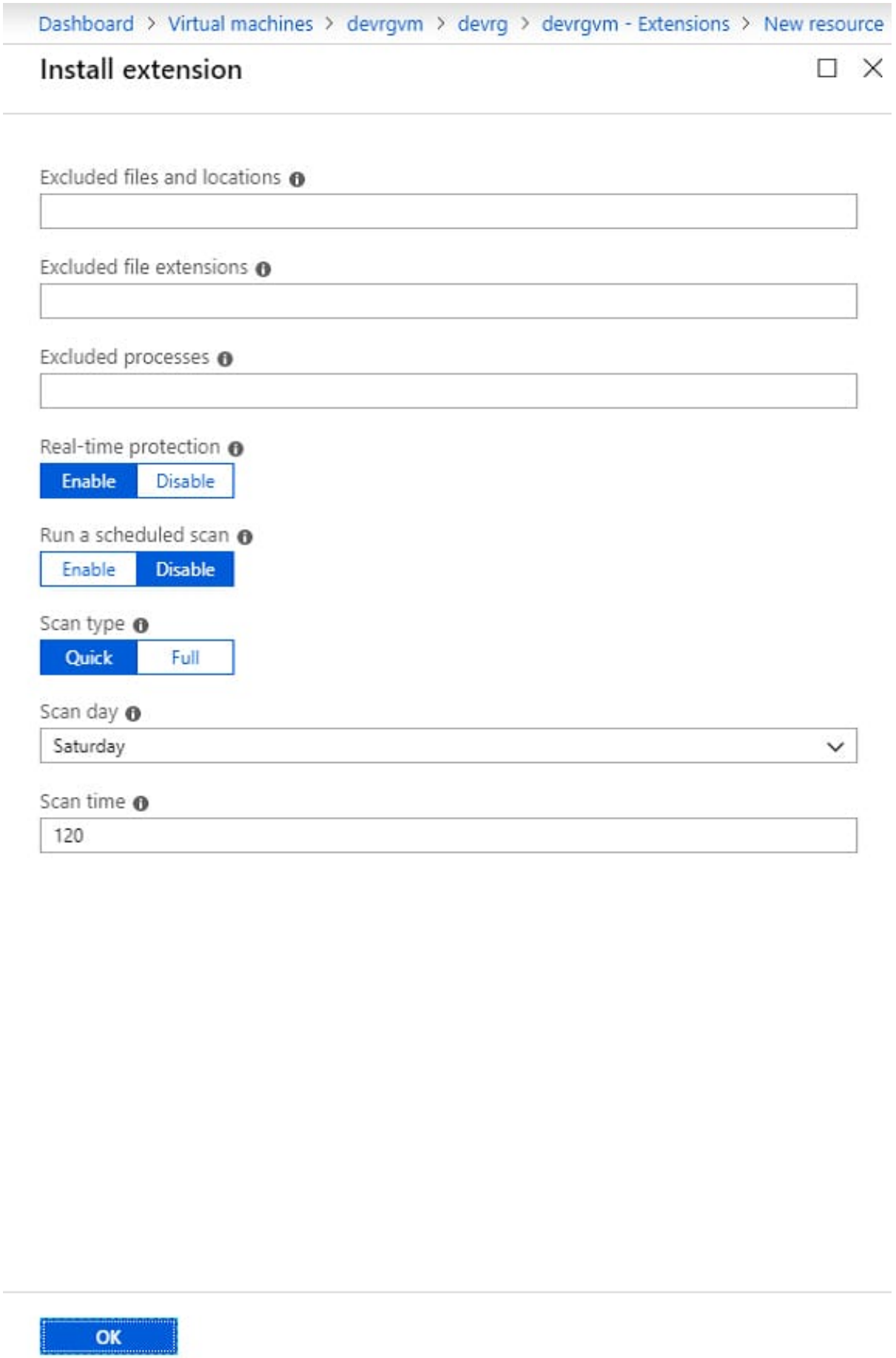
2.

Select the Microsoft Antimalware extension and press Create.

3.

Fill the “Install extension” form as desired and press OK. Scheduled: Enable Scan type: Full Scan day: Sunday




Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions > New resource
Install extension
Excluded files and locations
Excluded file extensions
Excluded processes
Real-time protection
Enable
Disable
Run a scheduled scan
Enable
Disable
Scan type
Quick
Full
Scan day
Saturday
Scan time
120
OK

Reference: https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/

QUESTION 4

References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
  "if" : {
   "allOf": [
      {
     "field" : "type",
     "equals": "Microsoft.Compute/virtualMachines"
       }
       {
     "field" : "Microsoft.Compute/imageSKU",
          "equals" : "2016-Datacenter",
            }
        ]
     },
     "then" : {
          "effect" : "[ Append / Deny / DeployIfNotExists ]",
          "details" : {
           "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
           "roleDefinitionsIds" : [
            "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
           ],
           "name" : "customExtension",
           "deployment" : {
                "properties" : {
            "mode": "incremental",
            "parameters" : {
             },
             "[ existenceCondition / resources / template ]": {
               }
             }
          }
       }
    }
}
```

Correct Answer:

Answer Area

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.

Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

References:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

QUESTION 5

You have an Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.

You discover that vulnerability security scans were not performed.

You need to ensure that the images are scanned for vulnerabilities when they are uploaded to Registry1.

What should you do?

A. From the Azure portal modify the Pricing tier settings.

B. From Azure CLI, lock the container images.

C. Upload the container images by using AzCopy

D. Push the container images to Registry1 by using Docker

Correct Answer: A

Reference: https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/