Prüfungsnummer:AZ-800

Prüfungsname: Administering Windows Server Hybrid Core Infrastructure

Version:demo

Achtung: Aktuelle englische Version zu AZ-800 bei uns ist gratis!!

1.Sie haben eine Azure Active Directory Domain Services (Azure AD DS)-Domäne mit dem Namen it-pruefungen.de.

Sie müssen einem Administrator die Möglichkeit geben, Gruppenrichtlinienobjekte (GPOs) zu verwalten. Die Lösung muss das Prinzip der Vergabe geringstmöglicher Rechte verwenden.

Zu welcher Gruppe sollten Sie den Administrator hinzufügen?

A.AAD DC-Administratoren
B.Domänen-Admins
C.Schema-Admins
D.Organisations-Admins
E.Gruppenrichtlinien-Ersteller-Besitzer

Korrekte Antwort: A

Erläuterungen:

Einstellungen für Benutzer- und Computerobjekte in Azure Active Directory Domain Services (Azure AD DS) werden häufig über Gruppenrichtlinienobjekte (GPOs) verwaltet. Azure AD DS umfasst integrierte GPOs für die Container AADDC-Benutzer und AADDC-Computer. Sie können diese integrierten GPOs anpassen, um die Gruppenrichtlinie nach Bedarf für Ihre Umgebung zu konfigurieren. Mitglieder der Gruppe Azure AD DC-Administratoren haben Gruppenrichtlinien-Administratorrechte in der Azure AD DS-Domäne und können auch benutzerdefinierte Gruppenrichtlinienobjekte und Organisationseinheiten erstellen.

In einer Hybridumgebung werden die in einer lokalen AD DS-Umgebung konfigurierten Gruppenrichtlinien nicht mit Azure AD DS synchronisiert. Um Konfigurationseinstellungen für Benutzer oder Computer in Azure AD DS zu definieren, bearbeiten Sie eines der Standard-Gruppenrichtlinienobjekte, oder erstellen Sie ein benutzerdefiniertes Gruppenrichtlinienobjekt.

Anmerkung: In einer Windows Server Active Directory Domain Services (AD DS)-Domäne würden wir den Administrator zur Gruppe Richtlinien-Ersteller-Besitzer hinzufügen.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Verwalten von Gruppenrichtlinien in einer von Azure Active Directory Domain Services verwalteten Domäne

2.Sie erstellen ein neues Azure-Abonnement.

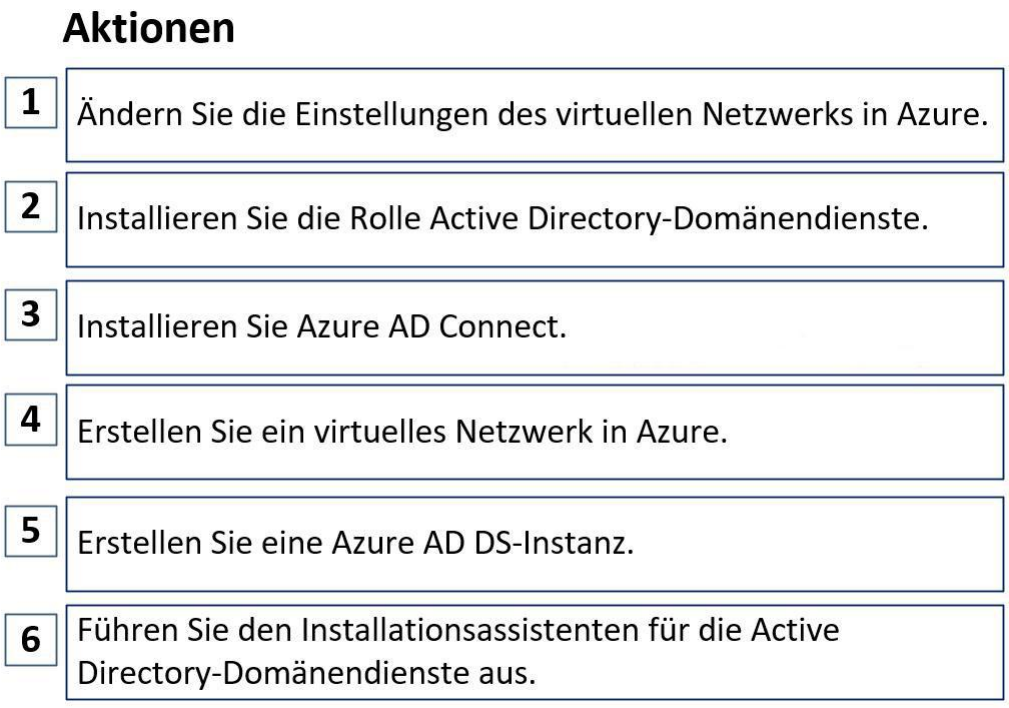
Sie planen, Azure Active Directory Domain Services (Azure AD DS) und virtuelle Computer in Azure bereitzustellen. Die virtuellen Computer werden mit Azure AD DS verbunden.

Sie müssen die Active Directory-Domänendienste (AD DS) bereitstellen, um sicherzustellen, dass die virtuellen Computer bereitgestellt und Azure AD DS hinzugefügt werden können.

Welche drei Schritte führen Sie in Reihenfolge aus?

(Die verfügbaren Aktionen werden in der Abbildung dargestellt. Klicken Sie auf die Schaltfläche Zeichnung und ordnen Sie die erforderlichen Schritte in der richtigen Reihenfolge an.)

Abbildung



A.Reihenfolge: 2, 6, 3
B.Reihenfolge: 4, 5, 6
C.Reihenfolge: 4, 5, 1

D.Reihenfolge: 4, 1, 3

Korrekte Antwort: C

Erläuterungen:

Azure Active Directory Domain Services (Azure AD DS) stellt verwaltete Domänendienste bereit, z. B. Domänenbeitritt, Gruppenrichtlinie, LDAP und Kerberos-/NTLM-Authentifizierung, die mit Windows Server Active Directory vollständig kompatibel sind. Sie können diese Domänendienste nutzen, ohne selbst Domänencontroller bereitstellen, verwalten und patchen zu müssen. Azure AD DS lässt sich in Ihren vorhandenen Azure AD-Mandanten integrieren. Dank dieser Integration können Benutzer sich mit ihren Unternehmensanmeldeinformationen anmelden, und Sie können vorhandene Gruppen und Benutzerkonten verwenden, um den Zugriff auf Ressourcen zu sichern.

Zuerst müssen wir ein virtuelles Netzwerk und ein Subnetz in Azure erstellen. Im zweiten Schritt stellen wir Azure AD DS im virtuellen Netzwerk bereit und im dritten Schritt ändern wir die DNS-Servereinstellungen des virtuellen Netzwerks so, dass auf die AAD DS-Domänencontroller verwiesen wird. Sobald wir die Bereitstellung abgeschlossen haben, können wir virtuelle Azure-Computer im virtuellen Netzwerk bereitstellen und sie der verwalteten Azure AD DS Domäne hinzufügen.

Eine Windows Server Active Directory-Domänendienste (AD DS)-Domäne wird für dieses Szenario nicht benötigt.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Tutorial: Erstellen und Konfigurieren einer verwalteten Azure Active Directory Domain Services-Domäne

3.Sie haben eine Azure Active Directory Domain Services (Azure AD DS)-Domäne.

Sie erstellen einen neuen Benutzer mit dem Namen Admin1.

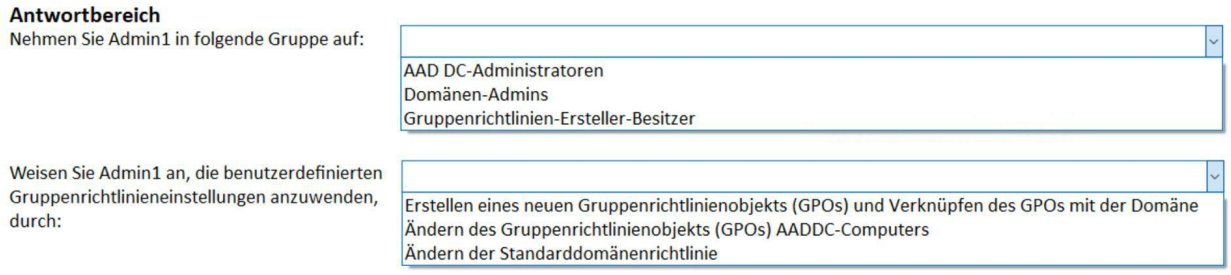
Sie müssen Admin1 ermöglichen, benutzerdefinierte Gruppenrichtlinieneinstellungen auf allen Computern in der Domäne bereitzustellen. Ihre Lösung muss das Prinzip der Vergabe geringstmöglicher Rechte verwenden.

Was sollten Sie in die Lösung einbeziehen?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich

aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung



A.Nehmen Sie Admin1 in folgende Gruppe auf: AAD DC-Administratoren
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Ändern des Gruppenrichtlinienobjekts (GPOs) AADDC-Computers
B.Nehmen Sie Admin1 in folgende Gruppe auf: AAD DC-Administratoren
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Erstellen eines neuen Gruppenrichtlinienobjekts (GPOs) und Verknüpfen des GPOs mit der Domäne
C.Nehmen Sie Admin1 in folgende Gruppe auf: Domänen-Admins
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Ändern der Standarddomänenrichtlinie
D.Nehmen Sie Admin1 in folgende Gruppe auf: Domänen-Admins
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Erstellen eines neuen Gruppenrichtlinienobjekts (GPOs) und Verknüpfen des GPOs mit der Domäne
E.Nehmen Sie Admin1 in folgende Gruppe auf: Gruppenrichtlinien-Ersteller-Besitzer
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Ändern des Gruppenrichtlinienobjekts (GPOs) AADDC-Computers
F.Nehmen Sie Admin1 in folgende Gruppe auf: Gruppenrichtlinien-Ersteller-Besitzer
Weisen Sie Admin1 an, die benutzerdefinierten Gruppenrichtlinieneinstellungen anzuwenden, durch: Ändern der Standarddomänenrichtlinie

Korrekte Antwort: A

Erläuterungen:

Einstellungen für Benutzer- und Computerobjekte in Azure Active Directory Domain Services (Azure AD DS) werden häufig über Gruppenrichtlinienobjekte (GPOs) verwaltet. Azure AD DS umfasst integrierte GPOs für die Container AADDC-Benutzer und AADDC-Computer. Sie können diese integrierten GPOs anpassen, um die Gruppenrichtlinie nach Bedarf für Ihre Umgebung zu konfigurieren. Mitglieder der Gruppe Azure AD DC-Administratoren haben Gruppenrichtlinien-Administratorrechte in der Azure AD DS-Domäne und können auch benutzerdefinierte Gruppenrichtlinienobjekte und Organisationseinheiten erstellen.

In einer Hybridumgebung werden die in einer lokalen AD DS-Umgebung konfigurierten Gruppenrichtlinien nicht mit Azure AD DS synchronisiert. Um Konfigurationseinstellungen für Benutzer oder Computer in Azure AD DS zu definieren, bearbeiten Sie eines der Standard-Gruppenrichtlinienobjekte, oder erstellen Sie ein benutzerdefiniertes Gruppenrichtlinienobjekt.

Anmerkung: In einer Windows Server Active Directory Domain Services (AD DS)-Domäne würden wir den Administrator zur Gruppe Richtlinien-Ersteller-Besitzer hinzufügen.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Verwalten von Gruppenrichtlinien in einer von Azure Active Directory Domain Services verwalteten Domäne

4.Sie haben 10 On-Premises Server, auf denen Windows Server ausgeführt wird.

Sie planen, Azure-Netzwerkadapter zu verwenden, um die Server mit den Ressourcen in Azure zu verbinden.

Welche Voraussetzungen benötigen Sie On-Premises und in Azure?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

A.Um die On-Premises Server zu konfigurieren, verwenden Sie: Azure CLI
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Einen privaten Endpunkt

B.Um die On-Premises Server zu konfigurieren, verwenden Sie: Routing und Remote Access
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Azure Bastion
C.Um die On-Premises Server zu konfigurieren, verwenden Sie: Server-Manager
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Azure Firewall
D.Um die On-Premises Server zu konfigurieren, verwenden Sie: Server-Manager
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Azure Bastion
E.Um die On-Premises Server zu konfigurieren, verwenden Sie: Windows Admin Center
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Einen öffentlichen Azure Load Balancer
F.Um die On-Premises Server zu konfigurieren, verwenden Sie: Windows Admin Center
Um die Azure-Ressourcen und Azure-Netzwerkadapter zu verbinden, verwenden Sie: Ein Gateway für virtuelle Netzwerke

Korrekte Antwort: F

Erläuterungen:

Viele Workloads, die lokal und in Multi-Cloud-Umgebungen ausgeführt werden, erfordern Verbindungen zu virtuellen Computern (VMs), die in Microsoft Azure ausgeführt werden. Sie haben mehrere Möglichkeiten, einen Server mit einem Azure Virtual Network zu verbinden, beispielsweise Site-to-Site-VPN, Azure Express Route und Point-to-Site-VPN.

Windows Admin Center und der Azure-Netzwerkadapter bieten die Möglichkeit, den Server mit nur einem Mausklick über eine Point-to-Site-VPN-Verbindung mit Ihrem virtuellen Netzwerk zu verbinden. Der Prozess automatisiert die Konfiguration des virtuellen Netzwerkgateways und des lokalen VPN-Clients.

Die Verwendung eines Azure-Netzwerkadapters für die Verbindung mit einem virtuellen Netzwerk erfordert Folgendes:

Ein Azure-Konto mit mindestens einem aktiven Abonnement.
Ein vorhandenes virtuelles Netzwerk.
Internetzugriff für die Zielserver, die Sie mit dem virtuellen Azure-Netzwerk verbinden möchten.
Eine Windows Admin Center-Verbindung zu Azure.
Die neueste Version von Windows Admin Center.
Wenn es kein vorhandenes Azure Virtual Network-Gateway gibt, wird eines von Windows Admin Center für Sie erstellt. Dieser Setupvorgang kann bis zu 25 Minuten dauern. Nachdem der Azure-Netzwerkadapter erstellt wurde, können Sie direkt von Ihrem Server aus auf VMs im virtuellen Netzwerk zugreifen.

Wenn Sie die Konnektivität nicht mehr benötigen, wählen Sie unter Netzwerke den Azure-Netzwerkadapter aus, den Sie trennen möchten, wählen Sie im oberen Menü Trennen und dann im Popupfenster VPN trennen-Bestätigung die Option Ja aus.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Verwenden des Azure-Netzwerkadapters, um einen Server mit einem Azure Virtual Network zu verbinden

5.Sie haben einen Server mit dem Namen Server1. Auf Server1 ist das Windows Admin Center installiert. Das von Windows Admin Center verwendete Zertifikat wurde von einer Zertifizierungsstelle (CA) bezogen.

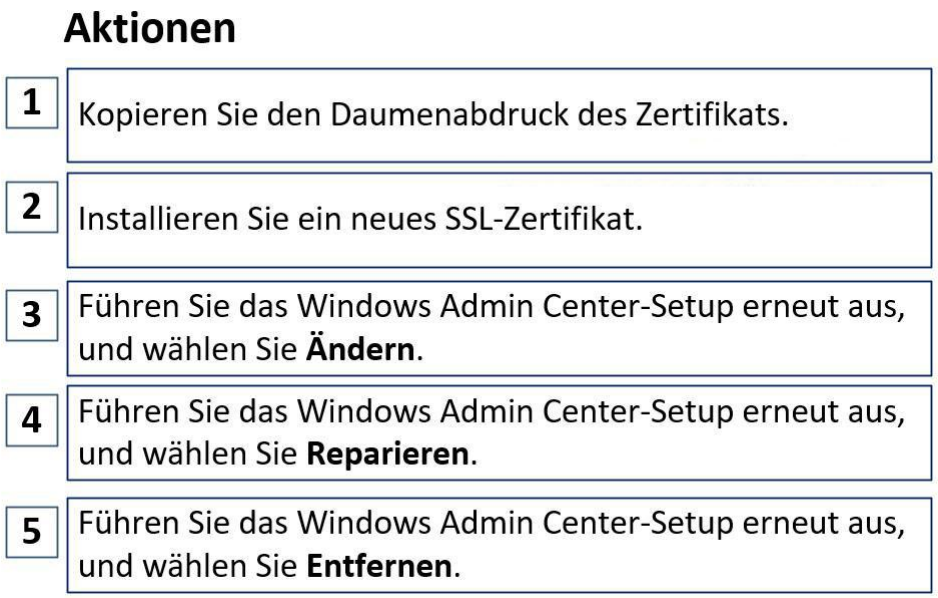
Das Zertifikat läuft ab.

Sie müssen das Zertifikat ersetzen.

Welche drei Schritte führen Sie in Reihenfolge aus?

(Die verfügbaren Aktionen werden in der Abbildung dargestellt. Klicken Sie auf die Schaltfläche Zeichnung und ordnen Sie die erforderlichen Schritte in der richtigen Reihenfolge an.)

Abbildung



A.Reihenfolge: 5, 2, 1
B.Reihenfolge: 2, 1, 3

C.Reihenfolge: 2, 1, 4
D.Reihenfolge: 1, 5, 2

Korrekte Antwort: B

Erläuterungen:

Unter Windows Server wird Windows Admin Center als Netzwerkdienst installiert. Geben Sie den Port an, den der Dienst überwacht und dies erfordert ein Zertifikat für HTTPS. Das Installationsprogramm kann zu Testzwecken ein selbstsigniertes Zertifikat erstellen, oder Sie können den Fingerabdruck eines Zertifikats bereitstellen, der bereits auf dem Computer installiert ist. Wenn Sie das generierte Zertifikat verwenden, wird es den DNS-Namen des Servers entsprechen. Wenn Sie Ihr eigenes Zertifikat verwenden, stellen Sie sicher, dass der im Zertifikat angegebene Name mit dem Computernamen übereinstimmt (Platzhalterzertifikate werden nicht unterstützt). Sie haben die Option, Ihre TrustedHosts von Windows Admin Center verwalten zu lassen.

Wenn Sie Windows Admin Center als Dienst bereitgestellt haben, müssen Sie ein Zertifikat für HTTPS bereitstellen. Um dieses Zertifikat zu einem späteren Zeitpunkt zu aktualisieren, führen Sie das Installationsprogramm erneut aus, und wählen Sie Ändern aus.

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Installieren von Windows Admin Center

6.Sie haben einen On-Premises Windows Server mit dem Namen Server1. Server1 verfügt über eine Internetverbindung.

Sie haben ein Azure-Abonnement.

Sie müssen Server1 mithilfe von Azure Monitor überwachen.

Welche Ressourcen sollten Sie im Azure-Abonnement erstellen und was sollten Sie auf Server1 installieren?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

Antwortbereich

Im Abonnement erstellen:

- Ein Azure Files-Speicherkonto
- Einen Log Analytics-Arbeitsbereich
- Eine Azure SQL-Datenbank und eine Datenerfassungsregel
- Ein Azure Blob-Speicherkonto und eine Datenerfassungsregel

Auf Server1 installieren:

- Den Microsoft Monitoring Agenten (MMA)
- Das Log Analytics-Gateway
- Die Serverrolle Device Health Attestation

A.Im Abonnement erstellen: Ein Azure Files-Speicherkonto
Auf Server1 installieren: Den Microsoft Monitoring Agenten (MMA)
B.Im Abonnement erstellen: Ein Azure Files-Speicherkonto
Auf Server1 installieren: Die Serverrolle Device Health Attestation
C.Im Abonnement erstellen: Einen Log Analytics-Arbeitsbereich
Auf Server1 installieren: Das Log Analytics-Gateway
D.Im Abonnement erstellen: Einen Log Analytics-Arbeitsbereich
Auf Server1 installieren: Den Microsoft Monitoring Agenten (MMA)
E.Im Abonnement erstellen: Eine Azure SQL-Datenbank und eine Datenerfassungsregel
Auf Server1 installieren: Die Serverrolle Device Health Attestation
F.Im Abonnement erstellen: Ein Azure Blob-Speicherkonto und eine Datenerfassungsregel
Auf Server1 installieren: Das Log Analytics-Gateway

Korrekte Antwort: D

Erläuterungen:

Azure Monitor ist eine Lösung, die Telemetriedaten aus einer Vielzahl von Ressourcen sammelt, analysiert und verarbeitet, einschließlich Windows Server und VMs, sowohl On-Premises als auch in der Cloud.

Daten, die von lokalen Windows Servern generiert werden, werden in einem Log Analytics-Arbeitsbereich in Azure Monitor gesammelt. Sie können in einem Arbeitsbereich verschiedene Überwachungslösungen aktivieren. Dies sind Sätze von Logik, die Erkenntnisse für ein bestimmtes Szenario bieten. Überwachungslösungen, die in einem Arbeitsbereich aktiviert werden können, sind beispielsweise die Azure-Updateverwaltung, Azure Security Center und Azure Monitor für VMs.

Wenn Sie eine Überwachungslösung in einem Log Analytics-Arbeitsbereich aktivieren, beginnen alle Server, die an diesen Arbeitsbereich berichten, mit dem Sammeln von Daten, die für diese Lösung relevant sind, damit die Lösung Erkenntnisse für alle Server

im Arbeitsbereich generieren kann.

Um Telemetriedaten auf einem lokalen Server zu sammeln und in den Log Analytics-Arbeitsbereich zu pushen, erfordert Azure Monitor die Installation des Microsoft Monitoring Agent (MMA).

Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

Überwachen von Servern und Konfigurieren von Warnungen mit Azure Monitor