Prüfungsnummer:AZ-305

Prüfungsname:(deutsche Version und englische Version) Designing Microsoft Azure Infrastructure Solutions

Version:demo

https://www.itpruefungsfragen.de/

Achtung: Aktuelle englische Version zu AZ-305 bei uns ist gratis!!

1.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Das Unternehmen hat einen Azure Active Directory-Mandanten mit dem Namen it-pruefungen.de.

Der Mandant enthält eine Sicherheitsgruppe mit dem Namen Gruppe1. Gruppe1 ist für den Mitgliedschaftstyp "Zugewiesen" konfiguriert und hat 50 Mitglieder, darunter 20 Gastbenutzer.

Sie müssen eine Lösung zur Bewertung der Mitgliedschaften in Gruppe1 empfehlen. Die Lösung muss folgende Anforderungen erfüllen:
Die Bewertung muss automatisch alle drei Monate wiederholt werden.
Jedes Mitglied muss die Möglichkeit erhalten, selbst zu berichten, ob es weiterhin Mitglied in Gruppe1 sein muss.
Benutzer, die melden, dass sie nicht länger Mitglied von Gruppe1 sein müssen, müssen automatisch aus Gruppe1 entfernt werden.
Benutzer, die nicht zurückmelden, ob sie weiterhin Mitglied von Gruppe1 sein müssen, müssen automatisch aus Gruppe1 entfernt werden.
Was sollten Sie in Lösung einbeziehen?

A.Implementieren Sie Azure AD Identity Protection.
B.Ändern Sie den Mitgliedschaftstyp von Gruppe1 in "Dynamisch".
C.Erstellen Sie eine Zugriffsüberprüfung.
D.Implementieren Sie Azure AD Privileged Identity Management (PIM).

Korrekte Antwort: C

Erläuterungen:

Mithilfe von Azure Active Directory-Zugriffsüberprüfungen (Azure AD-Zugriffsüberprüfungen) können Organisationen Gruppenmitgliedschaften, den Zugriff auf Unternehmensanwendungen und Rollenzuweisungen effizient verwalten.Der Benutzerzugriff kann regelmäßig überprüft werden, um sicherzustellen, dass nur die richtigen Personen weiterhin Zugriff haben.

Zugriffsüberprüfungen in Azure Active Directory (Azure AD) unterstützen Ihre Organisation dabei, einen besseren Schutz des Netzwerks zu erreichen, indem der

Lebenszyklus des Ressourcenzugriffs verwaltet wird. Zugriffsüberprüfungen bieten folgende Möglichkeiten:

Planen regelmäßiger Überprüfungen oder Durchführen von Ad-hoc-Überprüfungen, um zu ermitteln, wer Zugriff auf bestimmte Ressourcen wie Anwendungen und Gruppen hat

Nachverfolgen von Überprüfungen, um Erkenntnisse zu gewinnen, sowie aus Gründen der Compliance oder der Einhaltung von Richtlinien

Delegieren von Überprüfungen an bestimmte Administratoren, Geschäftsinhaber oder Endbenutzer, die eine Notwendigkeit des fortwährenden Zugriffs selbst nachweisen können

Verwenden der Erkenntnisse, um effizient zu ermitteln, ob Benutzer weiterhin Zugriff haben sollen

Automatisieren der Überprüfungsergebnisse, z. B. Entfernen des Benutzerzugriffs auf Ressourcen

Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Was sind Azure AD-Zugriffsüberprüfungen?

Planen der Bereitstellung von Azure Active Directory-Zugriffsüberprüfungen

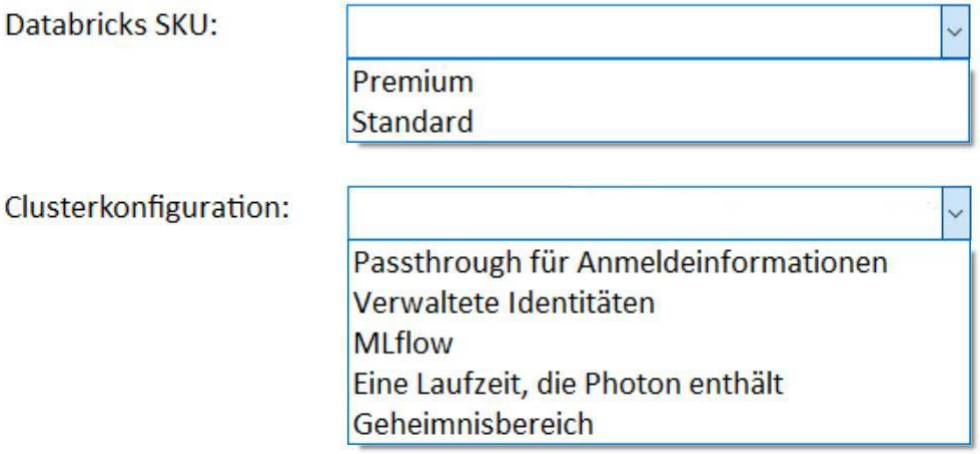
2.Sie planen, Azure Databricks bereitzustellen, um eine Anwendung für maschinelles Lernen zu unterstützen. Dateningenieure werden ein Azure Data Lake Storage-Konto in das Databricks-Dateisystem einbinden. Den Dateningenieuren sind Berechtigungen für Ordner im Data Lake direkt zugewiesen.

Sie müssen einen Entwurf für die geplante Databricks-Bereitstellung empfehlen. Ihre Lösung muss folgende Anforderungen erfüllen:
Sicherstellen, dass die Dateningenieure nur auf Ordner zugreifen können, für die sie Berechtigungen haben.
Der Entwicklungsaufwand muss minimiert werden.
Die Kosten müssen minimiert werden.
Was sollten Sie in die Empfehlung aufnehmen?

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

Abbildung

Antwortbereich



A.Databricks SKU: Premium
Clusterkonfiguration: Passthrough für Anmeldeinformationen
B.Databricks SKU: Premium
Clusterkonfiguration: Verwaltete Identitäten
C.Databricks SKU: Premium
Clusterkonfiguration: Geheimnisbereich
D.Databricks SKU: Standard
Clusterkonfiguration: Passthrough für Anmeldeinformationen
E.Databricks SKU: Standard
Clusterkonfiguration: MLflow
F.Databricks SKU: Standard
Clusterkonfiguration: Eine Laufzeit, die Photon enthält

Korrekte Antwort: A

Erläuterungen:

Azure Databricks ist eine Analyseplattform, die für die Microsoft Azure-Clouddienstplattform optimiert ist. Azure Databricks bietet drei Umgebungen für die Entwicklung datenintensiver Anwendungen: Databricks SQL, Databricks Data Science & Engineering und Databricks Machine Learning.

Databricks SQL stellt eine benutzerfreundliche Plattform für Analysten bereit, die SQL-Abfragen für ihren Data Lake erstellen, mehrere Visualisierungstypen zum Untersuchen von Abfrageergebnissen aus verschiedenen Perspektiven erstellen sowie Dashboards erstellen und freigeben möchten.

Sie können sich von Azure Databricks Clustern aus automatisch bei Azure Data Lake Storage Gen1 (ADLS Gen1) und Azure Data Lake Storage Gen2 (ADLS Gen2) authentifizieren, indem Sie dieselbe Azure Active Directory -Identität (Azure AD) verwenden, die Sie für die Anmeldung bei Azure Databricks verwenden. Wenn Sie Azure

Data Lake Storage Passthrough für Anmeldeinformationen für Ihren Cluster aktivieren, können Befehle, die Sie in diesem Cluster ausführen, Daten in Azure Data Lake Storage lesen und schreiben, ohne dass Sie Dienstprinzipal-Anmeldeinformationen für den Zugriff auf den Speicher konfigurieren müssen.

Azure Data Lake Storage Passthrough für Anmeldeinformationen wird nur mit Azure Data Lake Storage Gen1 und Gen2 unterstützt. Azure Blob Storage unterstützt keine Passthrough-Vorgehensweise für Anmeldeinformationen.

Azure Data Lake Storage Passthrough für Anmeldeinformationen erfordert einen Azure Databricks Premium Plan.

Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Zugreifen auf Azure Data Lake Storage mit Azure Active Directory Passthrough für Anmeldeinformationen

Was ist Azure Databricks?

3.Sie planen, eine Azure-Webanwendung mit dem Namen App1 bereitzustellen. Für den Zugriff auf App1 ist die erfolgreiche Authentifizierung durch Azure Active Directory erforderlich.

App1 wird von den Benutzern Ihres Unternehmens über das Internet aufgerufen. Alle Benutzer verfügen über Computer, auf denen Windows 10 ausgeführt wird und die mit Azure AD verbunden sind.

Sie müssen eine Lösung empfehlen, die sicherstellt, dass die Benutzer eine Verbindung mit App1 herstellen können, ohne zur Authentifizierung aufgefordert zu werden. Zudem darf der Zugriff auf App1 nur über unternehmenseigene Computer erfolgen.

Was sollten Sie für jede Anforderung empfehlen?

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

Abbildung

Antwortbereich

A.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Eine Azure AD-App-Registrierung
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Azure Richtlinie
B.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Eine Azure AD-App-Registrierung
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Eine Richtlinie für bedingten Zugriff
C.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Eine verwaltete Azure AD-Identität
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Azure Blueprints
D.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Eine verwaltete Azure AD-Identität
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Azure Anwendungsgateway
E.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Azure AD-Anwendungsproxy
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Eine Azure AD-Verwaltungseinheit
F.Die Benutzer können eine Verbindung mit App1 herstellen, ohne zur Authentifizierung aufgefordert zu werden: Azure AD-Anwendungsproxy
Die Benutzer können nur über unternehmenseigene Geräte auf App1 zugreifen: Azure Anwendungsgateway

Korrekte Antwort: B

Erläuterungen:

Anwendungsobjekte können, obwohl es Ausnahmen gibt, als die Definition einer Anwendung betrachtet werden. Anwendungsobjekte können im Azure-Portal über die Oberfläche App-Registrierungen verwaltet werden. Anwendungsobjekte stellen für Azure AD eine Beschreibung der Anwendung bereit und können als die Definition der

Anwendung betrachtet werden. Sie teilen dem Dienst basierend auf den Einstellungen der Anwendung mit, wie Token für die Anwendung ausgestellt werden müssen.Das Anwendungsobjekt ist nur in seinem Stammverzeichnis vorhanden. Dies gilt auch dann, wenn es sich um eine mehrinstanzenfähige Anwendung handelt, die Dienstprinzipale in anderen Verzeichnissen unterstützt.Das Anwendungsobjekt kann Folgendes enthalten (sowie zusätzliche Informationen, die hier nicht erwähnt werden):

Name, Logo und Herausgeber
Umleitungs-URIs
Geheimnisse (symmetrische und/oder asymmetrische Schlüssel für die Authentifizierung der Anwendung)
API-Abhängigkeiten (OAuth)
Veröffentlichte APIs/Ressourcen/Bereiche (OAuth)
App-Rollen (RBAC)
Metadaten und Konfiguration für einmaliges Anmelden (Single Sign-On, SSO)
Metadaten und Konfiguration für die Benutzerbereitstellung
Metadaten und Konfiguration für den Proxy
Anwendungen werden Azure AD hinzugefügt, damit sie die von Azure AD bereitgestellten Dienste nutzen können, beispielsweise:

Anwendungsauthentifizierung und -autorisierung
Benutzerauthentifizierung und -autorisierung
Einmaliges Anmelden (SSO) durch Verbund oder Kennwort
Benutzerbereitstellung und -synchronisierung
Rollenbasierte Zugriffssteuerung – Definition von Anwendungsrollen für rollenbasierte Autorisierungsprüfungen in einer Anwendung mithilfe des Verzeichnisses
OAuth-Autorisierungsdienste – werden von Microsoft 365 und anderen Microsoft-Anwendungen zum Autorisieren des Zugriffs auf APIs und Ressourcen verwendet
Anwendungsveröffentlichung und Proxy – Veröffentlichung einer Anwendung aus einem privaten Netzwerk im Internet
Verzeichnisschemaerweiterungs-Attribute: Erweitern Sie das Schema des Dienstprinzipals und von Benutzerobjekten, um zusätzliche Daten in Azure AD zu speichern.
Der bedingte Zugriff ist das Tool, das von Azure Active Directory verwendet wird, um Signale zusammenzuführen, Entscheidungen zu treffen und Organisationsrichtlinien zu erzwingen. Der bedingte Zugriff ist der Kern der neuen identitätsbasierten Steuerungsebene.

Die einfachsten Richtlinien für den bedingten Zugriff sind if-Anweisungen: Wenn ein Benutzer auf eine Ressource zugreifen möchte, muss er eine Aktion ausführen.Beispiel: Der Leiter der Lohnbuchhaltung möchte auf die Gehaltsabrechnungsanwendung zugreifen und muss für den Zugriff auf die Anwendung eine mehrstufige Authentifizierung durchführen.

Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Wie und warum werden Anwendungen zu Azure AD hinzugefügt?

Was ist bedingter Zugriff?

4.Sie entwerfen eine große Azure-Umgebung, die viele Abonnements enthält. Sie planen, Azure Policy als Teil einer Governance-Lösung zu verwenden.

Welchen drei Bereichen können Sie Azure-Richtliniendefinitionen zuweisen?

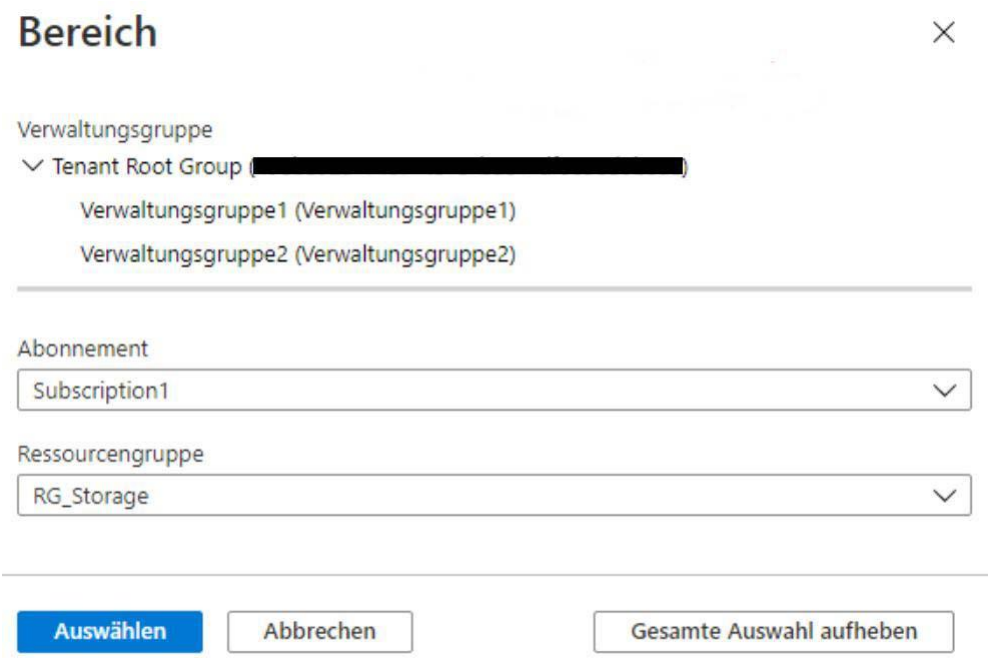
(Jede korrekte Antwort stellt eine vollständige Lösung dar. Wählen Sie zwei Antworten.)

A.Azure Active Directory (Azure AD)-Verwaltungseinheiten
B.Azure Active Directory (Azure AD)-Mandanten
C.Abonnements
D.Compute-Ressourcen
E.Ressourcengruppen
F.Verwaltungsgruppen

Korrekte Antwort: C, E, F

Erläuterungen:

Azure Policy wertet Ressourcen in Azure aus, indem die Eigenschaften dieser Ressourcen mit Geschäftsregeln verglichen werden. Diese im JSON-Format beschriebenen Geschäftsregeln werden als Richtliniendefinitionen bezeichnet. Um die Verwaltung zu vereinfachen, können mehrere Geschäftsregeln gruppiert werden, um eine Richtlinieninitiative (manchmal auch als Policy Set bezeichnet) zu bilden. Nachdem Ihre Geschäftsregeln erstellt wurden, wird die Richtliniendefinition oder -initiative jedem von Azure unterstützten Ressourcenbereich zugewiesen, z. B. Verwaltungsgruppen, Abonnements, Ressourcengruppen oder einzelnen Ressourcen. Die Zuweisung gilt für alle Ressourcen innerhalb des Resource Manager-Bereichs dieser Zuweisung. Unterbereiche können ggf. ausgeschlossen werden.



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

Was ist Azure Policy?

5.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Das Unternehmen hat eine Azure Active Directory (Azure AD)- Hybridbereitstellung.

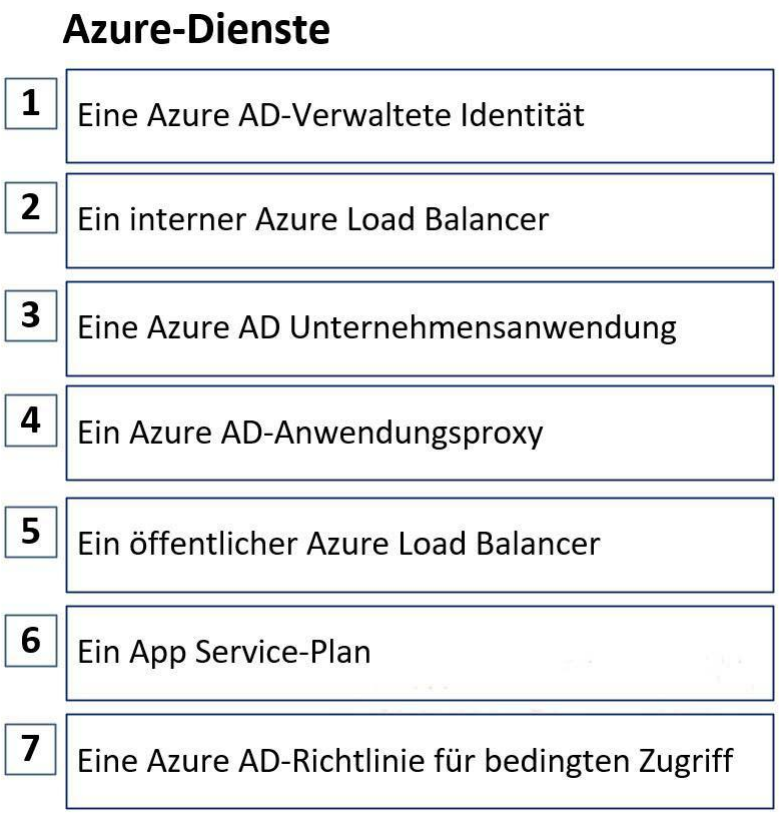
Das On-Premises Netzwerk des Unternehmens enthält einen Server mit dem Namen Server1. Server1 hostet eine ASP.NET-Anwendung mit dem Namen App1.

Sie müssen eine Lösung empfehlen, um sicherzustellen, dass sich Benutzer mit ihrem Azure AD-Konto und der Azure Multi-Faktor-Authentifizierung (MFA) anmelden, wenn sie über das Internet eine Verbindung zu App1 herstellen.

Welche drei Azure-Dienste sollten nacheinander bereitgestellt und konfiguriert werden?

(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, 7
B.Reihenfolge: 3, 4, 7
C.Reihenfolge: 6, 5, 7
D.Reihenfolge: 1, 6, 7

Korrekte Antwort: B

Erläuterungen:

Zunächst müssen wir App1 als Azure AD-Unternehmensanwendung registrieren. Im zweiten Schritt müssen wir einen Anwendungsproxy erstellen und mit dem internen und dem externen URL von App1 konfigurieren. Im letzten Schritt müssen wir die Multi-Faktor-Authentifizierung (MFA) für App1 mithilfe einer Richtlinie für bedingten Zugriff erzwingen.

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

Remotezugriff auf lokale Anwendungen über den Azure AD-Anwendungsproxy

6.Sie haben ein Azure-Abonnement, das ein Azure Blobspeicher-Konto mit dem Namen speicher1 enthält und Sie haben einen On-Premises Dateiserver mit dem Namen Server1, auf dem Windows Server 2016 ausgeführt wird. Server1 speichert 500 GB Unternehmensdaten.

Sie müssen eine Kopie der Dateien von Server1 in speicher1 speichern.

Welche zwei Azure-Dienste ermöglichen Ihnen, das Ziel zu erreichen?

(Jede korrekte Antwort stellt eine vollständige Lösung dar. Wählen Sie zwei Antworten.)

A.Ein Azure Logik-Apps-Integrationskonto
B.Ein Azure Import/Export-Auftrag
C.Azure Data Factory
D.Ein On-Premises Azure Analysis Services-Datengateway
E.Ein Azure Batch-Konto

Korrekte Antwort: B, C

Erläuterungen:

Mit dem Azure Import/Export-Dienst können Sie große Datenmengen auf sichere Weise in Azure Blob Storage und Azure Files übertragen, indem Sie Festplattenlaufwerke an ein Azure-Rechenzentrum senden. Sie können diesen Dienst auch zum Übertragen von Daten aus Azure Blob Storage auf Festplattenlaufwerke und zum Versand an lokale Standorte nutzen. Daten von einem oder mehreren Datenträgern können in Azure Blob Storage oder in Azure Files importiert werden.

Stellen Sie eigene Datenträger bereit, und übermitteln Sie Daten mit dem Azure Import/Export-Dienst. Sie können auch Laufwerke verwenden, die von Microsoft bereitgestellt werden.

Wenn Sie Daten mit den von Microsoft bereitgestellten Datenträgern übermitteln möchten, können Sie mithilfe des Azure Data Box-Datenträgers Daten in Azure importieren. Microsoft sendet über einen regionalen Transportdienstleister bis zu fünf verschlüsselte SSDs (Solid State Drives) mit einer Gesamtkapazität von 40 TB an Ihr Rechenzentrum. Sie können Datenträger schnell konfigurieren, Daten über eine USB-3.0-Verbindung auf die Datenträger kopieren und diese anschließend wieder an Azure zurücksenden.

Azure Data Factory eignet sich ebenfalls zum Übertragen von Daten aus einem lokalen Netzwerk, einem virtuellen Netzwerk in Azure oder der Cloud von Amazon zu einem Azure-Speicherkonto.

Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Was ist der Azure Import/Export-Dienst?

Verwenden des Azure Import/Export-Diensts zum Importieren von Daten in Azure Files

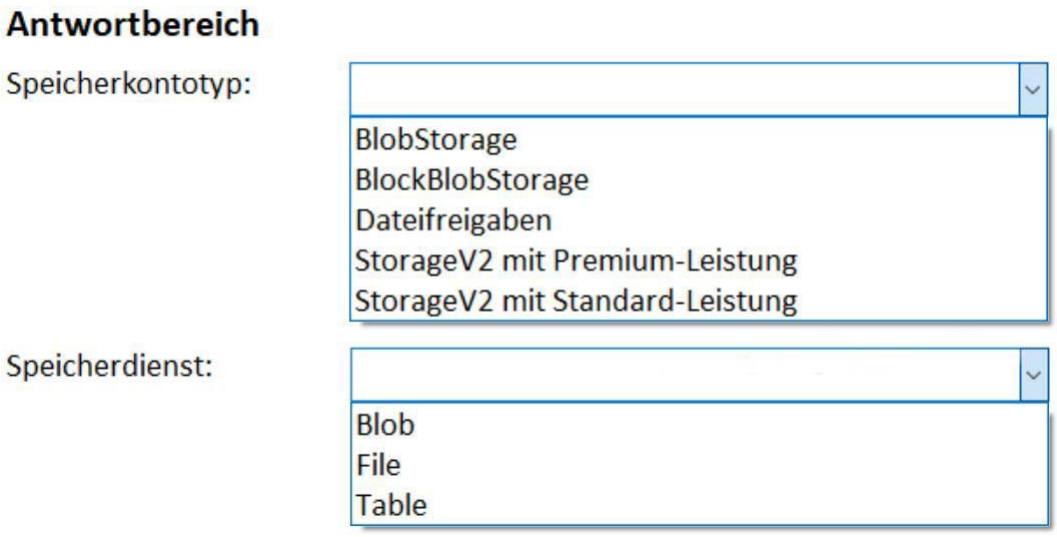
Kopieren von Daten in ein bzw. aus einem Dateisystem mithilfe von Azure Data Factory

7.Sie sind als Cloudadministrator für das Unternehmen it-pruefungen tätig. Sie müssen eine Speicherlösung für eine App entwerfen, die große Mengen häufig verwendeter Daten speichert.

Die Lösung muss folgende Anforderungen erfüllen:
Den Datendurchsatz maximieren.
Die Änderung von Daten für ein Jahr verhindern.
Die Latenz für Lese- und Schreibvorgänge minimieren.
Welchen Azure Storage-Kontotyp und welchen Speicherdienst sollten Sie verwenden?

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

Abbildung



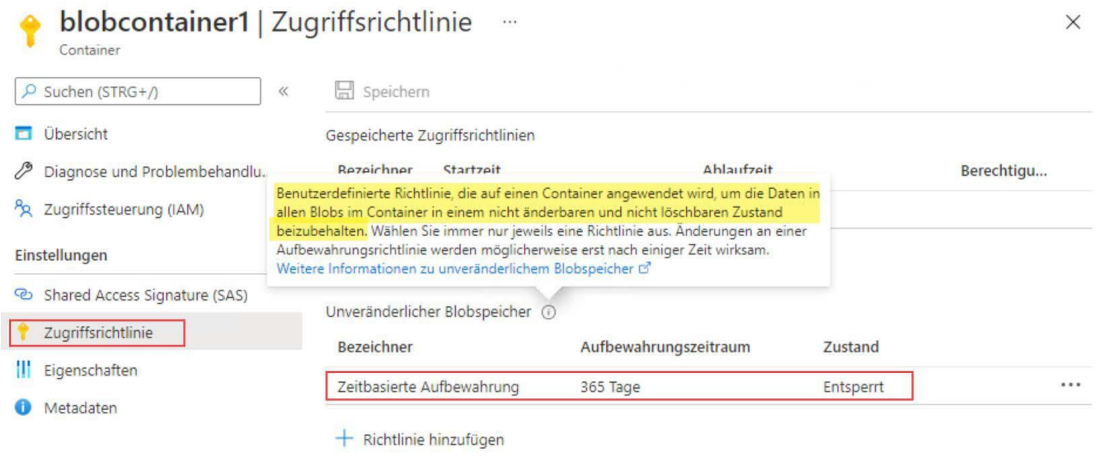
A.Speicherkontotyp: BlobStorage
Speicherdienst: Blob
B.Speicherkontotyp: BlockBlobStorage
Speicherdienst: Blob
C.Speicherkontotyp: StorageV2 mit Premium-Leistung
Speicherdienst: File
D.Speicherkontotyp: Dateifreigaben
Speicherdienst: File
E.Speicherkontotyp: StorageV2 mit Premium-Leistung
Speicherdienst: Table
F.Speicherkontotyp: StorageV2 mit Standard-Leistung

Speicherdienst: Table

Korrekte Antwort: B

Erläuterungen:

Um die Änderung der gespeicherten Daten für ein Jahr zu verhindern, müssen wir den Speicherdienst Blob verwenden. Blobcontainer unterstützen die Konfiguration einer Zugriffsrichtlinie für die zeitbasierte Aufbewahrung der im Container enthaltenen Blobs.



Um den bestmöglichen Datendurchsatz und die geringste Latenz für Lese-/Schreibvorgänge zu erhalten, müssen wir Premiumspeicher verwenden.

Premiumspeicher ist für die Kontotypen Blockblobs, Dateifregaben und Seitenblobs verfügbar.

Hinweis: StorageV2-Konten mit Premium-Leistung unterstützen nur Seitenblobs. Blockblobs, Anfügeblobs, Dateifreigaben, Tabellen und Warteschlangen sind nicht verfügbar.

Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Speichern unternehmenskritischer Blobdaten mit unveränderlichem Speicher

Speicherkontoübersicht

Blockblobspeicher mit Premium-Leistung