**Prüfungsnummer:**SC-100

**Prüfungsname:**(deutsche Version und englische Version) Microsoft Cybersecurity Architect

**Version:**demo

# Achtung: Aktuelle englische Version zu SC-100 bei uns ist gratis!!

1.Ihr Unternehmen verfügt über ein Azure Abonnement, das Azure Storage verwendet. Das Unternehmen plant, bestimmte Blobs mit Lieferanten zu teilen.

Sie müssen eine Lösung empfehlen, die den Lieferanten sicheren Zugriff auf bestimmte Blobs bietet, ohne die Blobs öffentlich zugänglich zu machen. Der Zugriff muss zeitlich begrenzt sein.

Was sollten Sie in Ihre Empfehlung einbeziehen?

A.Erstellen Sie Shared Access Signatures (SAS).
B.Geben Sie die Verbindungszeichenfolge des Zugriffsschlüssels frei.
C.Konfigurieren Sie Private Link-Verbindungen.
D.Konfigurieren Sie die Verschlüsselung mit vom Kunden verwalteten Schlüsseln (Customer Managed Keys, CMKs).

Korrekte Antwort: A

Erläuterungen:

Eine Shared Access Signature (SAS) ermöglicht den sicheren delegierten Zugriff auf Ressourcen in Ihrem Speicherkonto. Mit SAS können Sie genau steuern, wie ein Client auf Ihre Daten zugreifen kann. Zum Beispiel:

Auf welche Ressourcen der Client zugreifen kann

Welche Berechtigungen er für diese Ressourcen hat

Wie lange die SAS gültig ist

Arten von Shared Access Signatures
Azure Storage unterstützt drei Arten von Shared Access Signatures:

SAS für die Benutzerdelegierung

Dienst-SAS

Konto-SAS

SAS für die Benutzerdelegierung
Eine SAS für die Benutzerdelegierung wird durch Azure Active Directory-Anmeldeinformationen (Azure AD) sowie durch die für die SAS angegebenen Berechtigungen geschützt. Eine SAS für die Benutzerdelegierung gilt nur für Blobspeicher.

Dienst-SAS
Eine Dienst-SAS wird mit dem Speicherkontoschlüssel geschützt. Eine Dienst-SAS delegiert den Zugriff auf eine Ressource in nur einem der Azure Storage-Dienste: Blob Storage, Queue Storage, Table Storage oder Azure Files.

Konto-SAS
Eine Konto-SAS wird mit dem Speicherkontoschlüssel geschützt. Eine Konto-SAS delegiert den Zugriff auf Ressourcen in einem oder mehreren der Speicherdienste. Alle Vorgänge, die über eine Dienst-SAS oder eine SAS für die Benutzerdelegierung verfügbar sind, sind auch über eine Konto-SAS verfügbar.

Sie können auch den Zugriff auf Folgendes delegieren:

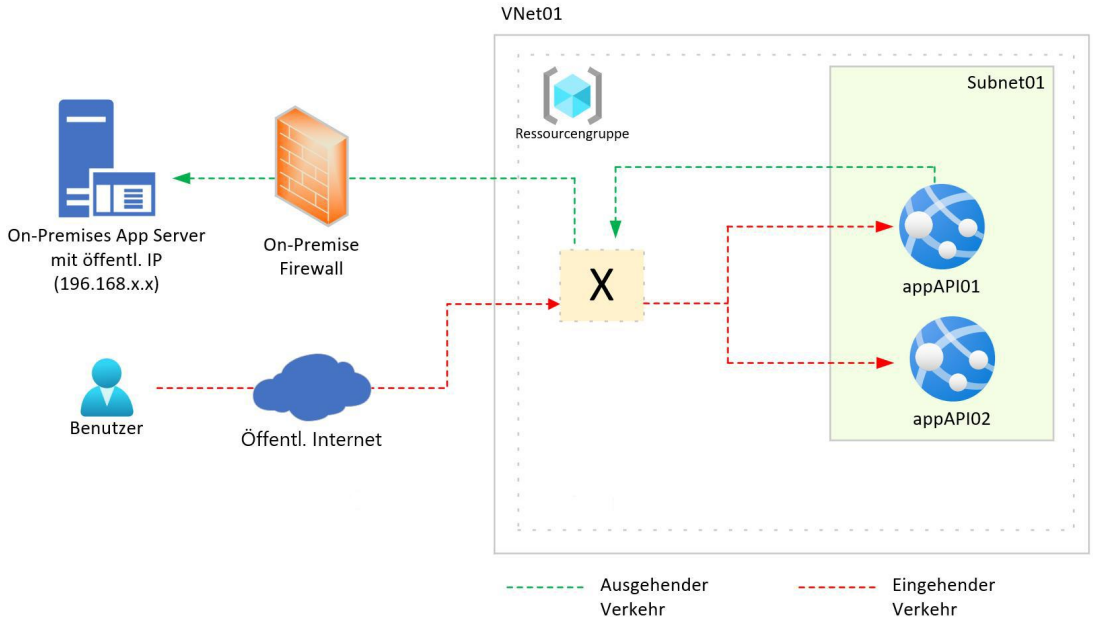
Vorgänge auf Dienstebene (z. B. Abrufen/Festlegen von Diensteigenschaften und Vorgänge zum Abrufen von Statistiken zum Dienst).

Lese-, Schreib-und Löschvorgänge, die mit einer Dienst-SAS nicht zulässig sind.

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

Grant limited access to Azure Storage resources using shared access signatures (SAS)

2.Ihr Unternehmen entwirft die nachstehend gezeigte Anwendungsarchitektur für Azure App Service Environment (ASE)-Web Apps:




Die Kommunikation zwischen dem On-Premises Netzwerk und Azure verwendet eine ExpressRoute-Verbindung.

Sie müssen eine Lösung empfehlen, die sicherstellt, dass die Web Apps mit dem On-Premises Anwendungsserver kommunizieren können. Ihre Lösung muss die Anzahl der öffentlichen IP-Adressen minimieren, die auf das On-Premises Netzwerk zugreifen dürfen.

Was sollten Sie in Ihre Empfehlung einbeziehen?

A.Azure Traffic Manager mit der Routingmethode "Priorität".
B.Azure Application Gateway v2 mit benutzerdefinierten Routen (User Defined Routes, UDRs).
C.Azure Front Door mit Azure Web Application Firewall (WAF).
D.Azure Firewall mit Richtlinienregelsätzen.

Korrekte Antwort: B

Erläuterungen:

Azure bietet verschiedene Lastenausgleichsdienste, mit denen Sie Ihre Workloads auf mehrere Computerressourcen verteilen können – Application Gateway, Front Door, Load Balancer und Traffic Manager.

Azure-Lastenausgleichsdienste können nach zwei Dimensionen kategorisiert werden: global vs. regional und HTTP(S) vs. Nicht-HTTP(S).

Global im Vergleich zu regional
Globale Lastenausgleichsdienste verteilen den Datenverkehr auf regionale Back-Ends, Clouds oder hybride lokale Dienste. Diese Dienste leiten den Endbenutzer-Datenverkehr an das nächstgelegene verfügbare Back-End weiter. Außerdem reagieren sie auf Änderungen von Zuverlässigkeit oder Leistung des Diensts, um Verfügbarkeit und Leistung zu maximieren. Sie können sich diese als Systeme vorstellen, die einen Lastenausgleich zwischen Anwendungsstempeln, Endpunkten oder Skalierungseinheiten, die in verschiedenen Regionen/geografischen Regionen gehostet werden, herstellen.

Regionale Lastenausgleichsdienste verteilen Datenverkehr in virtuellen Netzwerken auf virtuelle Computer (VMs) oder zonale und zonenredundante Dienstendpunkte innerhalb einer Region. Sie können sich diese als Systeme vorstellen, die einen Lastenausgleich zwischen virtuellen Computern, Containern oder Clustern innerhalb einer Region in einem virtuellen Netzwerk herstellen.

HTTP(S) im Vergleich zu Nicht-HTTP(S)
HTTP(S) -Lastenausgleichsdienste sind Layer-7-Lastenausgleichsmodule, die nur HTTP(S)-Datenverkehr akzeptieren. Sie sind für Webanwendungen oder andere HTTP(S)-Endpunkte vorgesehen. Sie enthalten Features wie SSL-Auslagerung, Web Application Firewall, pfadbasierten Lastenausgleich und Sitzungsaffinität.

Nicht-HTTP(S) -Lastenausgleichsdienste können Nicht-HTTP(S)-Datenverkehr verarbeiten und werden für Nicht-Web-Workloads empfohlen.

In der folgenden Tabelle werden die Azure-Lastenausgleichsdienste nach den folgenden Kategorien zusammengefasst:

| Dienst | Global/regional | Empfohlener Datenverkehr |
|---|---|---|
| Azure Front Door | Global | HTTP(S) |
| Traffic Manager | Global | Nicht-HTTP(S) |
| Application Gateway | Länderspezifisch | HTTP(S) |
| Azure Load Balancer | Länderspezifisch | Nicht-HTTP(S) |

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

Optionen für den Lastenausgleich

3.Ihr Unternehmen plant, alle On-Premises gehosteten virtuellen Computer nach Azure zu verschieben.

Ein Netzwerktechniker schlägt das in der folgenden Tabelle gezeigte Design für die virtuellen Netzwerke in Azure vor:

| Virtuelles Netzwerk | Beschreibung | Peering-Verbindung |
|---|---|---|
| Hub_VNet | Linux- and Windows-basierte VMs | VNet1, VNet2 |
| VNet1 | Windows-basierte VMs | Hub_VNet |
| VNet2 | Linux-basierte VMs | Hub_VNet |
| VNet3 | Windows-basierte VM-Skalierungsgruppen | VNet4 |
| VNet4 | Linux-basierte VM-Skalierungsgruppen | VNet3 |

Sie müssen eine Azure Bastion-Bereitstellung empfehlen, um sicheren Remotezugriff auf alle virtuellen Computer bereitzustellen.

Wie viele Azure Bastion-Subnetze sind basierend auf dem Design des virtuellen Netzwerks erforderlich?

A.1
B.2
C.3
D.4
E.5

Korrekte Antwort: B

Erläuterungen:

Azure Bastion ist ein von Ihnen bereitgestellter Dienst, mit dem Sie eine Verbindung mit einem virtuellen Computer herstellen können, indem Sie Ihren Browser und das Azure-Portal verwenden. Bei Azure Bastion handelt es sich um einen vollständig verwalteten PaaS-Dienst, den Sie in Ihrem virtuellen Netzwerk bereitstellen können. Dieser Dienst ermöglicht sichere und nahtlose RDP- und SSH-Verbindungen mit Ihren virtuellen Computern über TLS direkt im Azure-Portal. Beim Herstellen einer Verbindung über Azure Bastion benötigen Ihre VMs keine öffentliche IP-Adresse, keinen Agent und keine spezielle Clientsoftware.

Bastion bietet sichere RDP- und SSH-Verbindungen mit allen virtuellen Computern in dem virtuellen Netzwerk, in dem der Dienst bereitgestellt wird. Durch die Verwendung von

Azure Bastion wird verhindert, dass Ihre virtuellen Computer RDP- und SSH-Ports öffentlich verfügbar machen. Gleichzeitig wir weiterhin der sichere Zugriff per RDP/SSH ermöglicht.

Wir benötigen eine Azure Bastion-Bereitstellung in Hub_VNet, die es uns ermöglicht, eine Verbindung zu virtuellen Computern in Hub_VNet, in VNet1 und in VNet2 herzustellen. Zudem benötigen wird eine zweite Azure Bastion-Bereitstellung entweder in VNet3 oder VNet4, die es uns ermöglicht, eine Verbindung zu den virtuellen Computern in VNet3 und VNet4 herzustellen.

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

Was ist Azure Bastion?

4.Sie haben ein Azure Abonnement, für das Microsoft Defender for Cloud aktiviert ist.

Sie müssen ISO 27001:2013-Standards für das Abonnement durchsetzen. Ihre Lösung muss sicherstellen, dass nicht konforme Ressourcen automatisch in einen konformen Zustand versetzt werden.

Was sollten Sie verwenden?

A.Das Dashboard zur Einhaltung gesetzlicher Bestimmungen in Defender for Cloud
B.Azure Policy
C.Azure Blueprints
D.Rollenbasierte Zugriffssteuerung in Azure (Azure RBAC)

Korrekte Antwort: B

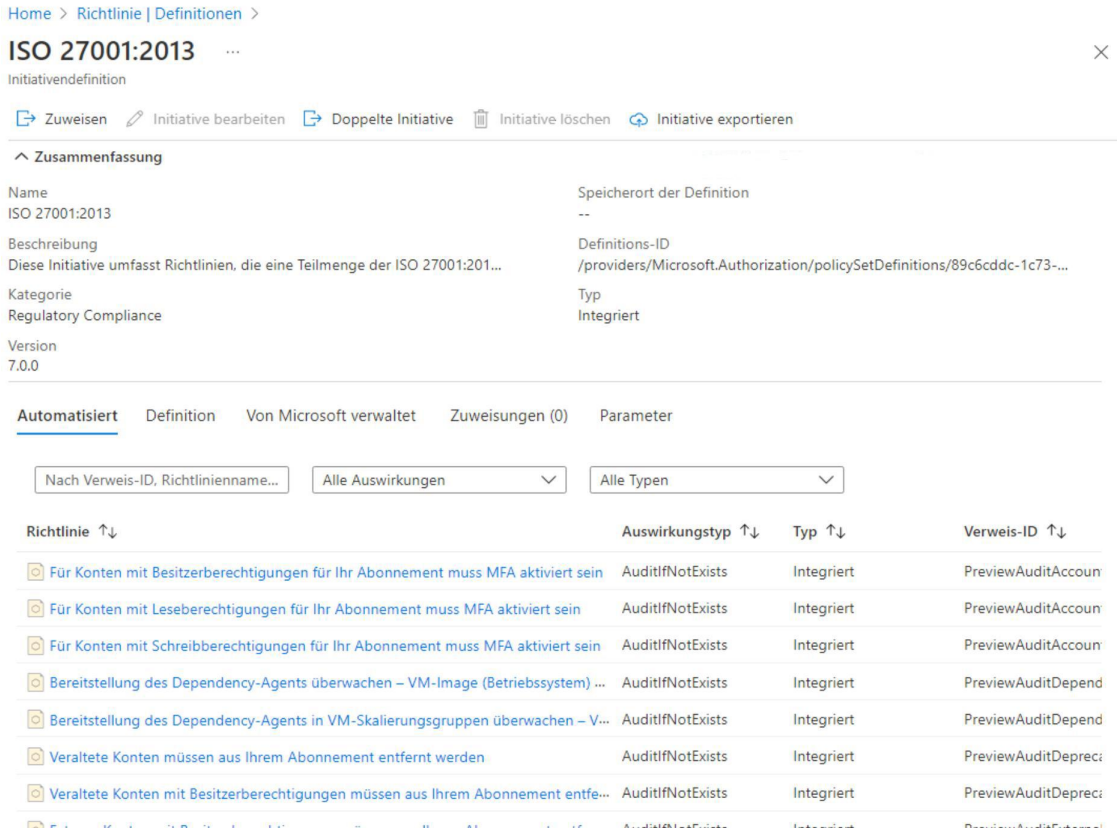
Erläuterungen:

Azure Policy hilft bei der Durchsetzung von Organisationsstandards und bei der Bewertung der Compliance nach Bedarf. Über sein Compliance-Dashboard bietet der Dienst eine aggregierte Ansicht zur Bewertung des Gesamtzustands der Umgebung mit der Möglichkeit, einen Drilldown zur Granularität pro Ressource und Richtlinie durchzuführen. Außerdem trägt er durch Massenwartung für vorhandene Ressourcen und automatische Wartung dazu bei, dass Ihre Ressourcen Compliance-Anforderungen erfüllen.

Häufige Anwendungsfälle für Azure Policy sind die Implementierung von Governance für Ressourcenkonsistenz, Einhaltung gesetzlicher Bestimmungen, Sicherheit, Kosten und

Verwaltung. Richtliniendefinitionen für diese häufigen Anwendungsfälle sind in ihrer Azure-Umgebung bereits integriert bereitgestellt, um Ihnen den Einstieg zu erleichtern.

Wir sollten die integrierte Richtlinieninitiative ISO 27001:2013 zuweisen, die aus 50 Richtlinien besteht und nicht-konforme Ressourcen durch automatische Wartungstasks in einen konformen ZUstand versetzt.




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

Was ist Azure Policy?

Korrigieren nicht konformer Ressourcen mit Azure Policy

Details zur integrierten Initiative zur Einhaltung der gesetzlichen Bestimmungen für ISO 27001:2013

5.Ihr Unternehmen verfügt über ein On-Premises Netzwerk und ein Azure Abonnement. Das Unternehmen hat kein Site-to-Site VPN und keine ExpressRoute-Verbindung zu Azure.

Sie planen die Sicherheitsstandards für Azure App Service-Web-Apps. Die Web-Apps greifen auf Microsoft SQL Server-Datenbanken im On-Premises Netzwerk zu.

Sie müssen Sicherheitsstandards empfehlen, die den Web-Apps den Zugriff auf die Datenbanken ermöglichen. Ihre Lösung muss die Anzahl offener, über das Internet zugänglicher Endpunkte für das On-Premises Netzwerk minimieren.

Was sollten Sie in Ihre Empfehlung einbeziehen?

A.Einen privaten Endpunkt
B.Hybridverbindungen
C.Virtual Network NAT Gateway-Integration
D.Integration virtueller Netzwerke (VNet-Integration)

Korrekte Antwort: B

Erläuterungen:

Hybrid Connections ist sowohl ein Dienst in Azure als auch ein Feature in Azure App Service. Als Dienst gehen seine Einsatzmöglichkeiten und Funktionen über die von Azure App Service hinaus.

In App Service kann mithilfe von Hybridverbindungen auf Anwendungsressourcen in einem beliebigen Netzwerk zugegriffen werden, das ausgehende Aufrufe an Azure über Port 443 ausführen kann. Hybridverbindungen ermöglichen den Zugriff von Ihrer App auf einen TCP-Endpunkt, sie bieten keine neue Möglichkeit, um auf Ihre App zuzugreifen. Bei der Verwendung in App Service entspricht jede Hybridverbindung einer Kombination aus einem einzelnen TCP-Host und einem Port. Dadurch können Ihre Apps auf Ressourcen unter jedem beliebigen Betriebssystem zugreifen, sofern es sich um einen TCP-Endpunkt handelt. Das Feature „Hybridverbindungen“ verfügt nicht über Informationen zum Anwendungsprotokoll oder zum abzurufenden Inhalt und benötigt diese Informationen auch nicht. Es ermöglicht lediglich den Netzwerkzugriff.

Funktionsweise
Hybridverbindungen erfordern, dass ein Relay-Agent bereitgestellt wird, über den sie sowohl den gewünschten Endpunkt als auch Azure erreichen können. Der Relay-Agent, Hybridverbindungs-Manager (HCM), ruft ausgehend über Port 443 Azure Relay auf. Von der Web-App-Site aus stellt die App Service-Infrastruktur auch eine Verbindung mit Azure Relay im Auftrag Ihrer Anwendung her. Über die verbundenen Verbindungen kann Ihre App auf den gewünschten Endpunkt zugreifen. Die Verbindung verwendet zum Schutz TLS 1.2 und zur Authentifizierung/Autorisierung SAS-Schlüssel.

Wenn Ihre App eine DNS-Anforderung stellt, die mit einem konfigurierten Hybridverbindungsendpunkt übereinstimmt, wird der ausgehende TCP-Datenverkehr über die Hybridverbindung weitergeleitet.

Vorteile der App Service-Hybridverbindungen
Die Funktion für Hybridverbindungen bietet eine Reihe von Vorteilen wie etwa Folgende:

Sie ermöglicht Apps den sicheren Zugriff auf lokale Systeme und Dienste.
Für das Feature ist kein Endpunkt erforderlich, der über das Internet zugänglich ist.
Es lässt sich schnell und einfach einrichten. Gateways sind nicht erforderlich.
Jede Hybridverbindung entspricht einer einzelnen Host-Port-Kombination, die auch einen Sicherheitsvorteil darstellt.
Firewalllücken sind normalerweise nicht erforderlich. Die Verbindungen sind alle ausgehend über Standardwebports.
Da das Feature auf Netzwerkebene ausgeführt wird, ist es nicht von der Sprache, die von Ihrer App verwendet wird, und von der Technologie, die vom Endpunkt verwendet wird, abhängig.
Sie kann verwendet werden, um über eine einzige App Zugriff in mehreren Netzwerken bereitzustellen.
Das Feature wird in einer allgemein verfügbaren Version von Windows- und Linux-Apps unterstützt. Für benutzerdefinierte Windows-Container wird es nicht unterstützt.
Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Azure App Service-Hybridverbindungen

Integrieren von Azure-Diensten mit virtuellen Netzwerken zur Netzwerkisolation

Virtual Network NAT Gateway-Integration

6.Ihr Unternehmen verfügt über eine Security Information and Event Management (SIEM)-Lösung eines Drittanbieters, die Splunk und Microsoft Sentinel verwendet.

Sie planen, Microsoft Sentinel mit Splunk zu integrieren.

Sie müssen eine Lösung empfehlen, um Sicherheitsereignisse von Microsoft Sentinel an Splunk zu senden.

Was sollten Sie in Ihre Empfehlung einbeziehen?

A.Azure Event Hub
B.Azure Data Factory
C.Eine Microsoft Sentinel-Arbeitsmappe

D.Einen Microsoft Sentinel-Datenconnector

Korrekte Antwort: A

Erläuterungen:

Wir können einen Azure Event Hub nutzen, um eine Side-by-Side-Architektur mit Microsoft Sentinel und Splunk zu implementieren. Wir können Microsoft Sentinel so konfigurieren, dass Vorfälle an Event Hub weitergeleitet werden, und Splunk so konfigurieren, dass Microsoft Sentinel-Vorfälle von Azure Event Hub konsumiert werden.

Splunk bietet ein Add-on für Microsoft Clouddienste, das es einem Splunk-Softwareadministrator ermöglicht, Aktivitätsprotokolle, Dienststatus, Betriebsmeldungen, Azure-Überwachungen, Azure-Ressourcendaten und Azure Storage-Tabellen- und Blob-Daten von einer Vielzahl von Microsoft-Clouddiensten mithilfe von Event Hubs abzurufen.

Hinweis: Microsoft Sentinel enthält keinen integrierten Datenconnector für Splunk.

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

Microsoft Sentinel Side-by-Side with Splunk via EventHub

Splunk Add-on for Microsoft Cloud Services

7.Ihr Unternehmen verfügt über ein Microsoft 365 E5-Abonnement.

Der Chief Compliance Officer plant, das Datenschutzmanagement im Arbeitsumfeld des Unternehmens zu verbessern.

Sie müssen eine Lösung empfehlen, um das Datenschutzmanagement zu verbessern.
Die Lösung muss folgende Anforderungen erfüllen:
Identifizieren ungenutzter personenbezogene Daten und den Benutzern ermöglichen, intelligente Entscheidungen im Umgang mit Daten zu treffen.
Den Benutzern Benachrichtigungen und Anleitungen zur Verfügung stellen, wenn ein Benutzer personenbezogene Daten in Microsoft Teams sendet.
Benutzern Empfehlungen zur Minimierung von Datenschutzrisiken geben.
Was sollten Sie in Ihre Empfehlung einbeziehen?

A.Microsoft Viva Insights
B.Advanced eDiscovery
C.Datenschutz-Risikomanagement in Microsoft Priva

D.Richtlinien zur Kommunikationscompliance im Insider-Risikomanagement

Korrekte Antwort: C

Erläuterungen:

Datenschutz-Risikomanagement (Privacy Risk Management) in Microsoft Priva bietet Ihnen die Möglichkeit, Richtlinien einzurichten, die Datenschutzrisiken in Ihrer Microsoft 365-Umgebung identifizieren und eine einfache Behebung ermöglichen. Richtlinien zum Datenschutzrisikomanagement sind als interne Richtlinien gedacht und können Ihnen bei Folgendem helfen:

Erkennen Sie überbelichtete persönliche Daten, damit Benutzer sie sichern können.
Erkennen und begrenzen Sie die Übertragung personenbezogener Daten über Abteilungen oder regionale Grenzen hinweg.
Helfen Sie Benutzern, die Menge ungenutzter personenbezogener Daten, die Sie speichern, zu identifizieren und zu reduzieren.
Privacy Risk Management bietet integrierte Vorlagen für diese Szenarien, um Sie bei der Erstellung von Richtlinien zu unterstützen. Sie können Ihren Ansatz auch verfeinern, indem Sie benutzerdefinierte Richtlinien erstellen und dabei eine dieser Vorlagen als Ausgangspunkt verwenden.

Wenn Richtlinienübereinstimmungen gefunden werden, können Administratoren Warnungen zu den Ergebnissen überprüfen und Entscheidungen zum Umgang mit den Daten treffen. Sie können auch E-Mail-Benachrichtigungen und für unterstützte Richtlinientypen Team-Benachrichtigungen konfigurieren, um Ihre Inhaltsbesitzer direkt über Richtlinienübereinstimmungen zu benachrichtigen. Sie können anhand dieser Benachrichtigungen Korrekturmaßnahmen ergreifen.

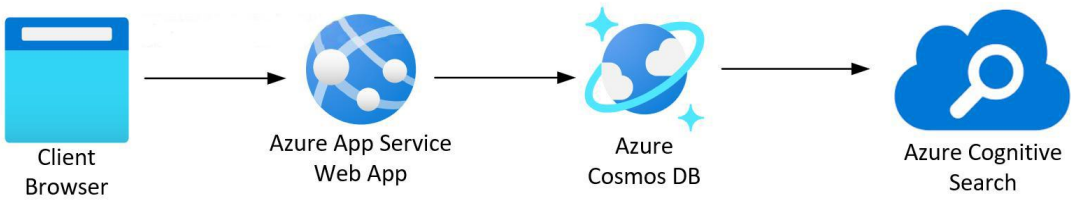
Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Weitere Informationen zu Microsoft Priva

Erfahren Sie mehr über Priva Privacy Risk Management

8.Ihr On-Premises Netzwerk enthält eine E-Commerce-Webanwendung, die in Angular und Node.js entwickelt wurde. Die Web-App verwendet eine MongoDB-Datenbank.

Sie planen, die Web-App nach Azure zu migrieren. Das Architekturteam schlägt die folgende Architektur vor:




Sie müssen eine Empfehlung für das Sichern der Verbindung zwischen der Web-App und der Datenbank geben. Ihre Lösung muss dem Zero Trust-Modell entsprechen.

Lösung: Sie empfehlen die Implementierung von Azure Application Gateway mit Azure Web Application Firewall (WAF).

Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:

Zero Trust ist ein neues Sicherheitsmodell, bei dem standardmäßig von einer Sicherheitsverletzung ausgegangen und jede Anforderung so überprüft wird, als stamme sie von einem nicht kontrollierten Netzwerk.

Um dieser neuen Welt der Datenverarbeitung gerecht zu werden, empfiehlt Microsoft dringend das Zero Trust-Sicherheitsmodell, das auf diesen Leitprinzipien basiert:

Durchführen einer expliziten Verifizierung: Ziehen Sie zur Authentifizierung und Autorisierung immer alle verfügbaren Datenpunkte heran.
Verwenden des Zugriffs mit den geringsten Rechten: Beschränken Sie den Benutzerzugriff mit Just-In-Time- und Just-Enough-Access (JIT/JEA), risikobasierten adaptiven Richtlinien und Datenschutz.
Ausgehen von einer Sicherheitsverletzung: Minimieren Sie Auswirkungsradius und Segmentzugriff. Überprüfen Sie die End-to-End-Verschlüsselung, und verwenden Sie Analysen, um für Transparenz zu sorgen, die Bedrohungserkennung voranzutreiben und die Abwehr zu verbessern.
Sowohl die Azure App Service-Web App als auch die Azure Cosmos DB werden in Azure ausgeführt. Um den Datenverkehr der Verbindungen zwischen den beiden Diensten lokal auf die virtuellen Netzwerke zu begrenzen und öffentliche Endpunkte zu vermeiden, sollten wir für beide Dienste private Endpunkte konfigurieren und die DNS-Konfiguration so ändern, dass die Verbindungszeichenfolge der Web App für die Datenbank in die IP-Adresse des privaten Endpunktes aufgelöst wird.

Ein privater Endpunkt ist eine Netzwerkschnittstelle, die eine private IP-Adresse aus Ihrem virtuellen Netzwerk verwendet. Diese Netzwerkschnittstelle bietet eine private und sichere Verbindung zwischen Ihnen und einem von Azure Private Link unterstützten Dienst. Indem Sie einen privaten Endpunkt aktivieren, binden Sie den Dienst in Ihr virtuelles Netzwerk ein.

Dieser Dienst könnte ein Azure-Dienst sein, wie z. B.:

Azure Storage
Azure Cosmos DB
Azure SQL-Datenbank
Ihr eigener Dienst, der einen Private Link-Dienst verwendet
Private Endpunkte ermöglichen die Konnektivität für Dienste in:

Virtuellen Netzwerken
Virtuellen Netzwerken mit regionalem Peering
Virtuellen Netzwerken mit globalem Peering
On-Premises Umgebungen, die VPN oder ExpressRoute verwenden
Diensten, die von Private Link unterstützt werden
Die folgenden Microsoft Docs-Artikel enthalten weitere Informationen zum Thema:

Zero Trust-Sicherheit

Was ist ein privater Endpunkt?