Prüfungsnummer:AZ-801

Prüfungsname:(deutsche Version und englische Version) Configuring Windows Server Hybrid Advanced Services

Version:demo

1.Sie haben in Microsoft Azure einen virtuellen Computer mit dem Namen VM1, auf dem Windows Server ausgeführt wird.

Sie planen, eine neue Branchenanwendung auf VM1 bereitzustellen.

Sie müssen sicherstellen, dass die Anwendung untergeordnete Prozesse erstellen kann.

Was sollten Sie auf VM1 konfigurieren?

A.Microsoft Defender Credential Guard
B.Microsoft Defender Anwendungssteuerung
C.Microsoft Defender SmartScreen
D.Exploit-Schutz

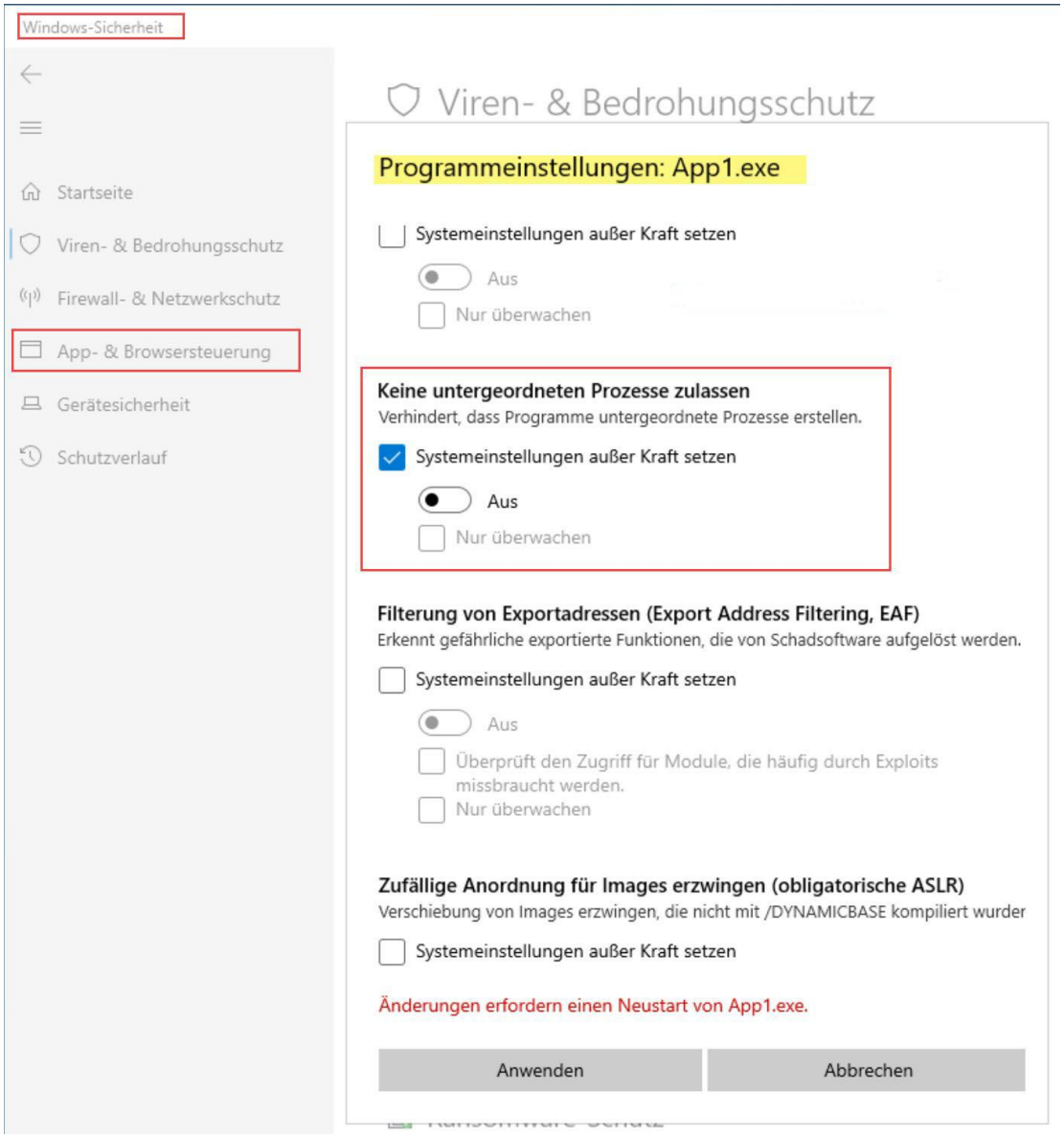
Korrekte Antwort: D

Erläuterungen:

Exploit-Schutz wendet automatisch eine Reihe von Exploit-Minderungstechniken sowohl auf die Betriebssystemprozesse als auch auf einzelne Apps an.

Sie können diese Einstellungen mithilfe der Windows-Sicherheit-App auf einem einzelnen Gerät konfigurieren. Alle Gegenmaßnahmen können für einzelne Apps konfiguriert werden. Einige Gegenmaßnahmen können auch auf Betriebssystemebene angewendet werden.

Wir müssen den Exploit-Schutz für App1 so konfigurieren, dass App1 nicht an der Erstellung von untergeordneten Prozessen gehindert wird.



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

Anpassen des Exploit-Schutzes

2.Sie haben eine On-Premises Active Directory Domänendienste (AD DS)-Domäne, die unter Verwendung der Kennworthash-synchronisierung mit einem Azure Active Directory (Azure AD)-Mandanten synchronisiert wird.

Sie haben ein Microsoft 365-Abonnement.

Alle Geräte sind hybrid mit Azure AD verbunden.

Benutzer berichten, dass sie ihr Kennwort manuell eingeben müssen, wenn sie auf Microsoft 365-Anwendungen zugreifen.

Sie müssen die Häufigkeit reduzieren, mit der Benutzer beim Zugriff auf Microsoft 365- und Azure-Dienste zur Eingabe ihres Kennworts aufgefordert werden.

Wie gehen Sie vor?

A.Konfigurieren Sie in Azure AD eine Richtlinie für bedingten Zugriff für die Microsoft Office 365-Anwendungen.
B.Erstellen Sie in der DNS-Zone der AD DS-Domäne einen Autodiscover-Eintrag.
C.Aktivieren Sie in Azure AD Connect die einmalige Anmeldung (SSO).
D.Konfigurieren Sie in Azure AD Connect die Passthrough-Authentifizierung.

Korrekte Antwort: D

Erläuterungen:

Wir können das einmalige Anmelden (Single Sign-On, SSO) in Azure AD Connect aktivieren oder die Passthrough-Authentifizierung konfigurieren, um die Notwendigkeit der Eingabe von Benutzernamen und Kennwort für die Anmeldung an Microsoft 365-Diensten zu verringern bzw. zu eliminieren.

Mit dem nahtlosen einmaligen Anmelden von Azure Active Directory (Azure AD Seamless Single Sign-On) werden Benutzer automatisch angemeldet, wenn sie an ihren mit dem Unternehmensnetzwerk verbundenen Unternehmens-Desktops arbeiten. Nahtloses SSO ermöglicht Ihren Benutzern einen einfachen Zugriff auf Ihre cloudbasierten Anwendungen, ohne dass zusätzliche lokale Komponenten erforderlich sind.

Zum Aktivieren des einmaligen Anmeldens muss das Feature in Azure AD Connect aktiviert und der URL https://autologon.microsoftazuread-sso.com manuell oder mithilfe einer Gruppenrichtlinie in AD DS zu den Intranetzoneneinstellungen der Benutzer hinzugefügt werden. Wenn die URL nicht zur Intranetzone der Internet Explorer-Einstellungen der Benutzer hinzugefügt wird, funktioniert das einmalige Anmelden nicht.

Die Passthrough-Authentifizierung verwendet einen Agenten (PTA-Agent), der auf dem Azure AD Connect-Server ausgeführt wird. Der Agent meldet Benutzer an, indem er ihre Kennwörter gegenüber dem dem On-Premises Active Directory validiert, ohne dass die Clientcomputer der Benutzer zusätzlich konfiguriert werden müssen.

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

Nahtloses einmaliges Anmelden mit Azure Active Directory: Schnellstart

Azure Active Directory-Passthrough-Authentifizierung: Schnellstart

3.Sie haben 10 Server in einer Arbeitsgruppe, auf denen Windows Server ausgeführt wird.

Sie müssen die Server so konfigurieren, dass der gesamte Netzwerkverkehr zwischen den Servern verschlüsselt wird. Die Lösung muss so sicher wie möglich sein.

Welche Authentifizierungsmethode sollten Sie in einer Verbindungssicherheitsregel konfigurieren?

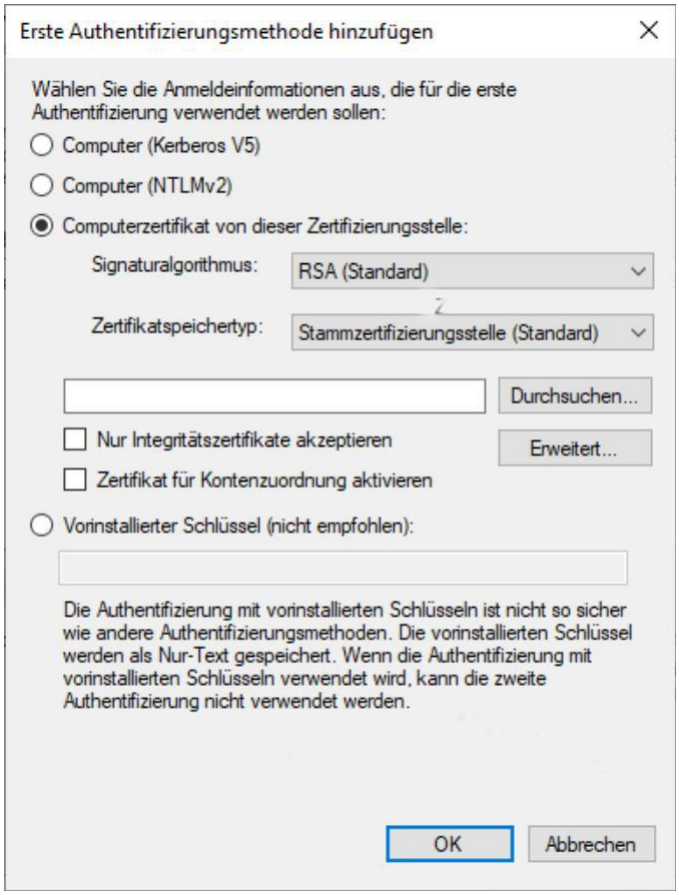
A.NTLMv2
B.Vorinstallierter Schlüssel
C.Kerberos V5
D.Computerzertifikat

Korrekte Antwort: D

Erläuterungen:

In einer Umgebung ohne Domäne können wir Computerzertifikate oder einen vorinstallierten Schlüssel als Authentifizierungsmethoden für eine Verbindungssicherheitsrichtlinie verwenden. NTLMv2 und Kerberos V5 erfordern Domänenanmeldeinformationen für die Authentifizierung.

Die Verwendung eines Computerzertifikats ist sicherer als die Verwendung eines vorinstallierten Schlüssels.

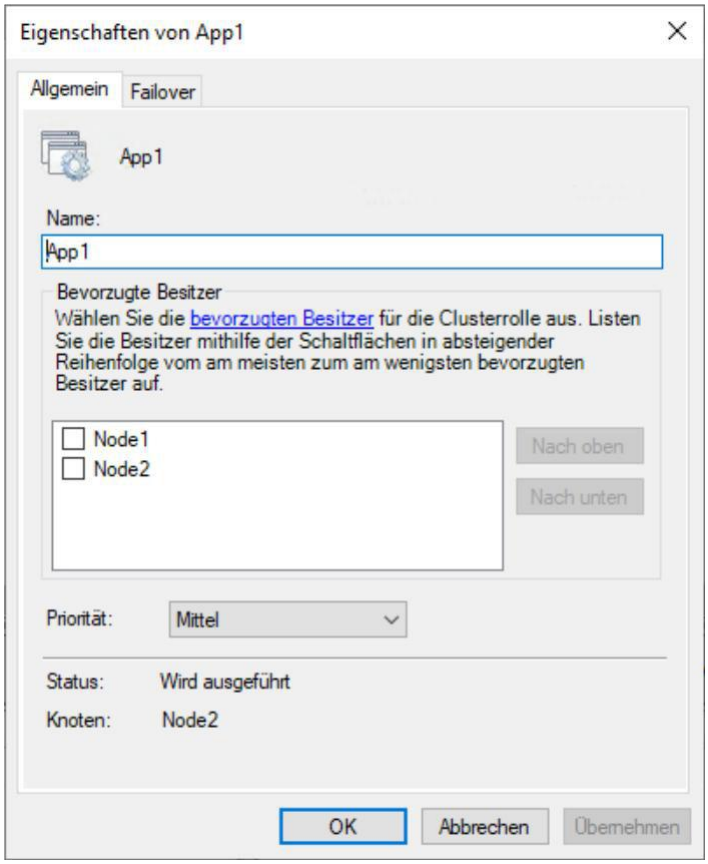


Der folgende Microsoft Docs-Artikel enthält weitere Informationen zum Thema:

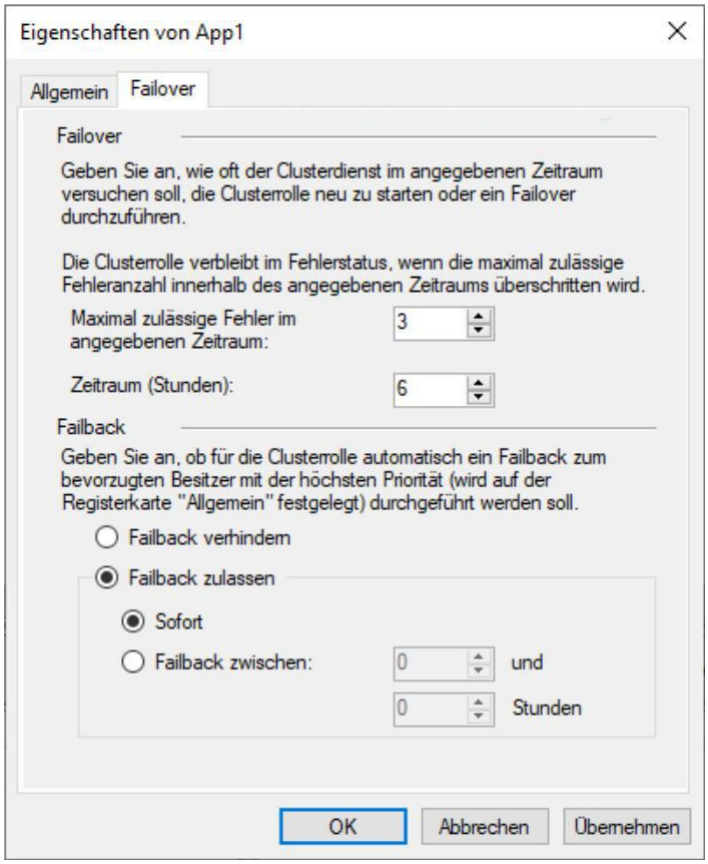
Erstellen einer Authentifizierungsanforderungsregel

4.Sie haben einen Failovercluster mit dem Namen Cluster1, der eine Anwendung mit dem Namen App1 hostet.

Die Registerkarte Allgemein der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Die Registerkarte Failover der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Node1 wird unerwartet heruntergefahren.

Sie müssen sicherstellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

Lösung: Sie aktivieren in den Failover-Einstellungen die Option "Failback verhindern".

Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:

App1 wird derzeit auf Node2 ausgeführt. Die Liste der bevorzugten Besitzer ist für App1 nicht konfiguriert, keiner der Knoten ist als bevorzugter Besitzer markiert. Wenn Node1 heruntergefahren und neu gestartet wird, wird die Rolle App1 weiterhin auf Node2 ausgeführt. Es wird kein Failback ausgelöst. Wir müssen keine Konfiguration vornehmen,

um sicherzustellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

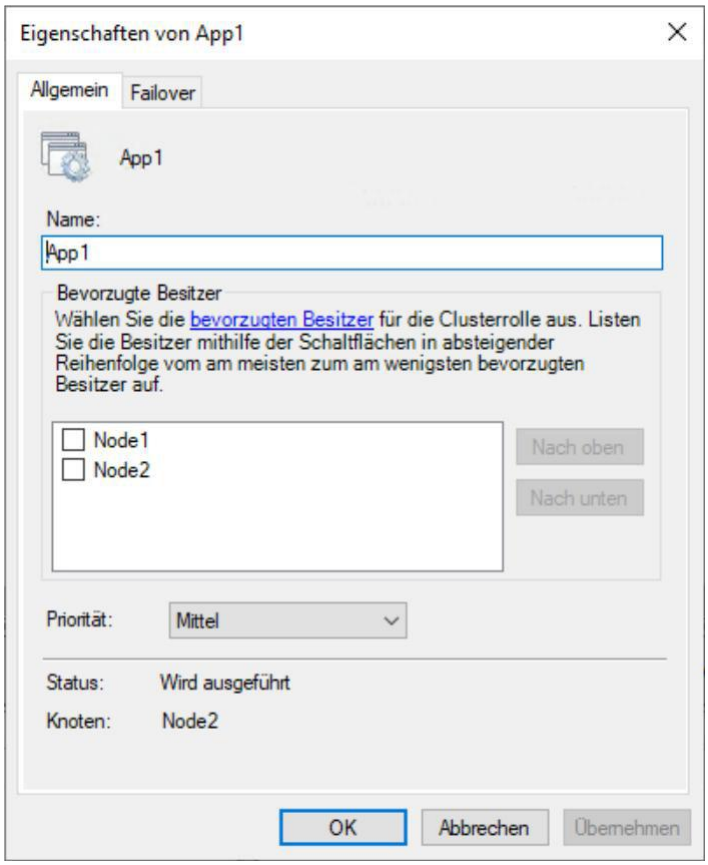
Wenn Node1 und Node2 als bevorzugte Besitzer markiert wären und Node1 neu starten würde, würde der Neustart ein Failback von App1 von Node2 auf Node1 auslösen.

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

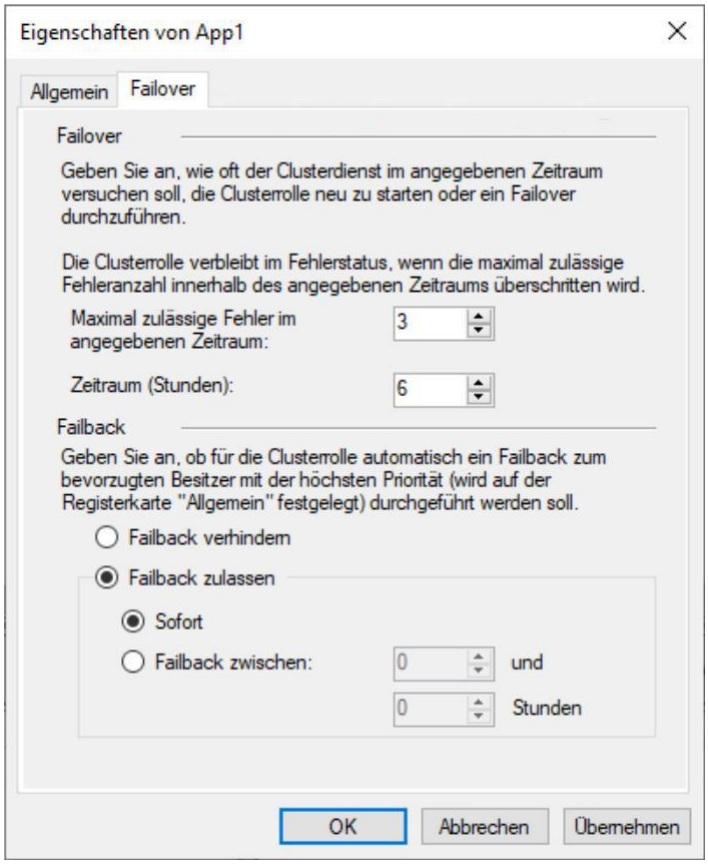
Clustered Role and Resource Properties

5.Sie haben einen Failovercluster mit dem Namen Cluster1, der eine Anwendung mit dem Namen App1 hostet.

Die Registerkarte Allgemein der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Die Registerkarte Failover der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Node1 wird unerwartet heruntergefahren.

Sie müssen sicherstellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

Lösung: Sie erhöhen den Wert der Option "Maximal zulässige Fehler im angegebenen Zeitraum" für die Clusterrolle App1.

Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:

App1 wird derzeit auf Node2 ausgeführt. Die Liste der bevorzugten Besitzer ist für App1 nicht konfiguriert, keiner der Knoten ist als bevorzugter Besitzer markiert. Wenn Node1 heruntergefahren und neu gestartet wird, wird die Rolle App1 weiterhin auf Node2 ausgeführt. Es wird kein Failback ausgelöst. Wir müssen keine Konfiguration vornehmen,

um sicherzustellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

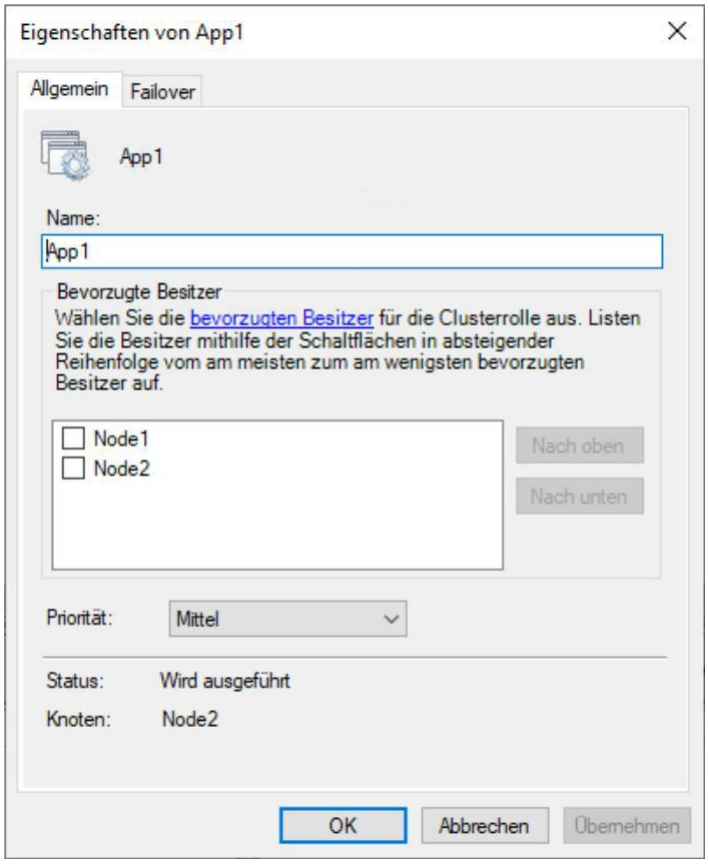
Wenn Node1 und Node2 als bevorzugte Besitzer markiert wären und Node1 neu starten würde, würde der Neustart ein Failback von App1 von Node2 auf Node1 auslösen.

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

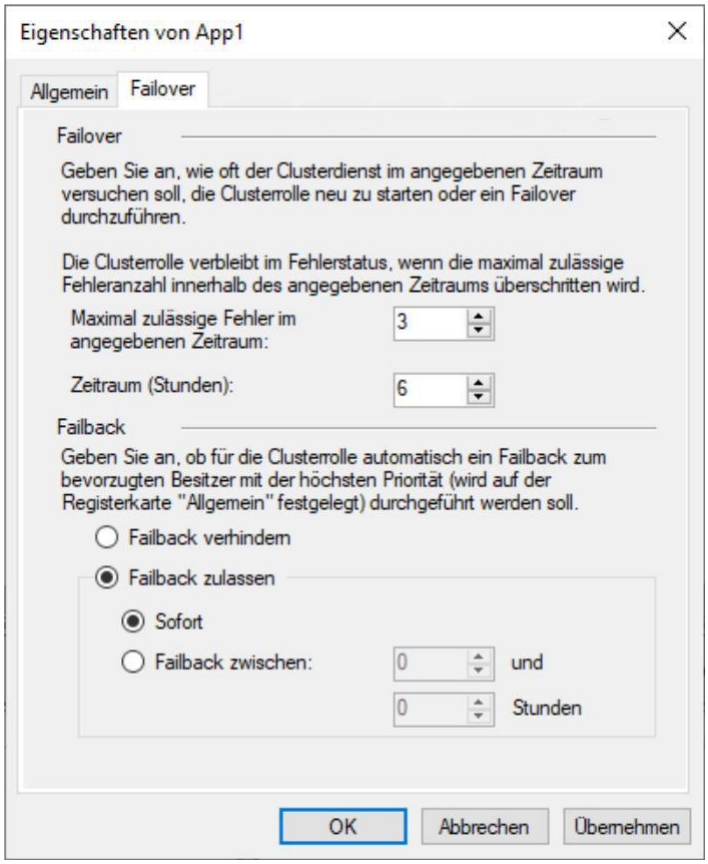
Clustered Role and Resource Properties

6.Sie haben einen Failovercluster mit dem Namen Cluster1, der eine Anwendung mit dem Namen App1 hostet.

Die Registerkarte Allgemein der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Die Registerkarte Failover der Eigenschaften von App1 ist wie in der folgenden Abbildung gezeigt konfiguriert:



Node1 wird unerwartet heruntergefahren.

Sie müssen sicherstellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

Lösung: Sie schieben Server2 in den allgemeinen Einstellungen nach oben.

Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: A

Erläuterungen:

App1 wird derzeit auf Node2 ausgeführt. Die Liste der bevorzugten Besitzer ist für App1 nicht konfiguriert, keiner der Knoten ist als bevorzugter Besitzer markiert. Wenn Node1 heruntergefahren und neu gestartet wird, wird die Rolle App1 weiterhin auf Node2 ausgeführt. Es wird kein Failback ausgelöst. Wir müssen keine Konfiguration vornehmen, um sicherzustellen, dass App1 beim Start von Node1 weiterhin auf Node2 ausgeführt wird.

Das Hochschieben von Node2 an die oberste Position erfordert das Markieren von Node2 als bevorzugter Besitzer. Erst nach erfolgter Markierung des Knotens sind die Schaltflächen "Nach oben" und "Nach unten" verfügbar.

Durch das Festlegen von Node2 als bevorzugter Besitzer, wird sichergestellt, dass App1 immer auf Node2 ausgeführt wird, sofern Node2 verfügbar ist. Wenn für App1 bei einem Neustart von Node2 ein Failover auf Node1 ausgeführt wird, wird bei dieser Konfiguration nach Abschluss des Neustarts automatisch ein Failback der App zu Node2 (auf den bveorzugten Besitzer) durchgeführt.

Die Lösung ist nicht erforderlich, um das Ziel sicherzustellen. Das Festlegen von Node2 als bevorzugter Besitzer ist jedoch grundsätzlich die richtige Vorgehensweise, um das Ziel sicherzustellen.

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

Clustered Role and Resource Properties

7.Ihr Netzwerk enthält eine Active Directory-Domänendienste (AD DS)-Domäne mit dem Namen contoso.com. Die Domäne enthält die in der folgenden Tabelle aufgeführten Container und Organisationseinheiten (OUs):

Name	Inhalt
Domain Controllers	Alle Domänencontroller der Domäne
Domain Server	Alle Mitglliedserver der Domäne, auf denen Windows Server ausgeführt wird
Domain Clientcomputer	Alle Clientcomputer, auf denen Windows 10 in der Domäne ausgeführt wird
Domain Benutzer	Alle Benutzer der Domäne

Sie erstellen die in der folgenden Tabelle gezeigten Gruppenrichtlinienobjekte (GPOs) in der Domäne:

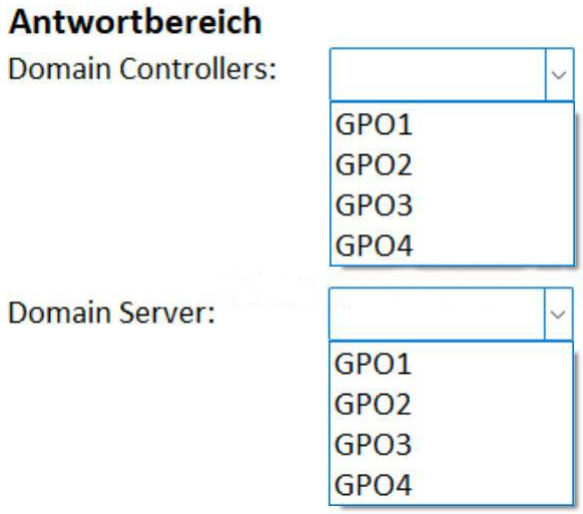
Name	Ipsec-Einstellung
GPO1	Erfordern der Authentifizierung mithilfe von Kerberos V5 für eingehende Verbindungen
GPO2	Anfordern der Authentifizierung mithilfe von Kerberos V5 für eingehende Verbindungen
GPO3	Erfordern der Authentifizierung mithilfe von X.509-Zertifikaten für eingehende Verbindungen
GPO4	Anfordern der Authentifizierung mithilfe von X.509-Zertifikaten für eingehende Verbindungen

Sie müssen die IPsec-Authentifizierung implementieren, um sicherzustellen, dass nur authentifizierte Computerkonten eine Verbindung zu den Mitgliedern der Domäne herstellen können. Ihre Lösung muss den administrativen Aufwand minimieren.

Welche GPOs sollten Sie auf die OU Domain Controllers und die OU Domain Server anwenden?

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

Abbildung



A.Domain Controllers: GPO1
Domain Server: GPO1
B.Domain Controllers: GPO1
Domain Server: GPO3
C.Domain Controllers: GPO2
Domain Server: GPO2
D.Domain Controllers: GPO3
Domain Server: GPO3
E.Domain Controllers: GPO3
Domain Server: GPO1
F.Domain Controllers: GPO4
Domain Server: GPO2

Korrekte Antwort: A