Prüfungsnummer:MS-200

Prüfungsname:(deutsche Version und englische Version)Planning and Configuring a Messaging Platform

Version:demo

Achtung: Aktuelle englische Version zu MS-200 bei uns ist gratis!!

1. Sie haben eine Microsoft Exchange Server 2019-Organisation mit einer Datenbankverfügbarkeitsgruppe (DAG). Die DAG enthält die in der folgenden Tabelle aufgeführten Server.

Name	Konfiguration
Exch1	Postfachserver
Exch2	Postfachserver
Exch3	Postfachserver
Server1	Zeugenserver

Sie installieren Windows Server 2019 auf einem neuen Server mit dem Namen Server2. Sie versuchen, Server2 der Exchange-Organisation als alternativen Zeugenserver hinzuzufügen. Der Versuch schlägt fehl und Sie erhalten die folgende Fehlermeldung: Error: An error occurred during discovery of the database availability group topology. Error: An error occurred while attempting a cluster operation. Error: Cluster API "AddClusterNode() (MaxPercentage=12) failed with 0x80070005, Error: Access is denied."
Sie müssen sicherstellen, dass Sie Server2 erfolgreich als alternativen Zeugenserver konfigurieren können.
Welchen Schritt führen Sie auf Server2 aus?

A.Erstellen Sie eine eingehende Firewall-Regel.
B.Fügen Sie der Gruppe Administratoren ein Mitglied hinzu.
C.Aktivieren Sie PowerShell-Remoting.
D.Erstellen Sie einen freigegebenen Ordner.

Korrekte Antwort: B

Erläuterungen:
Eine Datenbankverfügbarkeitsgruppe (Database Availability Group, DAG) besteht aus bis zu 16 Microsoft Exchange Server-Postfachservern, die eine automatische Wiederherstellung auf Datenbankebene nach einem Datenbank-, Server- oder Netzwerkfehler ermöglichen.

Beim Erstellen einer DAG haben Sie die Möglichkeit, einen Zeugenserver und ein Zeugenverzeichnis anzugeben. Wenn Sie einen Zeugenserver angeben, wird empfohlen, einen Exchange-Server mit Client Zugriffsdiensten zu verwenden.

Wenn es sich bei dem von Ihnen angegebenen Zeugenserver nicht um einen

Exchange-Server in Ihrer Organisation handelt, müssen Sie die universelle Sicherheitsgruppe "Exchange Trusted Subsystem" der lokalen Gruppe "Administratoren" auf dem Zeugenserver hinzufügen. Diese Sicherheitsrechte sind erforderlich, um sicherzustellen, dass mithilfe von Exchange ein Verzeichnis und eine Freigabe auf dem Zeugenserver bei Bedarf erstellt werden kann. Wenn die erforderlichen Berechtigungen nicht ordnungsgemäß konfiguriert werden, wird der folgende Fehler zurückgegeben:

Error: An error occurred during discovery of the database availability group topology. Error: An error occurred while attempting a cluster operation. Error: Cluster API "AddClusterNode() (MaxPercentage=12) failed with 0x80070005. Error: Access is denied."

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Erstellen einer Datenbankverfügbarkeitsgruppe

2. Sie haben eine Microsoft Exchange Server 2019-Organisation, die vier Postfachserver und einen Edge-Transport-Server enthält. Die Organisation unterstützt Hunderte von Remotebenutzern.
Sie müssen den Offlinezugriff auf Outlook im Web für alle Benutzer blockieren.
Wie gehen Sie?

A.Führen Sie das Cmdlet Set-OwaMailboxPolicy aus und geben Sie den Parameter -ExplicitLogonEnabled $true an.
B.Führen Sie das Cmdlet Set-OwaMailboxPolicy aus und geben Sie den Parameter -AllowOfflineOn NoComputers an.
C.Führen Sie auf dem Edge Transport-Server das Cmdlet Set-OwaVirtualDirectory aus und geben Sie den Parameter AllowOfflineOn NoComputers an.
D.Führen Sie auf jedem Postfachserver das Cmdlet Set-OwaVirtualDirectory aus und geben Sie den Parameter -ExternalURLs $null an.

Korrekte Antwort: C

Erläuterungen:
Das Cmdlet Set-OwaMailboxPolicy wird zum Konfigurieren vorhandener Outlook im Web-Postfachrichtlinien verwendet. Mit dem Cmdlet Set-OwaVirtualDirectory wird das virtuelle Webverzeichniss für Outlook im Web konfiguriert. Beide Cmdlets verfügen über den Parameter AllowOfflineOn. Da die Organisation über einen Edge-Transport-Server verfügt, sollten wir den Offlinemodus für Outlook im Web auf dem EdgeTransport-Server deaktivieren.
Der Parameter AllowOfflineOn gibt an, wann Outlook im Web im Offlinemodus für unterstützte Webbrowser verfügbar ist.

Gültige Werte sind:

PrivateComputersOnly: Der Offline-Modus ist in privaten Computersitzungen verfügbar. Standardmäßig werden in Exchange 2013 oder höher alle Outlook-Web-Sitzungen als private Computer betrachtet. In Exchange 2013 oder höher können Benutzer öffentliche Computersitzungen nur angeben, wenn Sie die private / öffentliche Auswahl auf der Anmeldeseite aktiviert haben (wenn der Parameterwert LogonPagePublicPrivateSelectionEnabled auf $true gesetzt ist).

NoComputers: Der Offline-Modus ist deaktiviert.

AllComputers: Der Offline-Modus ist für öffentliche und private Computersitzungen verfügbar. Dies ist der Standardwert.
Wenn der Offlinemodus verfügbar ist, können Benutzer den Offlinemodus in Outlook im Web selbst aktivieren oder deaktivieren.

3. Ihr Netzwerk enthält eine Active Directory-Gesamtstruktur. Die Gesamtstruktur enthält zwei Domänen mit den Namen it-pruefungen.de und exchange.it-pruefungen.de sowie eine Microsoft Exchange Server 2019-Organisation.
Die relevanten Server sind wie in der folgenden Tabelle gezeigt konfiguriert.

Name	Betriebssystem	Domäne	Plattform	Konfiguration
Server1	Windows Server 2019	exchange.it-pruefungen.de	Physikalisch	Domänencontroller
Server2	Windows Server 2019	it-pruefungen.de	Physikalisch	Mitgliedserver
Server3	Windows Server 2016	exchange.it-pruefungen.de	Physikalisch	Mitgliedserver
Server4	Windows Server 2019	exchange.it-pruefungen.de	Virtuell	Mitgliedserver
Ex1	Windows Server 2019	exchange.it-pruefungen.de	Physikalisch	Mitgliedserver
Ex2	Windows Server 2019	exchange.it-pruefungen.de	Physikalisch	Mitgliedserver

Auf EX1 und EX2 ist Exchange Server 2019 installiert. Beide Server sind Teil einer Datenbankverfügbarkeitsgruppe (DAG) mit dem Namen DAG1.
Sie müssen DAG1 einen zusätzlichen Server hinzufügen.
Welchen Server fügen Sie DAG1 hinzu?

A.Server1
B.Server2
C.Server3
D.Server4

Korrekte Antwort: D

Erläuterungen:
Für eine Datenbankverfügbarkeitsgruppe (DAG) bzw. für deren Mitglieder gelten die folgenden Anforderungen:

DNS (Domain Name System) muss ausgeführt werden. Der DNS-Server sollte im Idealfall dynamische Updates akzeptieren. Wenn der DNS-Server keine dynamischen Updates akzeptiert, müssen Sie einen DNS-Hosteintrag (A-Eintrag) für jeden Exchange-Server erstellen. Andernfalls funktioniert Exchange nicht ordnungsgemäß.

Jeder Postfachserver in einer DAG muss ein Mitgliedsserver in derselben Domäne sein.

Das Hinzufügen eines Exchange-Postfachservers, der auch ein Verzeichnisserver einer DAG ist, wird nicht unterstützt.

Der von Ihnen der DAG zugeordnete Name muss ein gültiger, verfügbarer und eindeutiger Computername mit maximal 15 Zeichen sein.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Planen der hohen Verfügbarkeit und Ausfallsicherheit von Standorten

4. Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Ihr Netzwerk enthält zwei Active Directory-Standorte mit den Namen Site1 und Site2.
Sie stellen eine neue Microsoft Exchange Server 2019-Organisation bereit, die an jedem Standort einen Postfachserver enthält.
Sie müssen die Organisation so konfigurieren, dass für den Exchange-AutoErmittlungsdienst (Autodiscover) ein einzelner Namespace verwendet wird.
Wie gehen Sie vor?

A.Erstellen Sie in DNS einen SRV-Eintrag mit dem Namen AutoDiscover.
B.Erstellen Sie in DNS einen TXT-Eintrag mit dem Namen AutoDiscover.
C.Führen Sie das Cmdlet Set-ClientAccessService aus.
D.Führen Sie das Cmdlet Set-AutodiscoverVirtualDirectory aus.

Korrekte Antwort: D

Erläuterungen:
Der AutoErmittlungsdienst stellt Clients Zugriff auf Exchange-Funktionen bereit und reduziert so die zur Benutzerkonfiguration und Bereitstellung erforderlichen Schritte auf ein Minimum. Im Falle von Exchange-Webdienste (EWS)-Clients wird der AutoErmittlungsdienst in der Regel zur Ermittlung der EWS-Endpunkt-URL verwendet. Die AutoErmittlung kann jedoch auch Informationen zum Konfigurieren von Clients liefern, die andere Protokolle verwenden. Die AutoErmittlung unterstützt Clientanwendungen innerhalb und außerhalb von Firewalls sowie Clientanwendungen in Ressourcengesamtstrukturen und Umgebungen mit mehreren Gesamtstrukturen.

Externe Clients ermitteln den AutoErmittlungsdienst über den CNAME-Eintrag autodiscover.domain.tld. Interne Clients ermitteln den AutoErmittlungsdienst über einen in Active Directory konfigurierten Dienstverbindungspunkt (Service Connection Point, SCP).

Der externe URL und der interne URL können mithilfe des Cmdlets Set-AutodiscoverVirtualDirectory festgelegt werden.
Die folgenden Technet-Artikel enthalten weitere Informationen zum Thema:
AutoErmittlungsdienst in Exchange Server
Set-AutodiscoverVirtualDirectory

5. Sie sind als Administrator für das Unternehmen it-pruefungen.de tätig. Das Unternehmen hat ein Microsoft Exchange Online-Abonnement.
Sie haben mehrere Transportregeln erstellt. Die Regeln wenden automatisch einen Haftungsausschluss auf E-Mail-Nachrichten an, die bestimmte Schlüsselwörter im Betreff enthalten und an Empfänger mit der E-Mail-Domäne faberg.de gesendet werden.
Sie erhalten einen Bericht, der besagt, dass einige Nachrichten ohne den Haftungsausschluss zugestellt wurden.
Sie müssen ermitteln, welche Transportregeln auf Nachrichten angewendet wurden, die an die Empfänger von faberg.de gesendet wurden.
Was verwenden Sie?

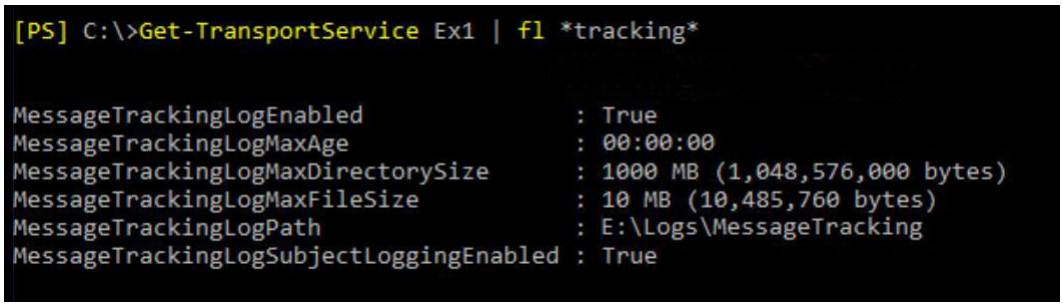
A.Eine URL-Ablaufverfolgung
B.Eine Nachrichtenablaufverfolgung
C.Die Protokolle des SMTP-Dienstes
D.Die Transportprotokolle

Korrekte Antwort: B

Erläuterungen:
Als Administrator können Sie herausfinden, was mit einer E-Mail passiert ist, indem Sie eine Nachrichtenablaufverfolgung im Exchange-Verwaltungskonsole (EAC) ausführen. Nach der Ausführung der Nachrichtenablaufverfolgung können Sie alle Ergebnisse in einer Liste anzeigen und Details zu den einzelnen Nachrichten sehen. Daten der Nachrichtenablaufverfolgung sind für die letzten 90 Tage verfügbar. Wenn eine Nachricht älter als 7 Tage ist, können Sie die Ergebnisse nur in einer herunterladbaren Ansicht anzeigen. CSV-Datei.

Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Ausführen einer Nachrichtenablaufverfolgung und Anzeigen der Ergebnisse im Exchange Admin Center
Suchen und Beheben von Problemen mit der E-Mail-Zustellung als Office 365 Business-Administrator

6. Sie haben einen Microsoft Exchange Server 2019-Postfachserver mit dem Namen EX1. Sie führen den in der folgenden Abbildung gezeigten Befehl aus:



Was bewirkt die Konfiguration?

A.Die Protokolldateien der Nachrichtenverfolgung werden 30 Tage lang aufbewahrt und anschließend gelöscht.
B.Die Protokolldateien der Nachrichtenverfolgung werden sofort gelöscht.
C.Die Protokolldateien der Nachrichtenverfolgung werden aufbewahrt, bis die Verzeichnisgrößenbeschränkung überschritten wird.
D.Die Protokolldateien der Nachrichtenverfolgung werden 365 Tage lang aufbewahrt und anschließend gelöscht.

Korrekte Antwort: C

Erläuterungen:
Das Nachrichtenverfolgungsprotokoll zeichnet die Nachrichtenaktivitäten während der Übertragung von Nachrichten über die Transportpipeline auf Postfachservern und Edge-Transport-Servern auf. Sie können Nachrichtenverfolgungsprotokolle für forensische Nachrichtenanalysen, Nachrichtenübermittlungsanalysen, die Berichterstellung und die Problembehandlung verwenden.

Verwenden Sie das Set-TransportService-Cmdlet in der Exchange-Verwaltungsshell auf Postfachserver und Edge-Transport-Servern für alle Konfigurationsaufgaben der Nachrichtenverfolgung. Beispiel:

Aktiveren und Deaktivieren der Nachrichtenverfolgung. Standardmäßig ist diese aktiviert.

Angeben des Speicherorts der Nachrichtenverfolgungs-Protokolldateien. Der Standardspeicherort ist %ExchangeInstallPath%TransportRoles\Logs\MessageTracking.

Angeben einer Maximalgröße für die einzelnen Nachrichtenverfolgungs-Protokolldateien. Der Standardwert beträgt 10 MB.

Angeben einer Maximalgröße für das Verzeichnis, das die Protokolldateien der Nachrichtenverfolgung enthält. Der Standardwert beträgt 1.000 MB.

Angeben des Höchstalters für die Protokolldateien der Nachrichtenverfolgung: Der Standardwert beträgt 30 Tage.

Aktivieren und Deaktivieren der Nachrichtenbetreffprotokollierung in den Nachrichtenverfolgungsprotokollen. Standardmäßig ist diese aktiviert.

Durch Festlegen des MessageTrackingLogMaxAge-Parameters auf den Wert 00:00:00 wird verhindert, dass Protokolldateien der Nachrichtenverfolgung aufgrund ihres Alters automatisch entfernt werden.Der folgende Technet-Artikel enthält weitere Informationen zum Thema:
Konfigurieren der Nachrichtenverfolgung