Prüfungsnummer:70-744

Prüfungsname: Securing Windows Server 2016

Version:demo

1. Ihr Netzwerk umfasst eine Active Directory-Domänendienste (AD DS) Domäne mit dem Namen it-pruefungen.de. Die Domäne enthält 100 Server. Sie stellen das Tool Local Administrator Password Solution (LAPS) im Netzwerk bereit.
Sie installieren einen neuen Server mit dem Namen Server5. Anschließend nehmen Sie Server5 in die Domäne auf.
Sie müssen sicherstellen, dass die Kennwörter der lokalen Administratoren von Server5 in der LAPS-Verwaltungskonsole verfügbar sind.
Wie gehen Sie vor?

A.Registrieren Sie AdmPwd.dll auf Server5.
B.Installieren Sie das Windows PowerShell Modul für LAPS auf Server5.
C.Ändern Sie die Sicherheitseinstellungen für das Computerkonto von Server5 in der Domäne.
D.Ändern Sie die Sicherheitseinstellungen für die Organisationseinheit (OU) Domain Controllers in der Domäne.

Korrekte Antwort: A

Erläuterungen:
Das Tool Local Administrator Password Solution (LAPS) ermöglicht die zentrale Verwaltung der lokalen Administratorkennwörter von Domänencomputern.
Es handelt sich um eine Lösung, bei der pro Client ein dynamisches Passwort generiert und im Active Directory hinterlegt wird. Die Lösung basiert auf den folgenden Komponenten:

- GPO Clienterweiterungen auf jedem Client, der mittels LAPS verwaltet werden soll.
- Verwaltungstools
- Grafische Benutzerschnittstelle zum Auslesen der Passwörter aus dem AD.
- PowerShell Modul zur Administration per PowerShell.
- Gruppenrichtlinienvorlagen zur Konfiguration der Clients.
- Zwei neue Attribute im Active-Directory-Schema.

Die Clienterweiteurngen können per MSI-Datei installiert werden. Alternativ kann die relevante Bibliotheksdatei (DLL) mithilfe von regsvr32 auch manuell registriert werden.
Der folgende Artikel enthält weitere Informationen zum Thema:
LAPS – lokales Admin-Passwort endlich sicher

2. Ihr Netzwerk umfasst eine Active Directory-Domänendienste (AD DS) Domäne mit dem Namen it-pruefungen.de. Sie stellen Microsoft Advanced Threat Analytics (ATA) in der

Domäne bereit.
Sie installieren das ATA-Dashboard auf einem Server mit dem Namen Server1 und das ATA-Gateway auf einem Server mit dem Namen Server2.
Sie müssen sicherstellen, dass Server2 NTLM-Authentifizierungsereignisse sammeln kann.
Was konfigurieren Sie?

A.Konfigurieren Sie die Domänencontroller für das Weiterleiten von Ereignissen mit der ID 4776 an Server2.
B.Konfigurieren Sie die Domänencontroller für das Weiterleiten von Ereignissen mit der ID 1000 an Server1.
C.Konfigurieren Sie Server2 für das Weiterleiten von Ereignissen mit der ID 1026 an Server1.
D.Konfigurieren Sie Server1 für das Weiterleiten von Ereignissen mit der ID 1000 an Server1.

Korrekte Antwort: A

Erläuterungen:
Advanced Threat Analytics (ATA) ist eine lokale Plattform, mit deren Hilfe Sie Ihr Unternehmen vor verschiedenen hochentwickelten und gezielten Cyberangriffen und Insiderbedrohungen schützen können.
ATA bezieht aus mehreren Datenquellen wie Protokollen und Ereignissen in Ihrem Netzwerk Informationen, um das Verhalten von Benutzern und anderen Personen in der Organisation zu lernen und anschließend ein Verhaltensprofil zu erstellen. ATA kann Ereignisse und Protokolle aus folgenden Quellen beziehen:

- SIEM-Integration
- Windows-Ereignisweiterleitung (Windows Event Forwarding; WEF)

Darüber hinaus nutzt ATA ein proprietäres Netzwerkanalysemodul, um den Netzwerkverkehr verschiedener Protokolle (z.B. Kerberos, DNS, RPC, NTLM und andere) zwecks Authentifizierung, Autorisierung und zum Sammeln von Informationen zu erfassen und zu analysieren. ATA sammelt die Informationen über:

- die Portspiegelung von Domänencontrollern und DNS-Servern bis zum ATA-Gateway.
- die direkt Bereitstellung eines ATA-Lightweight-Gateways (LGW) auf Domänencontrollern.

Um die Erkennungsfunktionalität zu verbessern, benötigt ATA die Windows-Ereignisprotokoll-ID 4776.
Konkrete Informationen zum Konfigurieren der Ereignissammlung finden Sie in dem folgenden Artikel:
Konfigurieren der Ereignissammlung

3. Hinweis: Diese Aufgabe gehört zu einer Reihe von Fragestellungen, die dasselbe

Szenario verwenden. Jede Aufgabe dieser Reihe bietet einen anderen Lösungsweg. Sie müssen entscheiden, ob die Lösung geeignet ist, das Ziel zu erreichen.
Ihr Netzwerk umfasst eine Active Directory-Gesamtstruktur mit dem Namen it-pruefungen.de. Auf allen Servern ist das Betriebssystem Windows Server 2016 installiert.
Die Gesamtstruktur enthält 2000 Clientcomputer, auf denen Windows 10 ausgeführt wird. Alle Clientcomputer werden mit einem angepassten Windows-Abbild installiert.
Sie müssen 10 Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) bereitstellen. Ihre Lösung muss sicherstellen, dass Administratoren Zugriff auf mehrere Anwendungen haben, die von allen Benutzern verwendet werden.
Lösung: Sie stellen 10 physikalische Computer als Virtualisierungshosts bereit. Sie stellen das Betriebssystem auf jedem Host mithilfe des angepassten Windows-Abbilds bereit. Anschließend erstellen Sie auf jedem Host eine virtuelle Gastmaschine für die Nutzung als Arbeitsstation mit privilegiertem Zugriff (PAW).
Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:
Das Konzept der Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) unterscheidet zwischen Arbeitsstationen, die für administrative bzw. senstivite Aufgaben verwendet werden und Arbeitsstationen für die alltägliche Nutzung. Das Konzept unterschiedet zwei PAW-Hardwareprofile.

Verwendung separater Hardwaregeräte für alltägliche Aufgaben und administrative Aufgaben.

Gemeinsame Verwendung eines Gerätes für alltägliche Aufgaben und administrative Aufgaben. Die Trennung erfolgt durch die Nutzung zweier Betriebssysteme. Das Betriebssystem für alltägliche Aufgaben kann als virtueller Computer auf der PAW-Arbeitsstaion betrieben werden. Das Betreiben einer PAW-Arbeitsstaion als virtueller Computer auf einem physischen Computer für die alltägliche Verwendung entspricht nicht den Anforderungen.
Siehe auch: Privileged Access Workstations

4. Hinweis: Diese Aufgabe gehört zu einer Reihe von Fragestellungen, die dasselbe Szenario verwenden. Jede Aufgabe dieser Reihe bietet einen anderen Lösungsweg. Sie müssen entscheiden, ob die Lösung geeignet ist, das Ziel zu erreichen.
Ihr Netzwerk umfasst eine Active Directory-Gesamtstruktur mit dem Namen it-pruefungen.de. Auf allen Servern ist das Betriebssystem Windows Server 2016 installiert.
Die Gesamtstruktur enthält 2000 Clientcomputer, auf denen Windows 10 ausgeführt wird.

Alle Clientcomputer werden mit einem angepassten Windows-Abbild installiert.
Sie müssen 10 Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) bereitstellen. Ihre Lösung muss sicherstellen, dass Administratoren Zugriff auf mehrere Anwendungen haben, die von allen Benutzern verwendet werden.
Lösung: Sie stellen einen physikalischen Computer mit dem Betriebssystem Windows Server 2016 als Virtualisierungshosts bereit. Sie erstellen 10 virtuelle Maschinen (VMs) und konfigurieren jede VM als Arbeitsstation mit privilegiertem Zugriff (PAW).
Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:
Auf einer Arbeitsstation mit privilegiertem Zugriff können keine Anwendungen für alltägliche Aufgaben verwendet werden. Es ist ein zusätzlicher virtueller oder physikalischer Computer erforderlich.
Das Konzept der Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) unterschiedet zwischen Arbeitsstationen, die für administrative bzw. senstivite Aufgaben verwendet werden und Arbeitsstationen für die alltägliche Nutzung. Das Konzept unterscheidet zwei PAW-Hardwareprofile.

Verwendung separater Hardwaregeräte für alltägliche Aufgaben und administrative Aufgaben.

Gemeinsame Verwendung eines Gerätes für alltägliche Aufgaben und administrative Aufgaben. Die Trennung erfolgt durch die Nutzung zweier Betriebssysteme. Das Betriebssystem für alltägliche Aufgaben kann als virtueller Computer auf der PAW-Arbeitsstaion betrieben werden. Das Betreiben einer PAW-Arbeitsstaion als virtueller Computer auf einem physischen Computer für die alltägliche Verwendung entspricht nicht den Anforderungen.
Siehe auch: Privileged Access Workstations

5. Hinweis: Diese Aufgabe gehört zu einer Reihe von Fragestellungen, die dasselbe Szenario verwenden. Jede Aufgabe dieser Reihe bietet einen anderen Lösungsweg. Sie müssen entscheiden, ob die Lösung geeignet ist, das Ziel zu erreichen.
Ihr Netzwerk umfasst eine Active Directory-Gesamtstruktur mit dem Namen it-pruefungen.de. Auf allen Servern ist das Betriebssystem Windows Server 2016 installiert.
Die Gesamtstruktur enthält 2000 Clientcomputer, auf denen Windows 10 ausgeführt wird.
Alle Clientcomputer werden mit einem angepassten Windows-Abbild installiert.
Sie müssen 10 Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) bereitstellen. Ihre Lösung muss sicherstellen, dass Administratoren Zugriff auf mehrere Anwendungen haben, die von allen Benutzern verwendet werden.

Lösung: Sie stellen 10 physikalische Computer bereit und konfigurieren sie als Arbeitsstation mit privilegiertem Zugriff (PAW). Sie stellen 10 zusätzliche Computer bereit und installieren sie mit dem angepassten Windows-Abbild.
Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: A

Erläuterungen:
Das Konzept der Arbeitsstationen mit privilegiertem Zugriff (Privileged Access Workstations, PAWs) unterscheidet zwischen Arbeitsstationen, die für administrative bzw. senstivite Aufgaben verwendet werden und Arbeitsstationen für die alltägliche Nutzung. Das Konzept unterschiedet zwei PAW-Hardwareprofile.

Verwendung separater Hardwaregeräte für alltägliche Aufgaben und administrative Aufgaben.

Gemeinsame Verwendung eines Gerätes für alltägliche Aufgaben und administrative Aufgaben. Die Trennung erfolgt durch die Nutzung zweier Betriebssysteme. Das Betriebssystem für alltägliche Aufgaben kann als virtueller Computer auf der PAW-Arbeitsstaion betrieben werden. Das Betreiben einer PAW-Arbeitsstaion als virtueller Computer auf einem physischen Computer für die alltägliche Verwendung entspricht nicht den Anforderungen.
Siehe auch: Privileged Access Workstations

6. Hinweis: Diese Aufgabe gehört zu einer Reihe von Fragestellungen, die dasselbe Szenario verwenden. Jede Aufgabe dieser Reihe bietet einen anderen Lösungsweg. Sie müssen entscheiden, ob die Lösung geeignet ist, das Ziel zu erreichen.
Ihr Netzwerk umfasst eine Active Directory-Domänendienste (AD DS) Domäne mit dem Namen it-pruefungen.de. Die Domäne enthält einen Computer, auf dem das Betriebssystem Windows 10 ausgeführt wird. Computer1 ist mit einem Heimnetzwerk und dem Unternehmensnetzwerk verbunden.
Das Unternehmensnetzwerk nutzt intern den Adressbereich 172.16.0.0/24.
Auf Computer1 wird eine Anwendung mit dem Namen App1 ausgeführt. App1 erwartet Verbindungen auf Port 8080.
Sie müssen verhindern, dass Verbindungen mit App1 hergestellt werden, wenn Computer1 mit dem Heimnetzwerk verbunden ist.
Lösung: Sie verwenden die Gruppenrichtlinienverwaltung und erstellen Richtlinien für Softwareeinschränkung.
Erfüllt das Vorgehen Ihr Ziel?

A.Ja
B.Nein

Korrekte Antwort: B

Erläuterungen:
Mithilfe der Richtlinien für Softwareeinschränkung können wir eine Hashregel erstellen, die das Ausführen von App1 verhindert. Die Forderung wäre damit erfüllt. App1 könnte bei dieser Konfiguration jedoch auch dann nicht ausgeführt werden, wenn der Computer nicht mit dem Heimnetzwerk, sondern mit dem Unternehmensnetzwerk verbunden ist. Ob dies akzeptabel ist, lässt sich der Aufgabe nicht zweifelsfrei entnehmen.
Da sich die Forderung explizit auf Verbindungen mit dem Heimnetzwerk bezieht, gehe ich davon aus, dass diese Lösung über das Ziel hinausschießt.