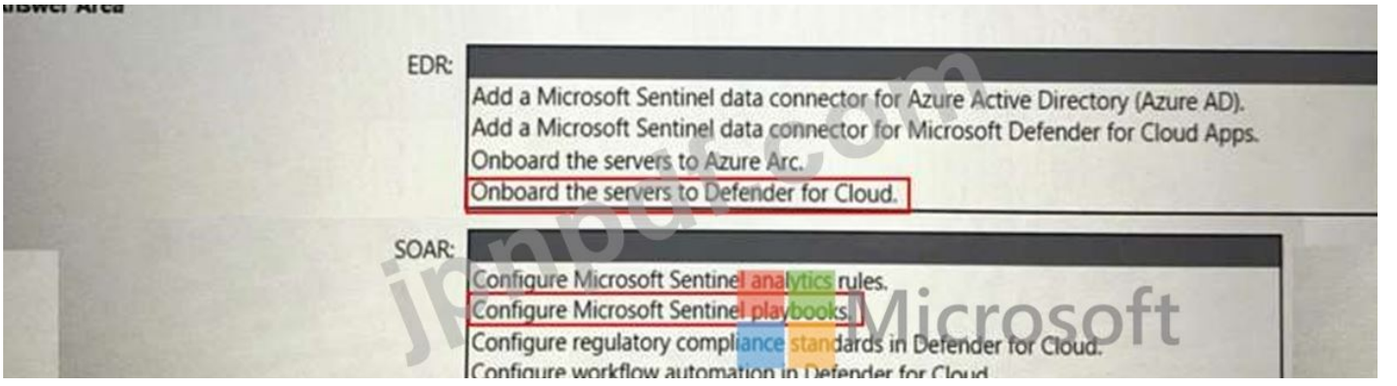
Microsoft.SC-100.v2023-12-30.q119

試験コード:	SC-100
試験名称:	Microsoft Cybersecurity Architect
認定資格:	Microsoft
無料問題数:	119
バージョン:	v2023-12-30
アクセス数:	877
ページビュー数:	1190
https://www.jpnpdf.com/Microsoft.SC-100.v2023-12-30.q119-mondaishu.html	

最新問題: **1**
あなたの会社には、Microsoft Defender for Cloud のセキュリティが強化された Azure サブスクリプションがあります。
同社は米国政府と契約を締結しました。NIST 800-53 に準拠するために現在のサブスクリプションを確認する必要があります。まず何をすべきでしょうか?
A. Defender for Cloud から、監査レポートの Azure セキュリティ ベースラインを確認します。
B. Defender for Cloud から、セキュリティ スコアの推奨事項を確認します。
C. Defender for Cloud から、規制遵守標準を追加します。
D. Defender for Cloud から、Defender for Cloud プランを有効にします。
Answer: (解答を表示する**)**

最新問題: **2**
Microsoft 365 サブスクリプションと Azure サブスクリプションをお持ちです。Microsoft 365 Defender と Microsoft Defender for Cloud が有効になっています。
Azure サブスクリプションには Microsoft Sentinel ワークスペースが含まれています。Microsoft Sentinel データ コネクタは、Microsoft 365、Microsoft 365 Defender、Defender for Cloud、および Azure 用に構成されています。
Windows Server を実行する Azure 仮想マシンをデプロイする予定です。
Microsoft Sentinel の拡張検出と応答 (EDR) およびセキュリティ オーケストレーション、自動化、および応答 (SOAR) 機能を有効にする必要があります。
各機能を有効にすることをどのように推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題**: 3**

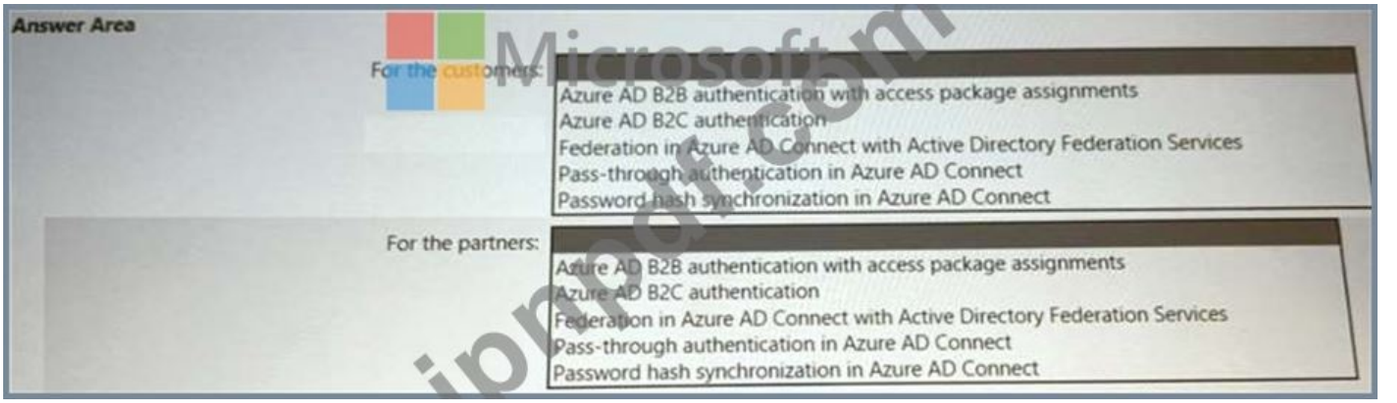
あなたの会社には Microsoft 365 E5 サブスクリプション、Azure サブスクリプション、オンプレミス アプリケーション、および Active Directory ドメイン サービス (AD DSV) があります。次の要件を満たす ID セキュリティ戦略を推奨する必要があります。

* 顧客が Facebook 資格情報を使用して Azure App Service Web サイトへの認証を行えることを保証します

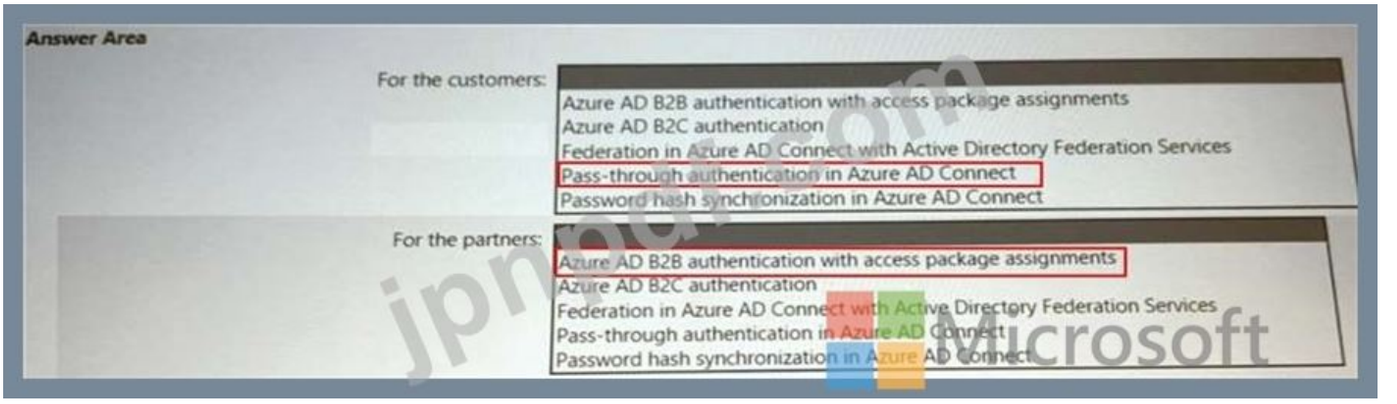
* パートナー企業が、割り当てられているプロジェクトの Microsoft SharePoint Online サイトにアクセスできるようにします。

このソリューションでは、追加のインフラストラクチャ コンポーネントを展開する必要性を最小限に抑える必要があります。推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

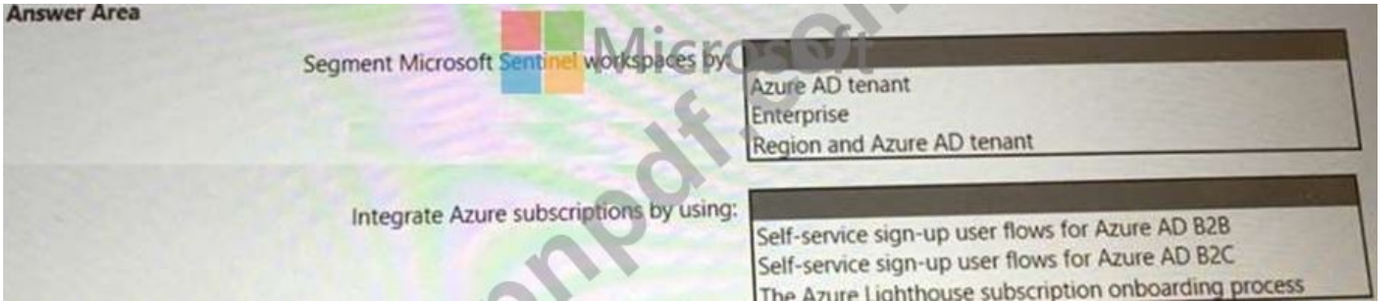


最新問題**: 4**

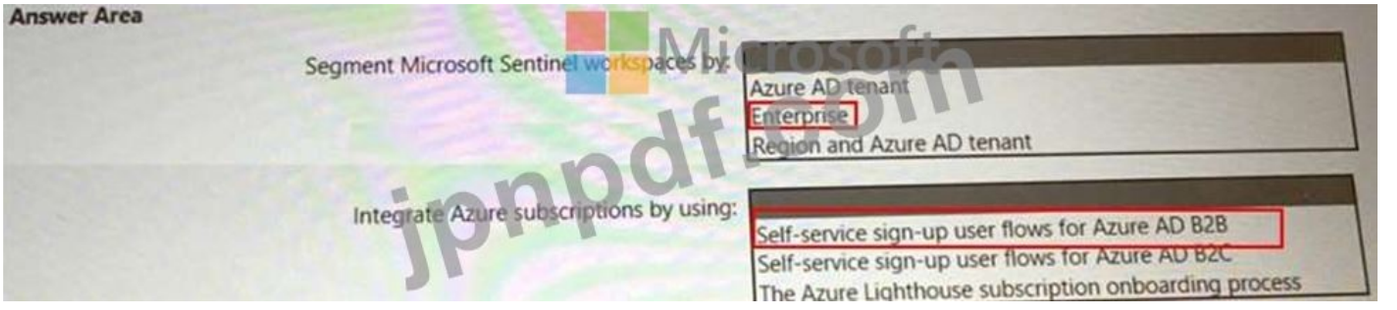
ハイブリッド要件、Microsoft Sentinel 要件、および法規制遵守要件を満たす SIEM および SOAR 戦略を推奨する必要があります。

何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 5**

Azure Cosmos DB Core (SQL) API アカウントのセキュリティ要件を計画しています。Azure Cosmos DB アカウントのデータにアクセスするすべてのユーザーを監査するソリューションを推奨する必要があります。推奨事項に含めるべき 2 つの構成はどれですか? それぞれの正解は、解決策の一部を示しています。注: 正しく選択するたびに 1 ポイントの価値があります。

A. Cosmos DB に対して Microsoft Defender を有効にします。

B. Azure Active Directory (Azure AD) のサインイン ログを Log Analytics ワークスペースに送信します。

C. Azure Cosmos DB のローカル認証を無効にします。

D. ID 用に Microsoft Defender を有効にします。

E. Azure Cosmos DB ログを Log Analytics ワークスペースに送信します。

Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs

最新問題**: 6**
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。不審な認証アクティビティのアラートがワークロード保護ダッシュボードに表示されます。
ワークフローの自動化を使用してアラートを評価および修正するソリューションを推奨する必要があります。ソリューションでは、開発労力を最小限に抑える必要があります。推奨事項には何を含めるべきですか?
A. Azure Monitor Webhook
B. Azure ロジック アプリ
C. Azure Event Hubs
D. Azure Functions アプリ
Answer: B (メーッセージを残す**)**
説明
Microsoft Defender for Cloud のワークフロー自動化機能は、セキュリティ アラート、推奨事項、規制遵守の変更に応じて Logic Apps をトリガーできます。注: Azure Logic Apps は、アプリ、データ、サービスやシステムなど。
このプラットフォームを使用すると、企業および企業間 (B2B) シナリオ向けの拡張性の高い統合ソリューションを迅速に開発できます。

最新問題**: 7**
あなたの会社にはオンプレミスの Microsoft SQL Server データベースがあります。
同社はデータベースを Azure に移行する予定です。
パッチ適用のための運用要件を最小限に抑え、動的データ マスキングを使用して機密データを保護する、データベースの安全なアーキテクチャを推奨する必要があります。ソリューションではコストを最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Azure SQL マネージド インスタンス
B. Azure 仮想マシン上の SQL Server
C. Azure SQL データベース
D. Azure Synapse Analytics 専用 SQL プール
Answer: (解答を表示する**)**

最新問題**: 8**
Microsoft 365 サブスクリプションをお持ちです
次のアクティビティを監視するには、セキュリティ ソリューションを推奨する必要があります。
* 侵害された可能性のあるユーザー アカウント
* Microsoft SharePoint Online からファイルの一括ダウンロードを実行するユーザー 各アクティビティの推奨事項には何を含める必要がありますか? 答えるには、適切なコンポーネントを正し

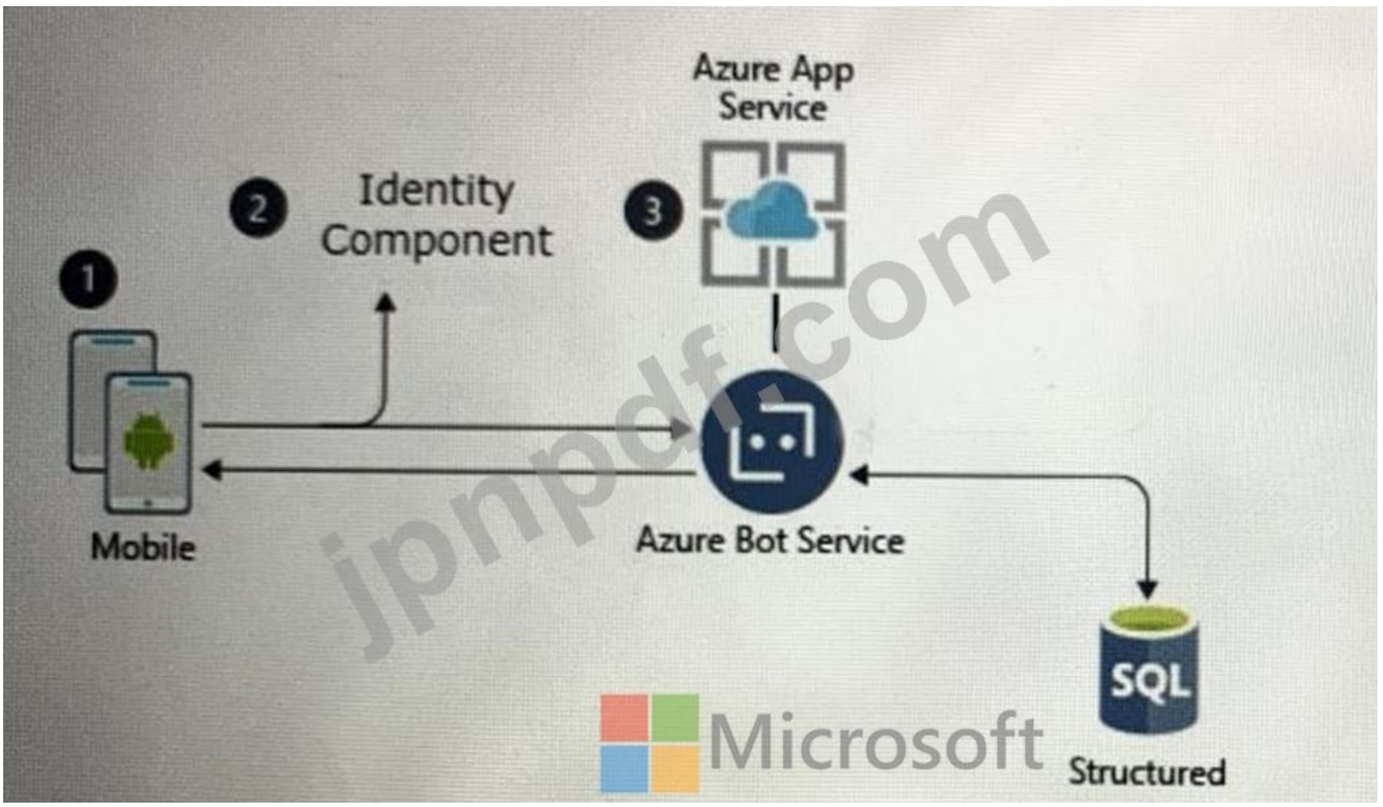
いアクティビティにドラッグします。各コンポーネントは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 各正解の選択は 1 ポイントの価値があります。

Answer:

説明

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks
https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

最新問題**: 9**
次の図に示すように、顧客は Azure を使用して、外部ユーザーが使用するモバイル アプリを開発しています。



アプリの ID 戦略を設計する必要があります。ソリューションは次の要件を満たす必要があります。

* Google、Facebook、Microsoft アカウントなどの外部 ID の使用を有効にします。
※顧客のアイデンティティストアとは別に管理されます。
* 各アプリの完全にカスタマイズ可能なブランディングをサポートします。

デザインを完成させるためにどのサービスをお勧めしますか?

A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B
C. Azure AD コネクト
D. Azure Active Directory ドメイン サービス (Azure AD DS)

Answer: (解答を表示する**)**

説明

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow
https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

最新問題**: 10**

あなたは、Azure Front Door インスタンスを通じて Azure App Service Web アプリへのアクセスを提供するためのセキュリティ戦略を設計しています。Web アプリが Front Door インスタンスを介したアクセスのみを許可するようにするソリューションを推奨する必要があります。

解決策: Front Door ID を持つ HTTP ヘッダーに基づいてアクセス制限を行うことをお勧めします。

これは目標を達成していますか?
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-正面玄関−

最新問題**: 11**
顧客は Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを持っています。
お客様は、セキュリティ インシデントを一元管理し、ログを分析し、アクティビティを監査し、展開されているすべてのサービスにわたる潜在的な脅威を検索したいと考えています。
顧客にソリューションを推奨する必要があります。ソリューションではコストを最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Microsoft 365 Defender
B. クラウド用 Microsoft Defender
C. マイクロソフト センチネル
D. クラウド アプリ向け Microsoft Defender
Answer: C (メーッセージを残す**)**

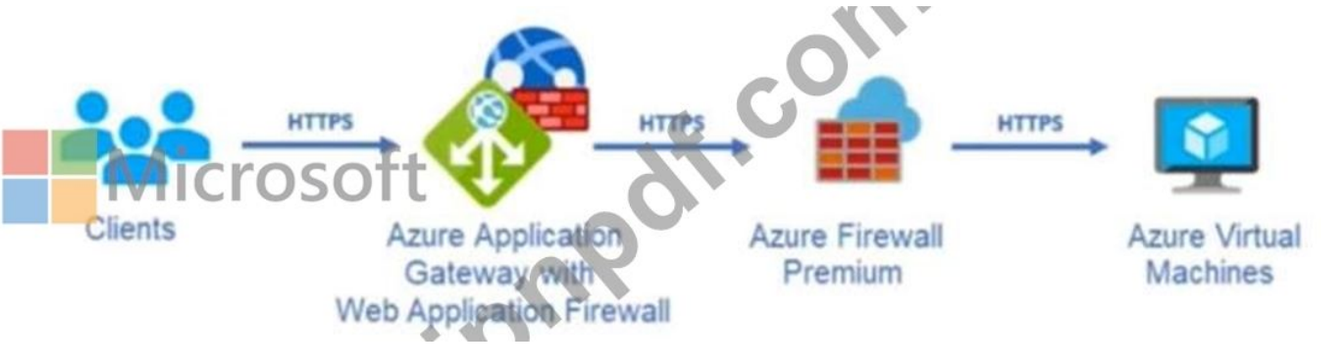
最新問題**: 12**
あなたの会社は Microsoft 365 サブスクリプションを持っており、ID に Microsoft Defender を使用しています。ID の侵害に関連するインシデントについて通知されます。
攻撃者が悪用できるように複数のアカウントを公開するソリューションを推奨する必要があります。攻撃者がアカウントを悪用しようとした場合、アラートをトリガーする必要があります。どの Defender for Identity 機能を推奨事項に含めるべきですか?
A. スタンドアロンセンサー
B. ハニートークン エンティティ タグ
C. 機密ラベル
D. カスタム ユーザー タグ
Answer: B (メーッセージを残す**)**
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity Sensitive タグは、価値の高い資産を識別するために使用されます。(ユーザー / デバイス / グループ)ハニートークン エンティティは悪意のある攻撃者の罠として使用されます。これらのハニートークン エンティティに関連付けられた認証により、アラートがトリガーされます。Defender for Identity は、Exchange サーバーを価値の高い資産と見なし、自動的に機密としてタグ付けします。

最新問題**: 13**

あなたの会社には、Splunk と Microsoft Sentinel を使用するサードパーティのセキュリティ情報およびイベント管理 (SIEM) ソリューションがあります。Microsoft Sentinel と Splunk を統合する予定です。
Microsoft Sentinel から Splunk にセキュリティ イベントを送信するソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. Microsoft Sentinel データ コネクタ
B. Azure イベント ハブ
C. Azure データ要素
D. Microsoft Sentinel ワークブック
Answer: (解答を表示する**)**
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029

最新問題**: 14**
Active Directory Domain Services (AD DS) ドメインと同期する Azure AD テナントがあります。クライアント コンピューターは Windows を実行し、Azure AD にハイブリッド参加しています。
あなたは、ランサムウェアからエンドポイントを保護する戦略を設計しています。この戦略は Microsoft セキュリティのベスト プラクティスに従っています。
Windows コンピュータの管理者グループからすべてのドメイン アカウントを削除する予定です。
アクセスが必要な場合にのみ Windows コンピュータへの管理アクセスをユーザーに提供するソリューションを推奨する必要があります。このソリューションでは、コンピュータの管理者アカウントが侵害された場合に、ランサムウェア攻撃の横方向の動きを最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Azure AD Privileged Identity Management (PIM)
B. ローカル管理者パスワード ソリューション (LAPS)
C. Azure AD ID 保護
D. 特権アクセス ワークステーション (PAW)
Answer: B (メーッセージを残す**)**

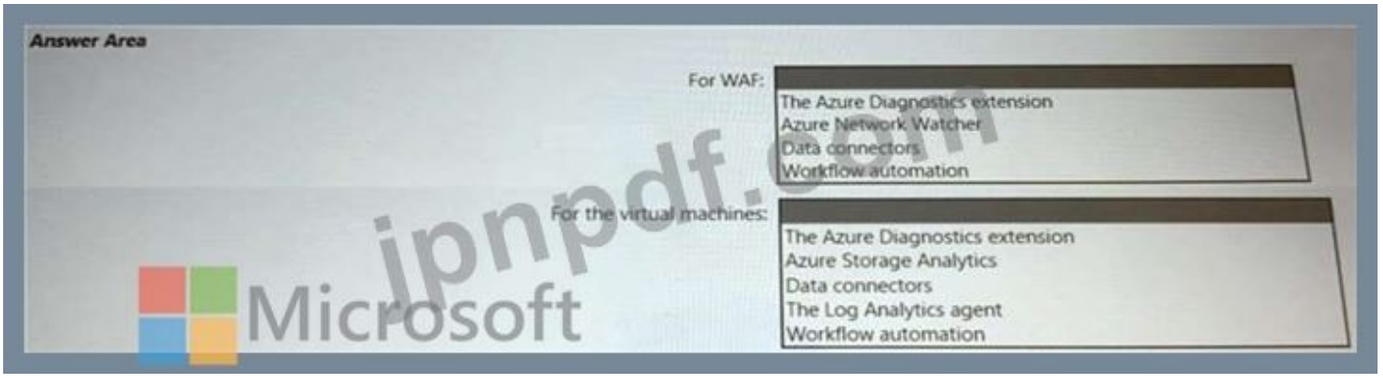
最新問題**: 15**
あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。



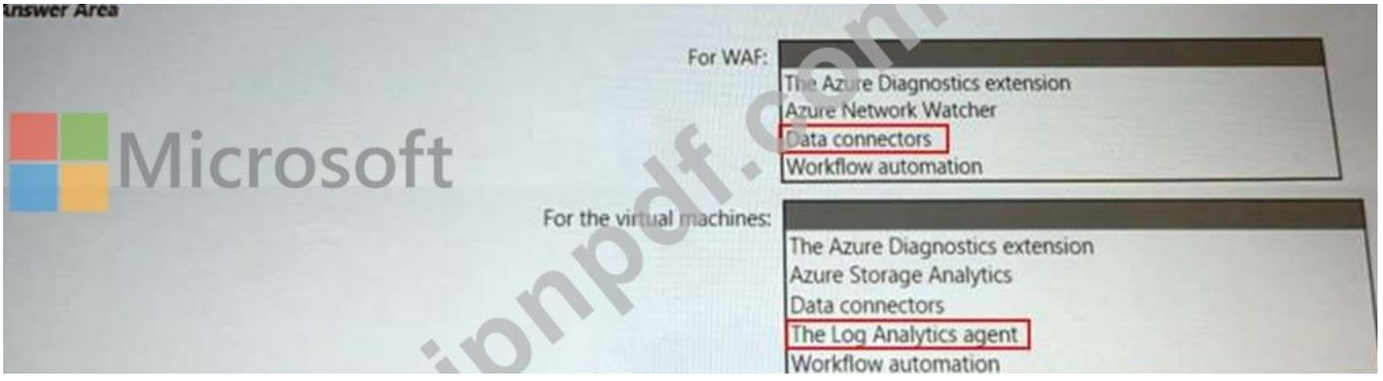
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。

* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。
* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。

ソリューションには何を含めるべきでしょうか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 16**

Azure 環境のコンプライアンスを評価しています。

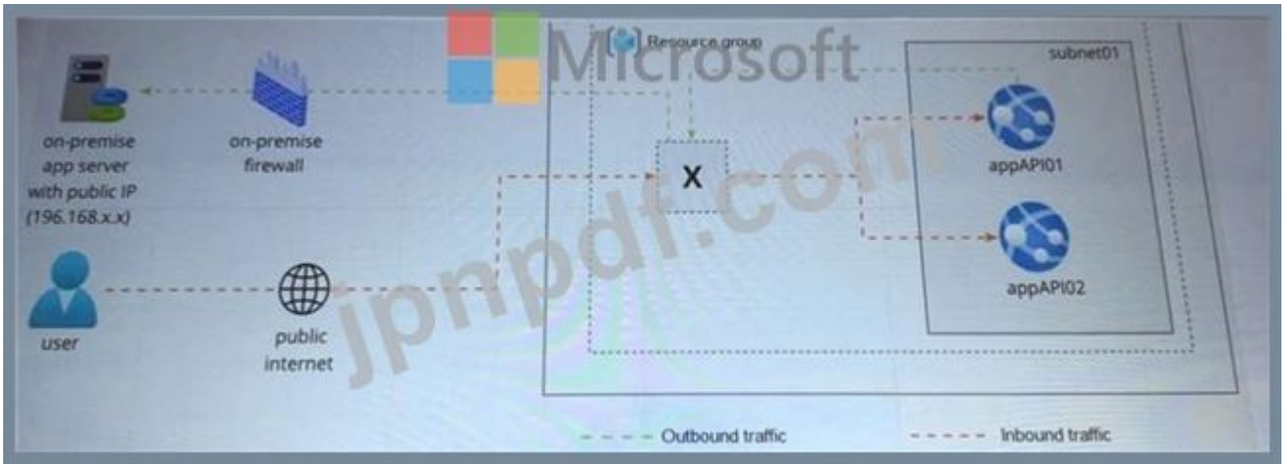
リソースを変更せずにコンプライアンスを評価するために使用できる Azure Policy 実装を設計する必要があります。

Azure Policy ではどの効果を使用する必要がありますか?

A. 拒否
B. 変更
C. 無効
D. 追加

Answer: A (メーッセージを残す)

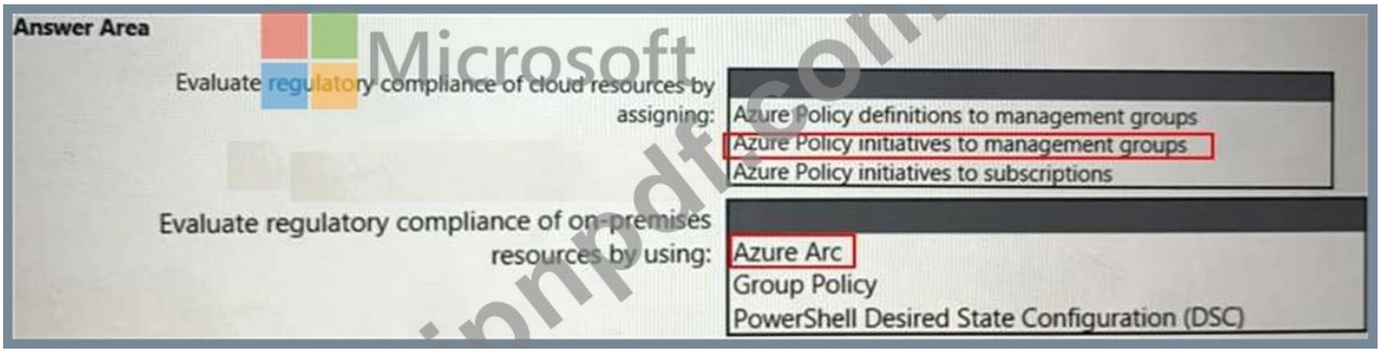
最新問題: **17**
あなたの会社は、展示に示されているように、Azure App Service Environment (ASE) Web アプリのアプリケーション アーキテクチャを設計しています。(展示」タブをクリックします。)



オンプレミス ネットワークと Azure の間の通信には ExpressRoute 接続が使用されます。
Web アプリがオンプレミスのアプリケーション サーバーと確実に通信できるようにするソリューションを推奨する必要があります。ソリューションでは、オンプレミス ネットワークへのアクセスが許可されるパブリック IP アドレスの数を最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. ユーザー定義ルート (UDR) を備えた Azure Application Gateway v2。
B. ポリシー ルール セットを備えた Azure Firewall
C. Azure Web アプリケーション ファイアウォール (WAF) を備えた Azure Front Door
D. 優先トラフィック ルーティング方法を備えた Azure Traffic Manager
Answer: (解答を表示する)

最新問題: **18**
管理された環境全体にわたる法規制への準拠を評価するソリューションを推奨する必要があります。ソリューションは、法規制遵守要件とビジネス要件を満たしている必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

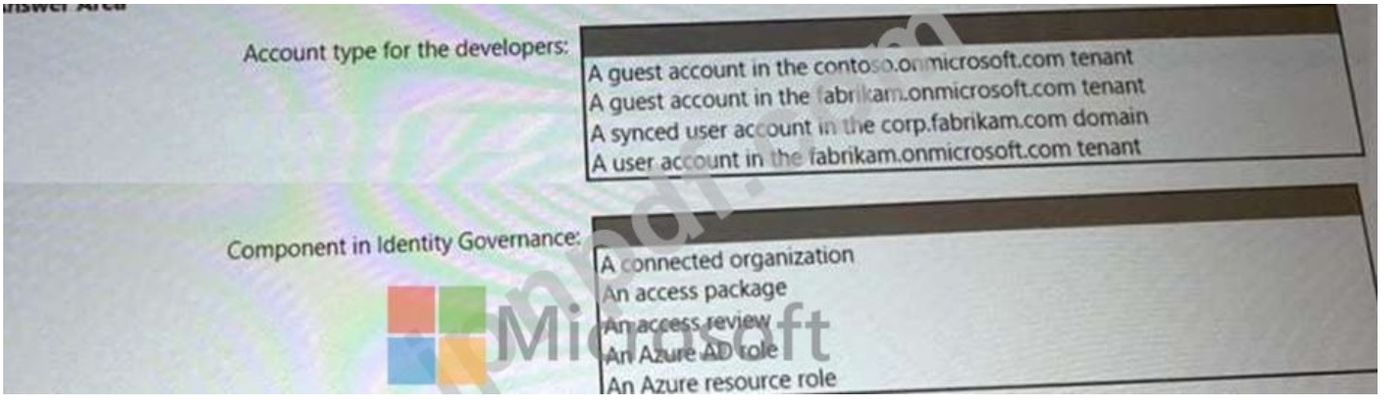
Answer:



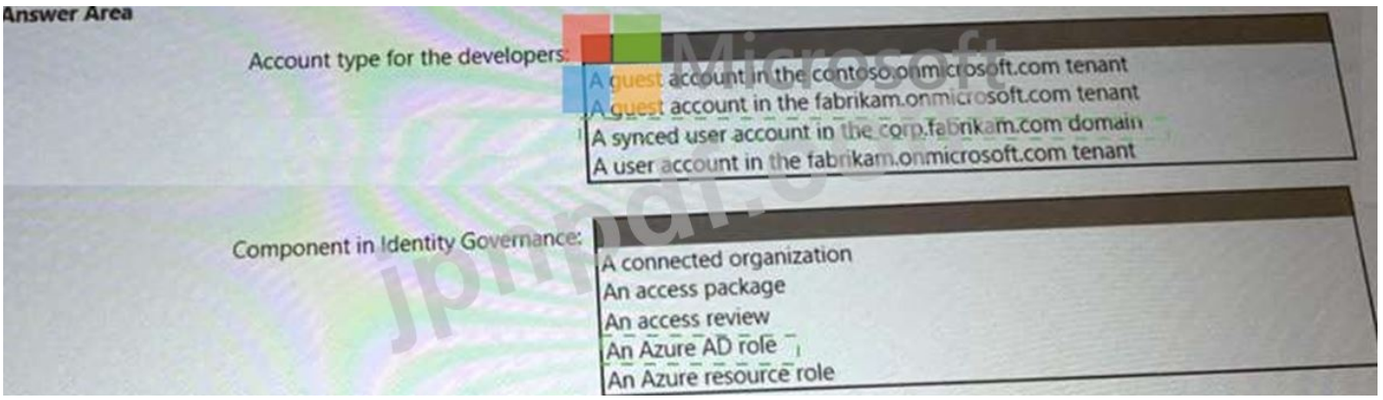
Explanation:

最新問題**: 19**

Contoso 開発者の要件を満たすには、Azure AD で何を作成する必要がありますか?



Answer:



最新問題: **20**
InfraSec グループのセキュリティ要件を満たすソリューションを推奨する必要があります。アクセスを委任するには何を使用する必要がありますか?
A. サブスクリプション
B. カスタムのロールベースのアクセス制御 (RBAC) ロール
C. リソースグループ
D. 管理グループ
Answer: A (メーッセージを残す**)**
トピック 2、Litware, Inc.
既存の環境
Litware には、Utvvare.com という名前の Active Directory Domain Services (AD D%) フォレストと同期する Azure Active Directory (Azure AD) テナントがあり、20 の Azure サブスクリプションにリンクされています。Azure AD Connect は、パススルー認証の実装に使用されます。パスワード ハッシュ同期は無効になり、パスワード ライトバックは有効になります。すべての Litware ユーザーは Microsoft 365 E5 ライセンスを持っています。
この環境には、いくつかの AD DS フォレスト、Azure AD テナント、および Litware の子会社に属する数百の Azure サブスクリプションも含まれています。
計画された変更
Litware は次の変更を実装する予定です。
* Azure AD テナントごとに管理グループ階層を作成します。
* Litware の既存の Azure 環境をリファクタリングし、将来のすべての Azure ワークロードをデプロイするためのランディング ゾーン戦略を設計します。
* Azure AD アプリケーション プロキシを実装して、現在 VPN を使用してアクセスされている内部アプリケーションへの安全なアクセスを提供します。
ビジネス要件
Litware は次のビジネス要件を特定します。
* 追加のオンプレミス インフラストラクチャを最小限に抑えます。
* 管理オーバーヘッドに関連する運用コストを最小限に抑えます。
ハイブリッドの要件
Litware では、次のハイブリッド クラウド要件を特定しています。
* Azure からの次のようなオンプレミス リソースの管理を有効にします。

* 施行とコンプライアンスの評価には Azure Policy を使用します。
* 変更追跡と資産インベントリを提供します。
* パッチ管理を実装します。
* ゲスト アカウントの維持にかかるオーバーヘッドを発生させずに、一元的なテナント間サブスクリプション管理を提供します。

Microsoft Sentinelの要件

Litware は、Microsoft Sentinel のセキュリティ情報およびイベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAK) 機能を活用する予定です。同社は、Microsoft Sentinel を使用して Security Operations Center (SOQ) を一元化したいと考えています。

アイデンティティ要件

Litware は次の ID 要件を特定します。
* AD DS ユーザー アカウントを直接ターゲットとするブルート フォース攻撃を検出します。
* Litware の Azure AD テナントに漏洩した資格情報の検出を実装します。
* Azure AD ユーザー アカウントをターゲットとしたブルート フォース攻撃によって AD DS ユーザー アカウントがロックアウトされるのを防ぎます。
* Litware の Azure AD テナントにユーザーとグループの委任管理を実装します (サポートを含む)。
* グループのプロパティ、メンバーシップ、およびライセンスの管理 ユーザーのプロパティ、パスワード、およびライセンスの管理
* ビジネスユニットに基づいたユーザー管理の委任。

規制遵守要件

Litware では、次の規制遵守要件を特定しています。
* 米国およびフランスに拠点を置く各子会社が所有するログ、テレメトリ、およびデータを収集する際に、データ常駐に関するコンプライアンスを保証します。
* 組み込みの Azure Policy 定義を活用して、管理された環境全体にわたる法規制への準拠を評価します。
* 最小特権の原則を使用します。

Azure ランディング ゾーンの要件

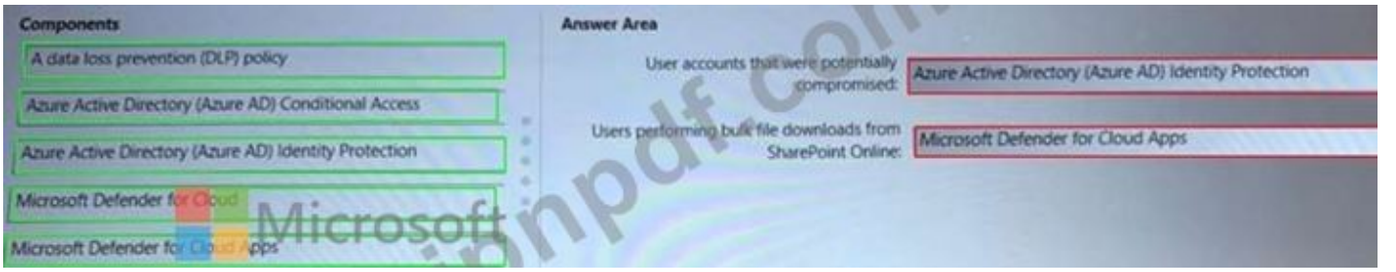
Litware は、次のランディング ゾーン要件を特定します。
* インターネットに向かうすべてのトラフィックを、専用の Azure サブスクリプションの Azure Firewall 経由でランディング ゾーンからルーティングします。
* ランディング ゾーンを対象とした安全なスコアを提供します。
* 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信していることを確認します。
* データ漏洩の可能性を最小限に抑えます。
* ネットワーク帯域幅を最大化します。

ランディング ゾーン アーキテクチャには、インターネットおよびハイブリッド接続のハブとして機能する専用のサブスクリプションが含まれます。各ランディング ゾーンには次の特徴があります。
* 専用のサブスクリプションで作成されます。
* litware.com の DNS 名前空間を使用します。
アプリケーションのセキュリティ要件
Litware は、次のアプリケーションのセキュリティ要件を特定します。
* Azure AD アプリケーション プロキシを使用してシングル サインオン (SSO) をサポートする内部アプリケーションを特定します。
* Microsoft SharePoint Online および Exchange Online データへのアクセスをリアルタイムで監視および制御します。

最新問題: **21**
あなたの会社は、すべてのオンプレミス ワークロードを Azure および Microsoft 365 に移行しようとしています。次の要件を満たす Microsoft Sentinel でセキュリティ オーケストレーション、自動化、および応答 (SOAR) 戦略を設計する必要があります。
* セキュリティ運用アナリストによる手動介入を最小限に抑えます
* Microsoft Teams チャネル内での Waging アラートをサポート
戦略には何を含めるべきでしょうか?
A. データコネクタ
B. プレイブック
C. ワークブック
D. KQL
Answer: C (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

最新問題: **22**
Microsoft 365 サブスクリプションをお持ちです
次のアクティビティを監視するには、セキュリティ ソリューションを推奨する必要があります。
* 侵害された可能性のあるユーザー アカウント
* Microsoft SharePoint Online からファイルの一括ダウンロードを実行するユーザー 各アクティビティの推奨事項には何を含める必要がありますか? 答えるには、適切なコンポーネントを正しいアクティビティにドラッグします。各コンポーネントは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 各正解の選択は 1 ポイントの価値があります。

Answer:

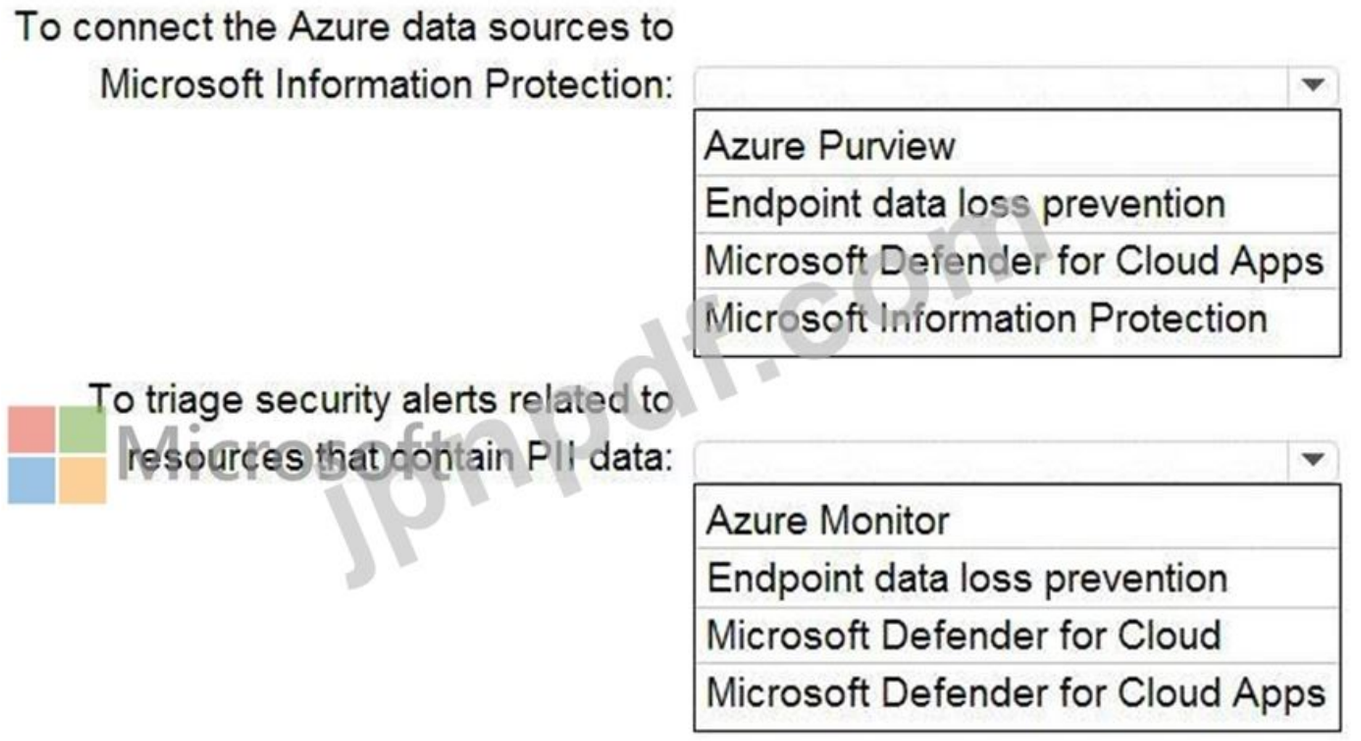


最新問題**: 23**

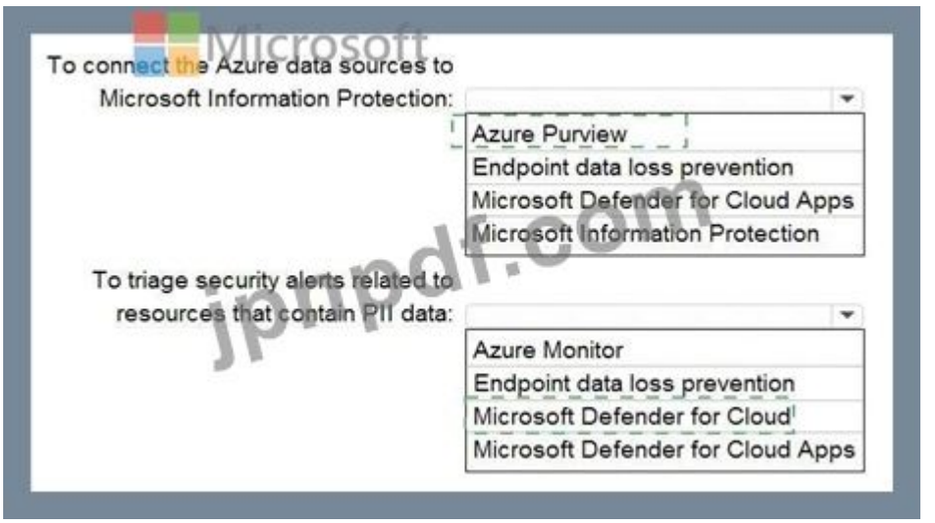
あなたの会社はデータを Azure に移行しています。データには個人を特定できる情報 (PII) が含まれています。同社は、Azure の PII データ ストアに Microsoft Information Protection を使用する予定です。Azure リソース内でリスクにさらされている PLL データを検出するソリューションを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

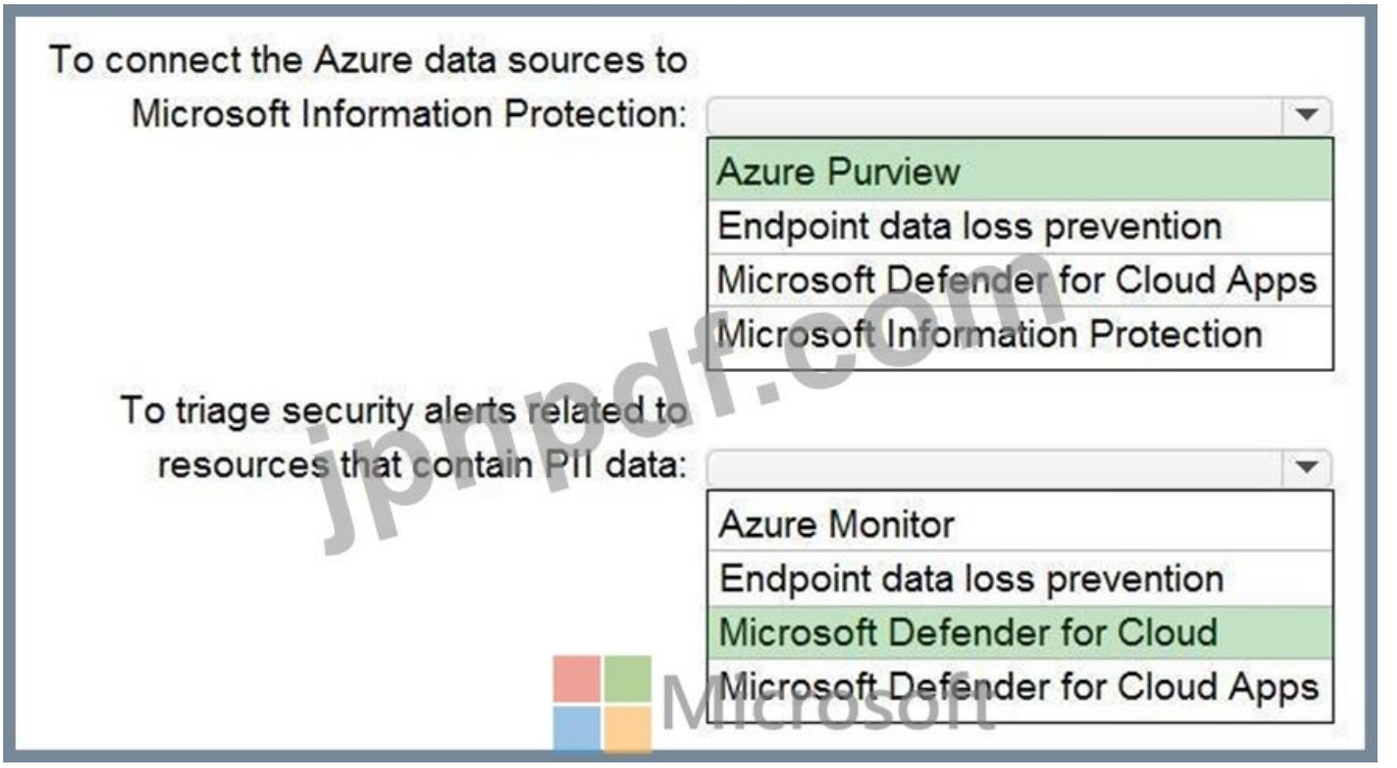


Answer:



説明

グラフィカル ユーザー インターフェイス、テキスト、アプリケーションの説明が自動生成される



データの機密性に基づいてセキュリティアクションに優先順位を付けます。

https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection。Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure リソースも同様) については、次のとおりです。

https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu

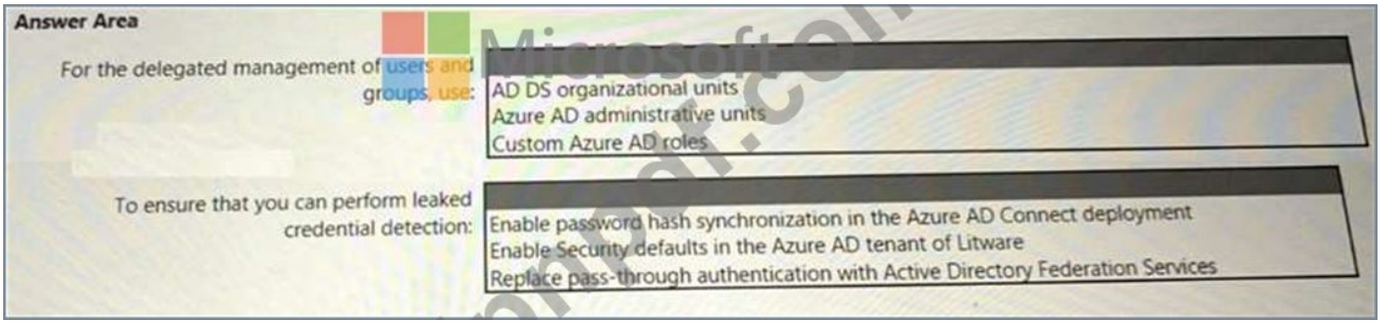
最新問題: **24**

SharePoint Online と Exchange Online のデータを保護するための戦略を設計する必要があります。ソリューションはアプリケーションのセキュリティ要件を満たしている必要があります。

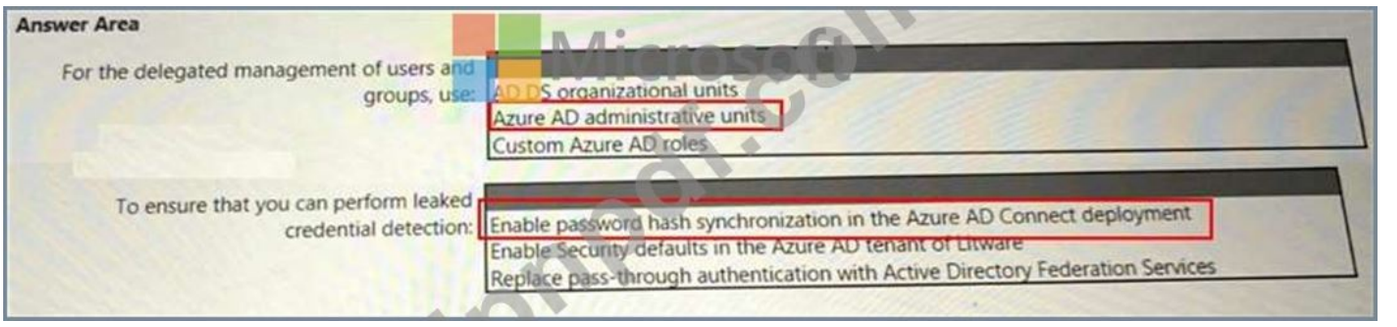
戦略で活用すべき 2 つのサービスはどれですか? それぞれの正解は、解決策の一部を示しています。ノート; 正しく選択するたびに 1 ポイントの価値があります。
A. Azure AD 条件付きアクセス
B. クラウド アプリ向け Microsoft Defender
C. クラウド用 Microsoft Defender
D. エンドポイント用 Microsoft Defender
E. Azure AD でのアクセスレビュー
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#conditional-access-application-control
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cloud-application-security

最新問題**: 25**
あなたの会社は、Azure Active Directory (Azure AD) B2C を使用する請求書発行アプリケーションを開発しています。
アプリケーションは App Service Web アプリとしてデプロイされます。ID 関連の攻撃からアプリケーションを保護するためのソリューションをアプリケーション開発チームに推奨する必要があります。どの 2 つの構成をお勧めしますか? それぞれの正解は、解決策の一部を示しています。注: 正しく選択するたびに 1 ポイントの価値があります。
A. Identity Governance のパッケージにアクセスします
B. Azure AD B2C のカスタム リソース所有者パスワード資格情報 (ROPC) フロー
C. Azure AD 条件付きアクセスとユーザー フローおよびカスタム ポリシーの統合
D. Azure AD B2C のスマート アカウント ロックアウト
E. リスク検出を監視するための Azure AD ワークブック
Answer: C,D (メーッセージを残す**)**

最新問題**: 26**
Litware の Azure AD テナントに ID セキュリティ ソリューションを推奨する必要があります。ソリューションは、ID 要件と法規制遵守要件を満たしている必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: **27**

Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを持っています。あなたは Microsoft Sentinel 展開を設計しています。

セキュリティ運用チームにソリューションを推奨する必要があります。ソリューションには、セキュリティ イベントを分析するためのカスタム ビューとダッシュボードが含まれている必要があります。Microsoft Sentinel で何を使用することをお勧めしますか?

A. プレイブック

B. ワークブック

C. ノート

D. 脅威インテリジェンス

Answer: B (メーッセージを残す**)**

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

最新問題: **28**

管理された環境全体にわたる法規制への準拠を評価するソリューションを推奨する必要があります。ソリューションは、法規制遵守要件とビジネス要件を満たしている必要があります。

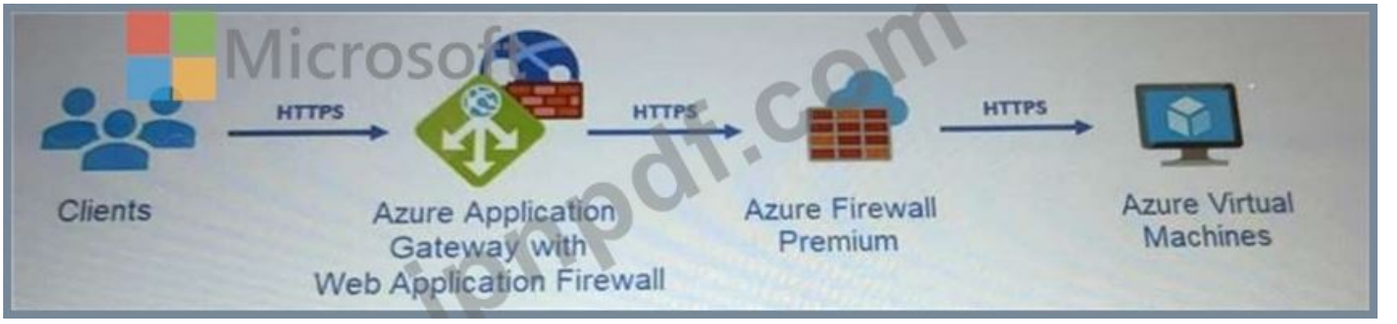
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題: **29**

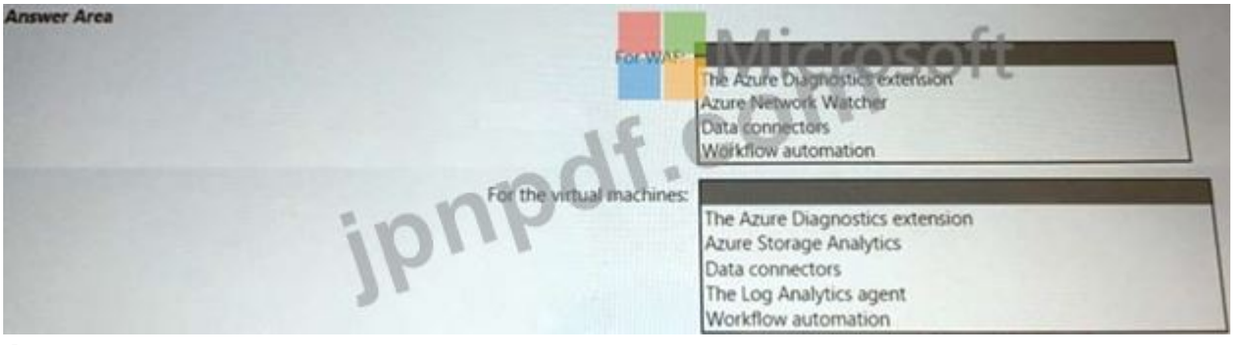
あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。



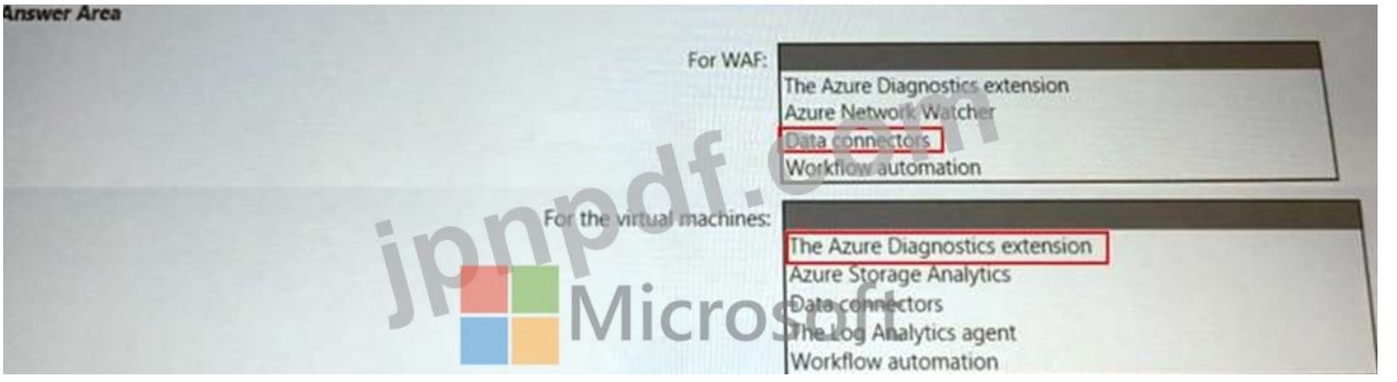
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。

* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。
* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。

ソリューションには何を含めるべきでしょうか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。

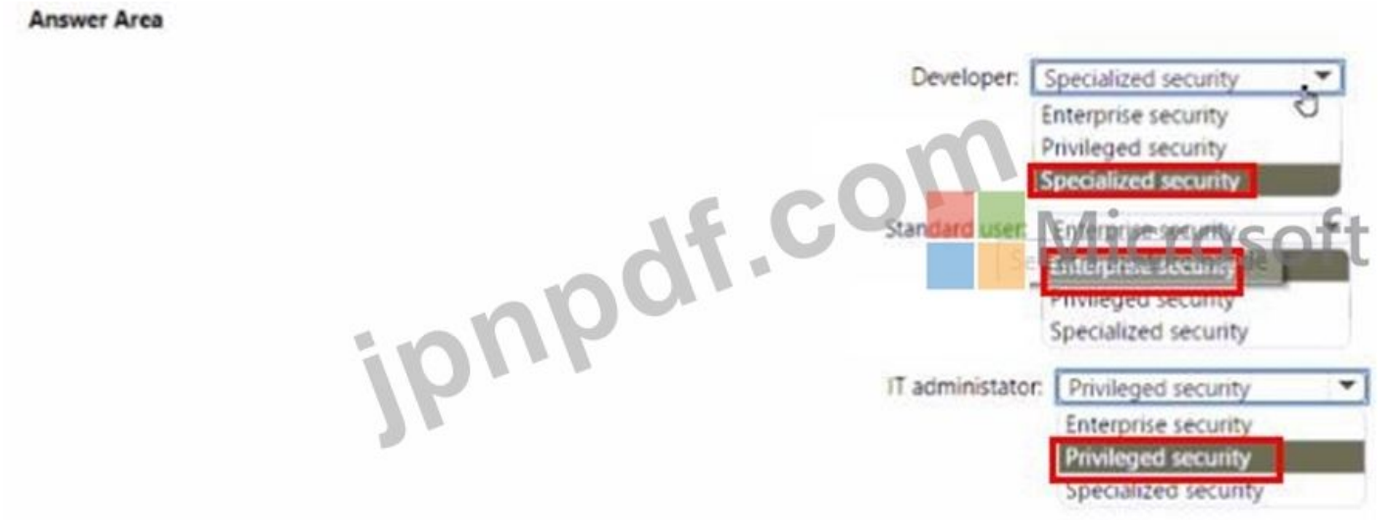


Answer:

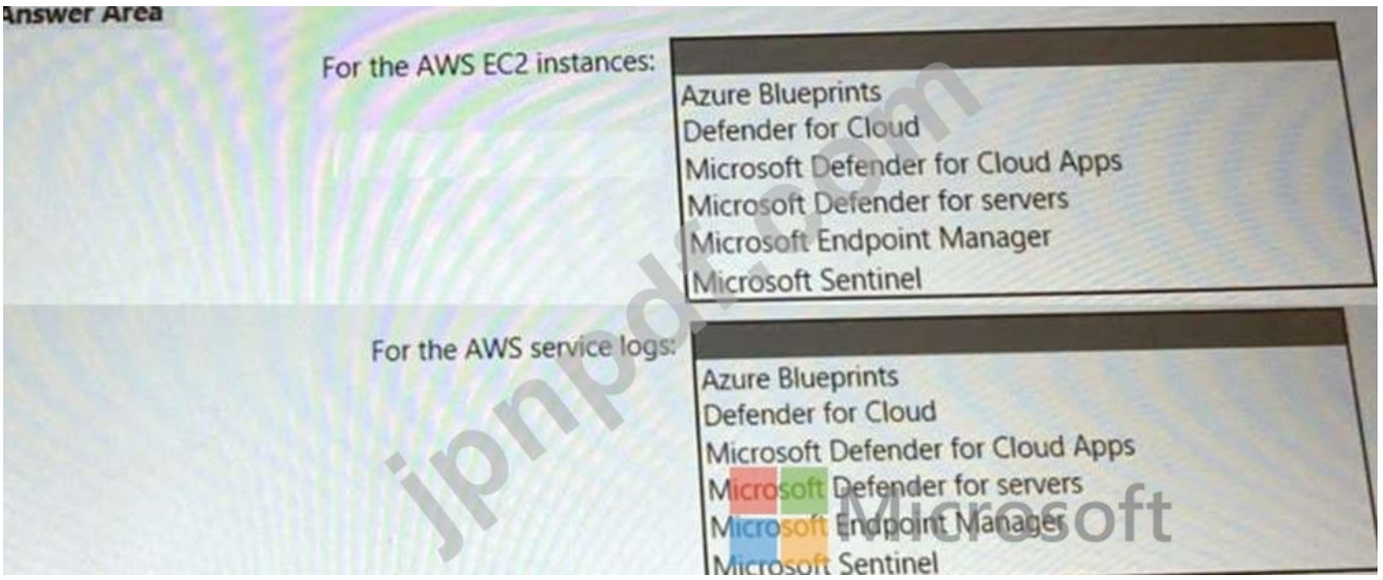


最新問題: **30**
セキュリティ アクセス戦略のセキュリティ レベルを計画しています。
どのジョブの役割をどのセキュリティ レベルで構成するかを特定する必要があります。ソリューションは、Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。
各職務にどのセキュリティ レベルを設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

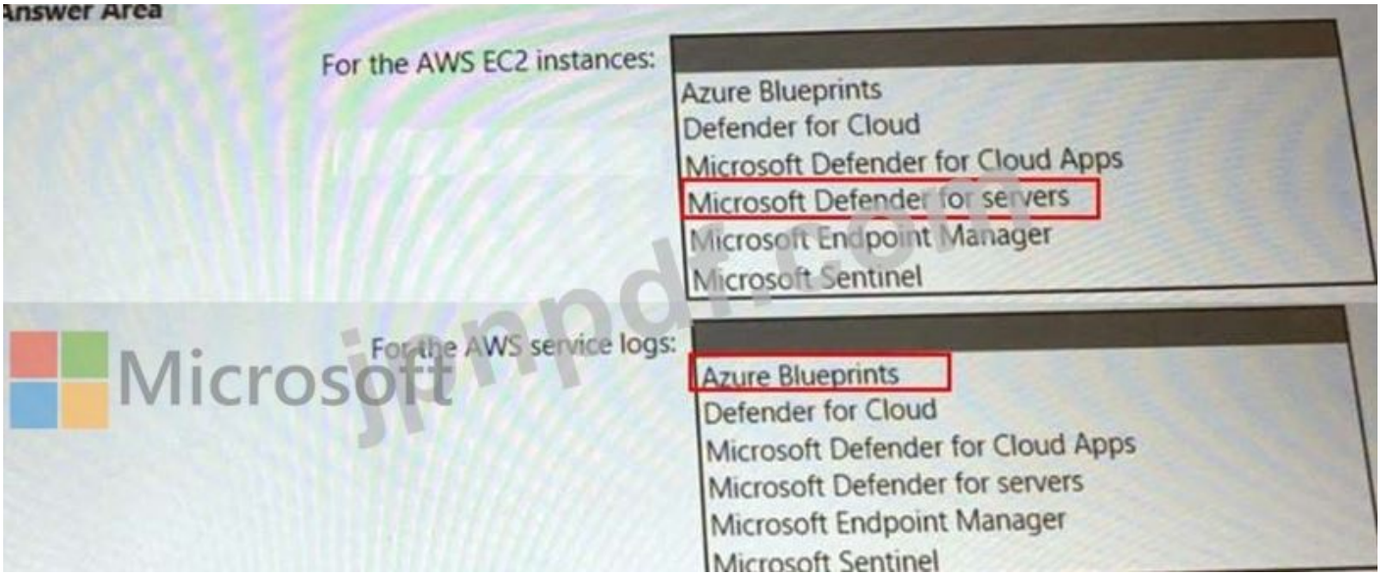
Answer:



最新問題: **31**
AWS の要件を満たすソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 32**

あなたの会社は、Azure 向け Microsoft Cloud Adoption Framework の DevSecOps ベスト プラクティスに従うことを計画しています。

Microsoft Cloud Adoption Framework for Azure に基づいたトップダウン アプローチを使用して脅威モデリングを実行する必要があります。

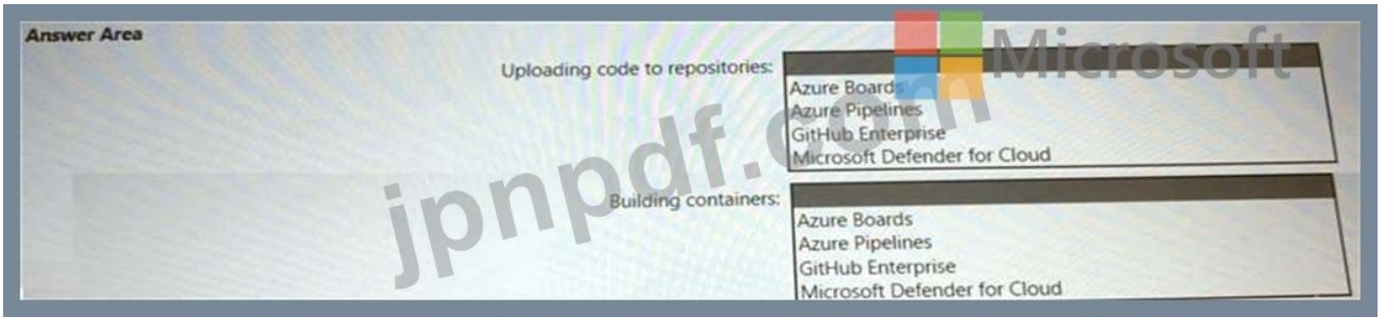
脅威モデリング プロセスを開始するには何を使用する必要がありますか?

A. STRIDEモデル
B. DREAD モデル
C. OWASP 脅威モデリング
Answer: C (メーッセージを残す**)**

最新問題**: 33**
あなたの会社は Microsoft 365 E5 ライセンスと Azure サブスクリプションを持っています。
同社は、次の場所に保存されている機密データに自動的にラベルを付けることを計画しています。
* Microsoft SharePoint Online
* Microsoft Exchange Online
*マイクロソフトチーム
機密データを特定して保護するための戦略を推奨する必要があります。
機密ラベル ポリシーにはどの範囲を推奨する必要がありますか? 答えるには、適切なスコープを正しい場所にドラッグします。各スコープは、1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題**: 34**
あなたの会社には、コンテナー化された Web アプリをデプロイするために使用される Azure App Service プランがあります。Web アプリを App Service プランにデプロイするための安全な DevOps 戦略を設計しています。コード スキャン ツールを安全なソフトウェア開発ライフサイクルに統合する戦略を推奨する必要があります。コードは次の 2 つのフェーズでスキャンする必要があります。
コードをリポジトリにアップロードする コンテナを構築する
各フェーズのコード スキャンをどこに統合する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。



Answer:

最新問題: **35**

あなたの会社には、コンテナー化された Web アプリをデプロイするために使用される Azure App Service プランがあります。Web アプリを App Service プランにデプロイするための安全な DevOps 戦略を設計しています。コード スキャン ツールを安全なソフトウェア開発ライフサイクルに統合する戦略を推奨する必要があります。コードは次の 2 つのフェーズでスキャンする必要があります。

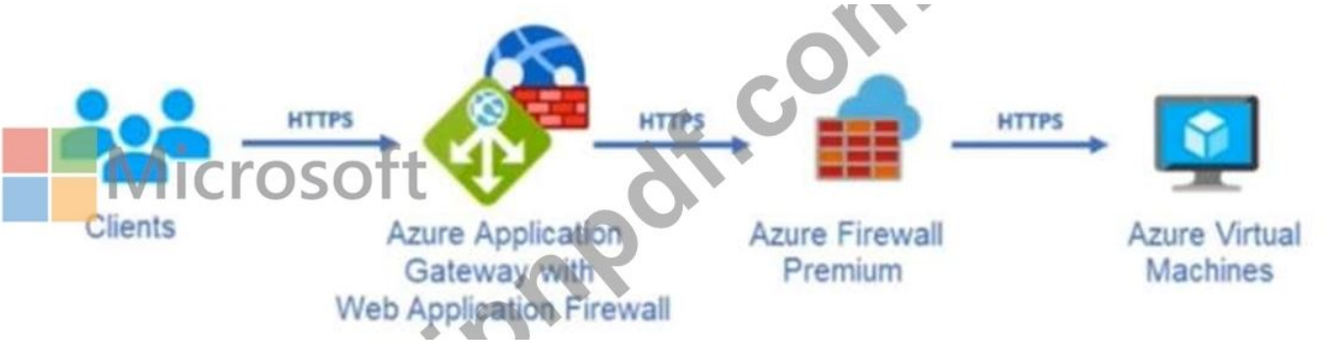
コードをリポジトリにアップロードする コンテナを構築する

各フェーズのコード スキャンをどこに統合する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

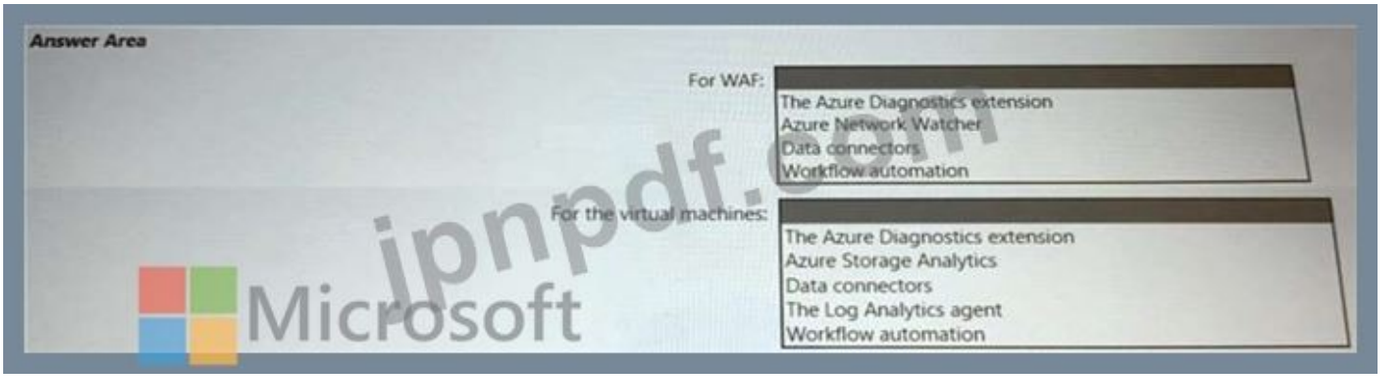
Answer:

最新問題: **36**

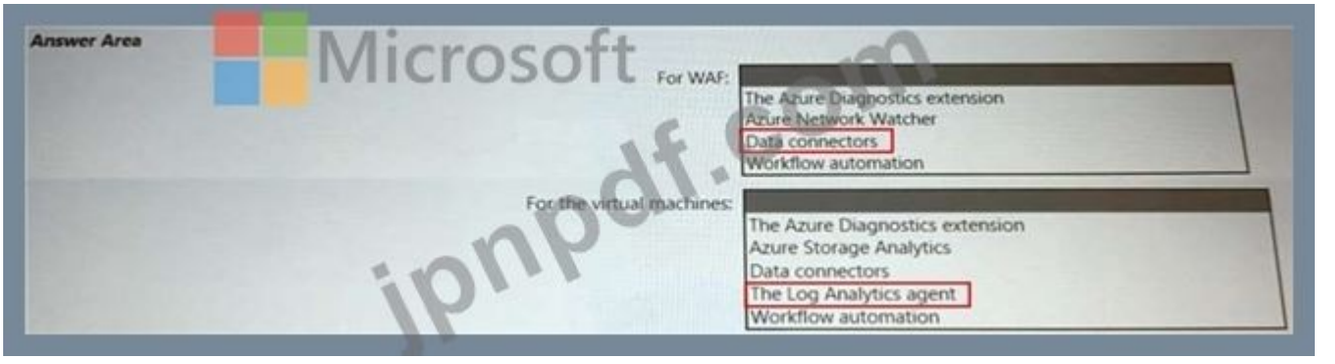
あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。



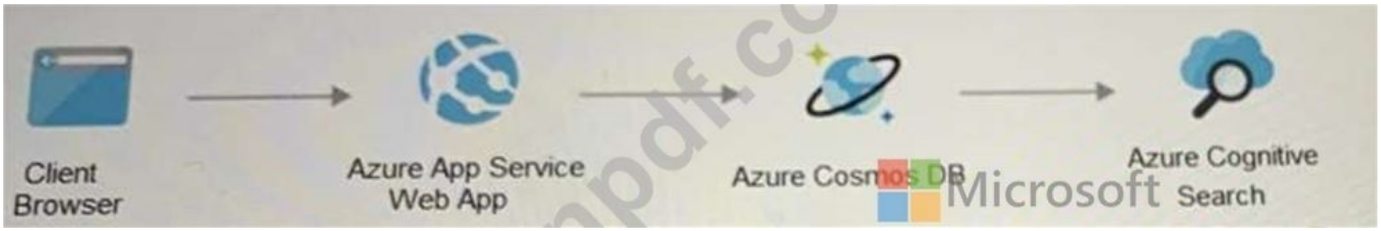
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。
* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。
* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。
ソリューションには何を含めるべきでしょうか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



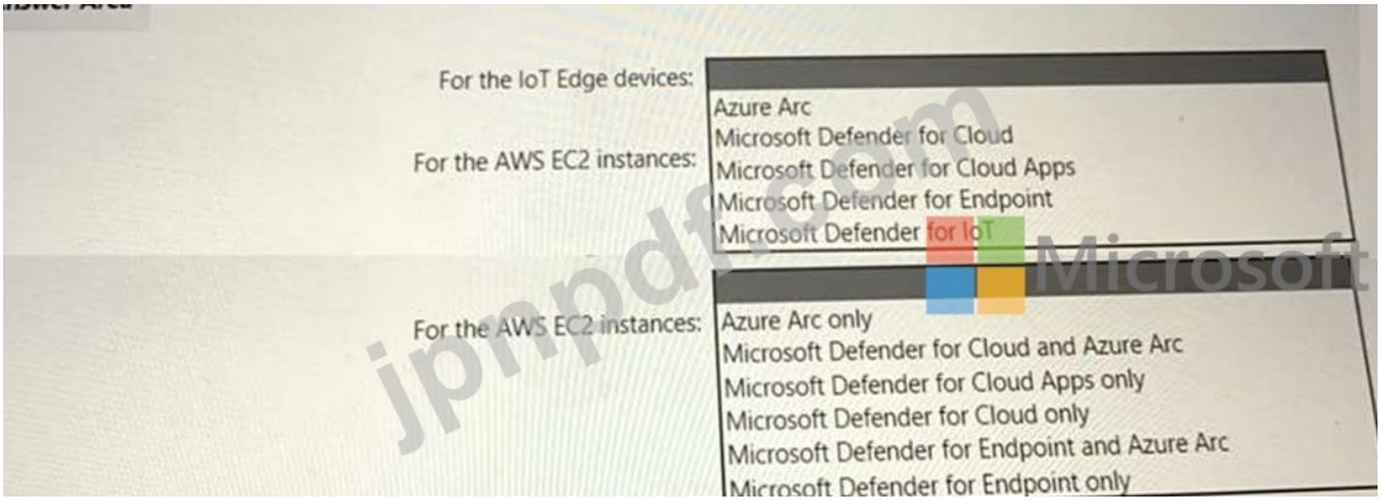
最新問題**: 37**
オンプレミス ネットワークには、Angular と Node.js で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行する予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。



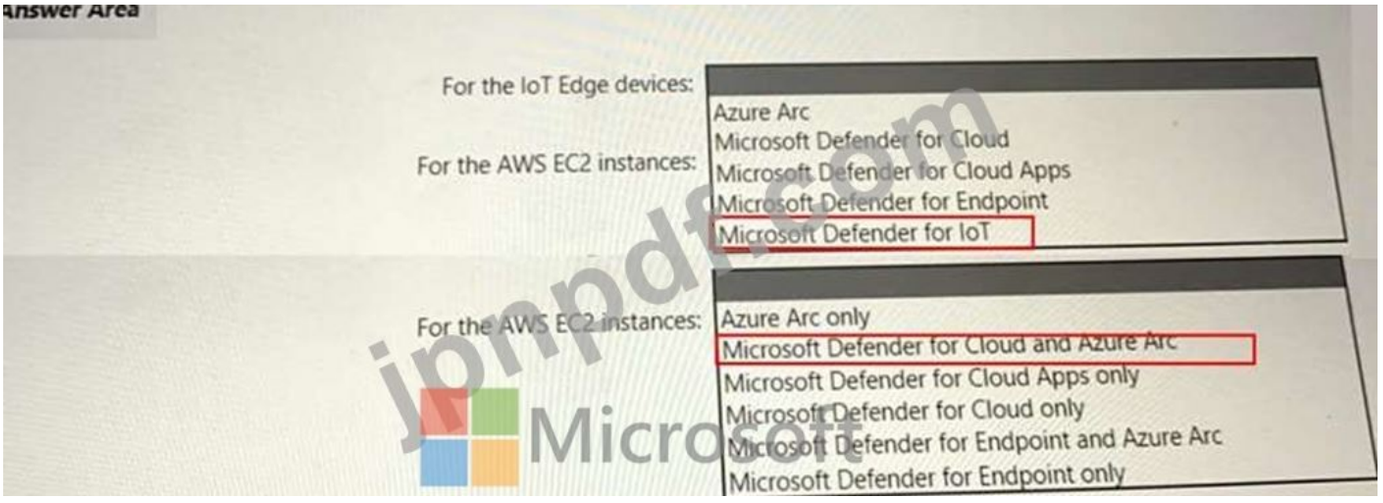
Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロトラスト モデルに従う必要があります。
解決策: Azure Web アプリケーション ファイアウォール (WAF) を使用して Azure Application Gateway を実装することをお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
説明
Azure が提供する PaaS サービス (Azure Storage、Azure Cosmos DB、Azure Web App など) を使用する場合は、PrivateLink 接続オプションを使用して、すべてのデータ交換がプライベート IP 空間経由で行われ、トラフィックが Microsoft ネットワークから出ないようにする必要があります。

最新問題: **38**
あなたの会社は、新しい Azure App Service Web アプリを開発しています。あなたは、Web アプリのセキュリティを検証するための設計支援を提供しています。
安全でないサーバー構成、クロスサイト スクリプティング (XSS)、SQL インジェクションなどの脆弱性について Web アプリをテストするためのソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. ランタイム アプリケーション SE/F 保護 (RASP)
B. 動的アプリケーション セキュリティ テスト (DAST)
C. 対話型アプリケーション セキュリティ テスト (IAST)
D. 静的アプリケーション セキュリティ テスト (SAST)
Answer: C (メーッセージを残す**)**

最新問題: **39**
あなたの会社には、Microsoft 365 サブスクリプション、Azure サブスクリプション、アマゾン ウェブ サービス (AWS) 実装を含むマルチクラウド環境があります。次のコンポーネントに対してセキュリティ体制管理ソリューションを推奨する必要があります。
* Azure LOT Edge デバイス
* AWS EC2 インスタンス
どのサービスを推奨事項に含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 40**

App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。

* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。

* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。

App1 のアクセス セキュリティ アーキテクチャを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答内の適切なオプションを選択してください。

ａ．注正しく選択するたびに 1 ポイントの価値があります。

Answer:

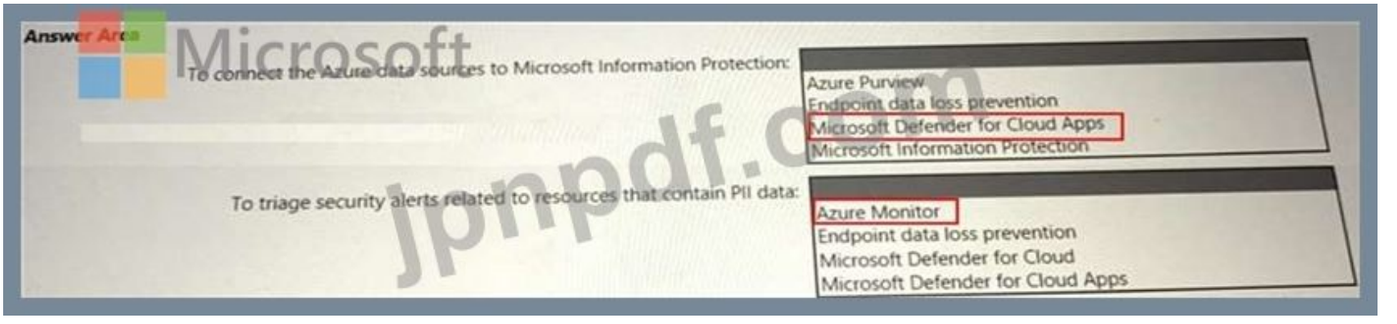
最新問題: **41**

あなたの会社はデータを Azure に移行しています。データには個人を特定できる情報 (PII) が含まれています。同社は、Azure の PII データ ストアに Microsoft Information Protection を使用する予定です。Azure リソース内でリスクにさらされている PLL データを検出するソリューションを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題: **42**

App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。

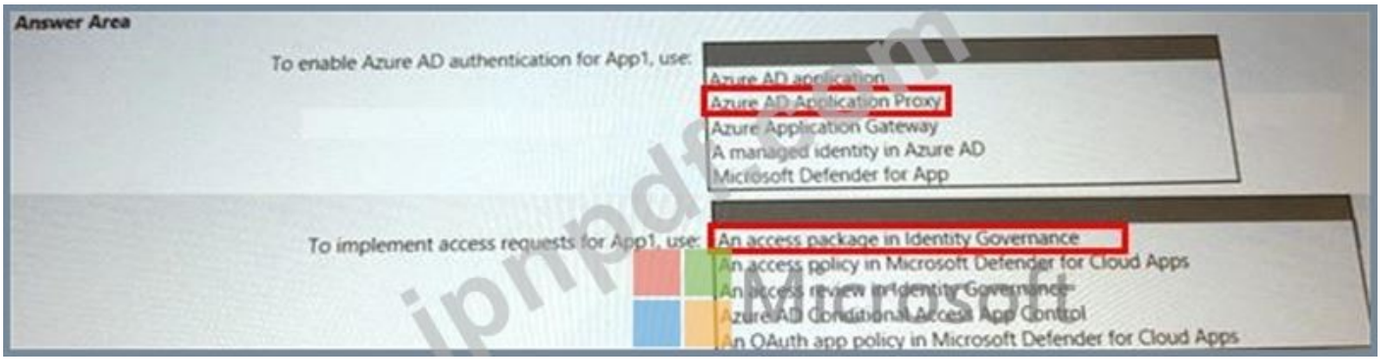
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。

App1 のアクセス セキュリティ アーキテクチャを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



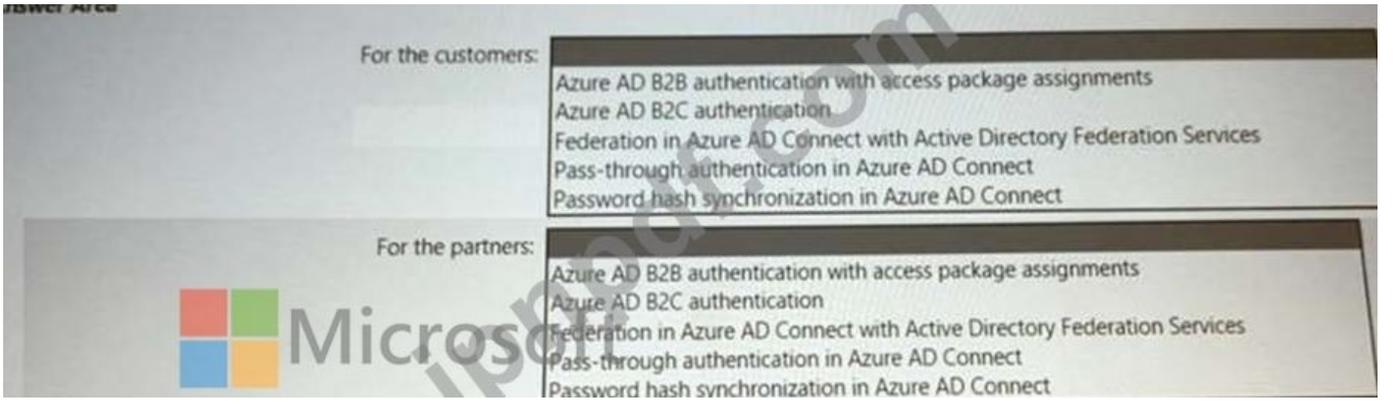
最新問題**: 43**

あなたの会社には Microsoft 365 E5 サブスクリプション、Azure サブスクリプション、オンプレミス アプリケーション、および Active Directory ドメイン サービス (AD DSV) があります。次の要件を満たす ID セキュリティ戦略を推奨する必要があります。

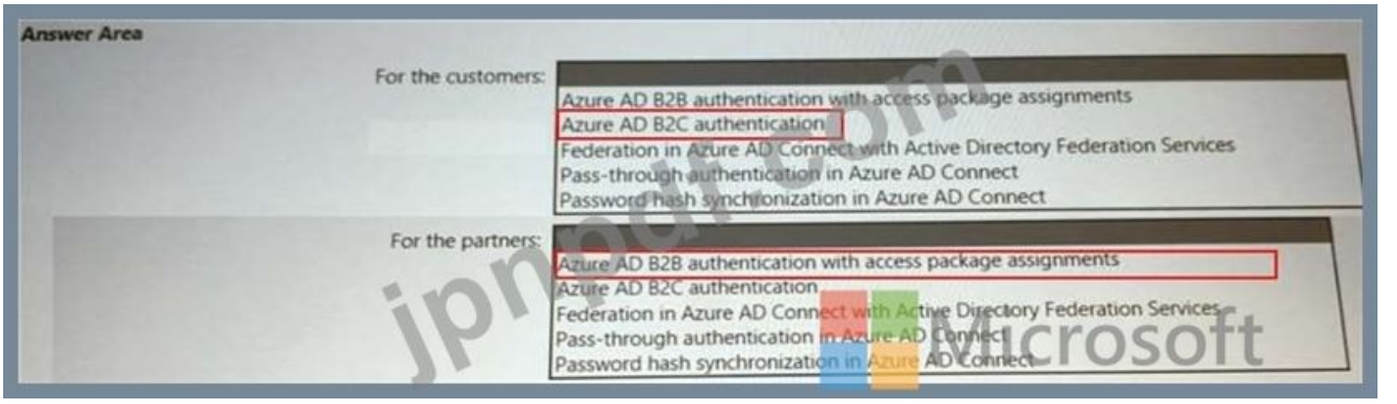
* 顧客が Facebook 資格情報を使用して Azure App Service Web サイトへの認証を行えることを保証します

* パートナー企業が、割り当てられているプロジェクトの Microsoft SharePoint Online サイトにアクセスできるようにします。ソリューションでは、追加のインフラストラクチャ コンポーネントを展開する必要性を最小限に抑える必要があります。推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

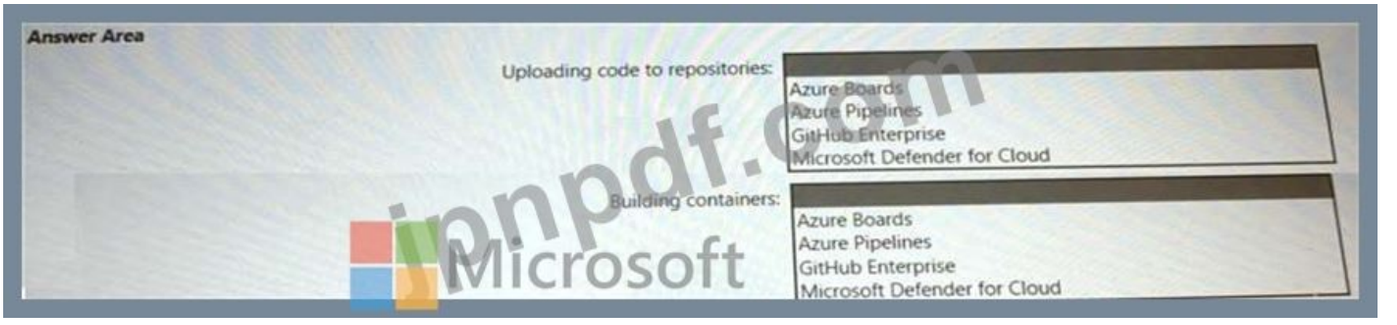
注: 正しく選択するたびに 1 ポイントの価値があります。



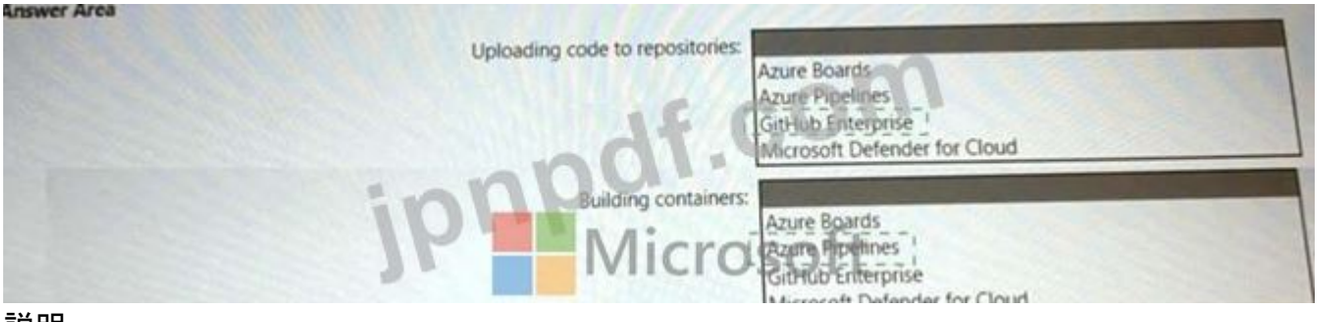
Answer:



最新問題: **44**
あなたの会社には、コンテナー化された Web アプリをデプロイするために使用される Azure App Service プランがあります。Web アプリを App Service プランにデプロイするための安全な DevOps 戦略を設計しています。コード スキャン ツールを安全なソフトウェア開発ライフサイクルに統合する戦略を推奨する必要があります。コードは次の 2 つのフェーズでスキャンする必要があります。
コードをリポジトリにアップロードする コンテナを構築する
各フェーズのコード スキャンをどこに統合する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。



Answer:



説明

https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec

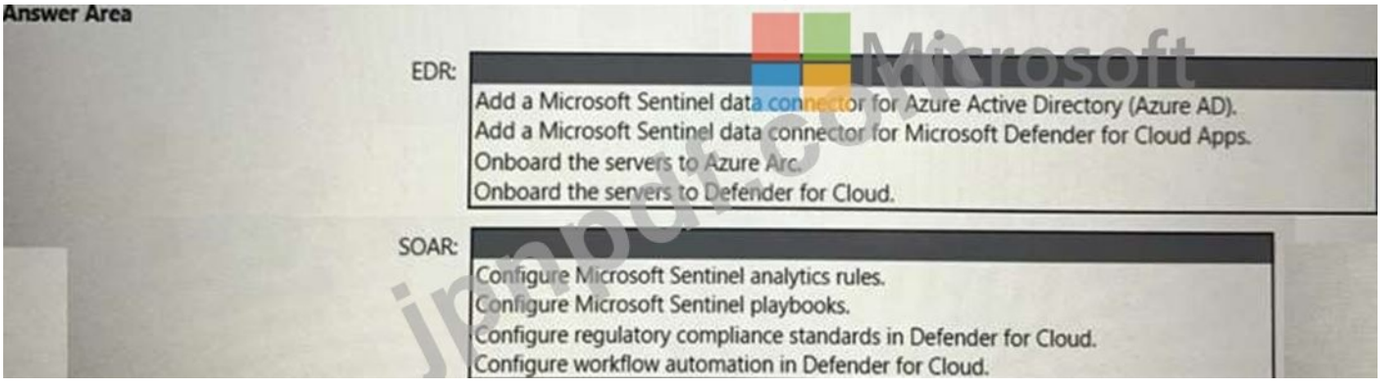
https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-contai

最新問題: **45**
Microsoft 365 E5 サブスクリプションをお持ちです。
機密データを含む電子メールの添付ファイルにウォーターマークを追加するソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. クラウド アプリ向け Microsoft Defender
B. アズール パービュー
C. インサイダーリスク管理
D. Microsoft 情報保護
Answer: (解答を表示する**)**

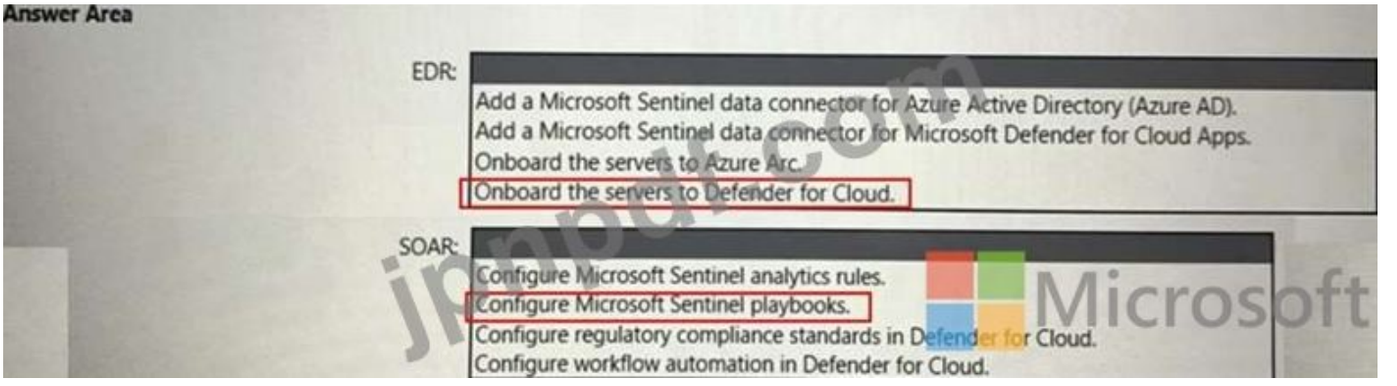
最新問題: **46**
あなたの会社は、Azure Active Directory (Azure AD) B2C を使用する請求書発行アプリケーションを開発しています。アプリケーションは App Service Web アプリとしてデプロイされます。ID 関連の攻撃からアプリケーションを保護するためのソリューションをアプリケーション開発チームに推奨する必要があります。どの 2 つの構成をお勧めしますか? それぞれの正解は、解決策の一部を示しています。注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure AD 条件付きアクセスとユーザー フローおよびカスタム ポリシーの統合
B. リスク検出を監視するための Azure AD ワークブック
C. Azure AD B2C のカスタム リソース所有者パスワード資格情報 (ROPC) フロー
D. Identity Governance のパッケージにアクセスします
E. Azure AD B2C のスマート アカウント ロックアウト
Answer: A,E (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

最新問題: **47**
Microsoft 365 サブスクリプションと Azure サブスクリプションをお持ちです。Microsoft 365 Defender と Microsoft Defender for Cloud が有効になっています。

Azure サブスクリプションには Microsoft Sentinel ワークスペースが含まれています。Microsoft Sentinel データ コネクタは、Microsoft 365、Microsoft 365 Defender、Defender for Cloud、および Azure 用に構成されています。
Windows Server を実行する Azure 仮想マシンをデプロイする予定です。
Microsoft Sentinel の拡張検出と応答 (EDR) およびセキュリティ オーケストレーション、自動化、および応答 (SOAR) 機能を有効にする必要があります。
各機能を有効にすることをどのように推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: **48**
あなたの会社は Microsoft 365 E5 ライセンスと Azure サブスクリプションを持っています。
同社は、次の場所に保存されている機密データに自動的にラベルを付けることを計画しています。
* Microsoft SharePoint Online
* Microsoft Exchange Online
*マイクロソフトチーム
機密データを特定して保護するための戦略を推奨する必要があります。
機密ラベル ポリシーにはどの範囲を推奨する必要がありますか? 答えるには、適切なスコープを正しい場所にドラッグします。各スコープは、1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題**: 49**

App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。

* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。

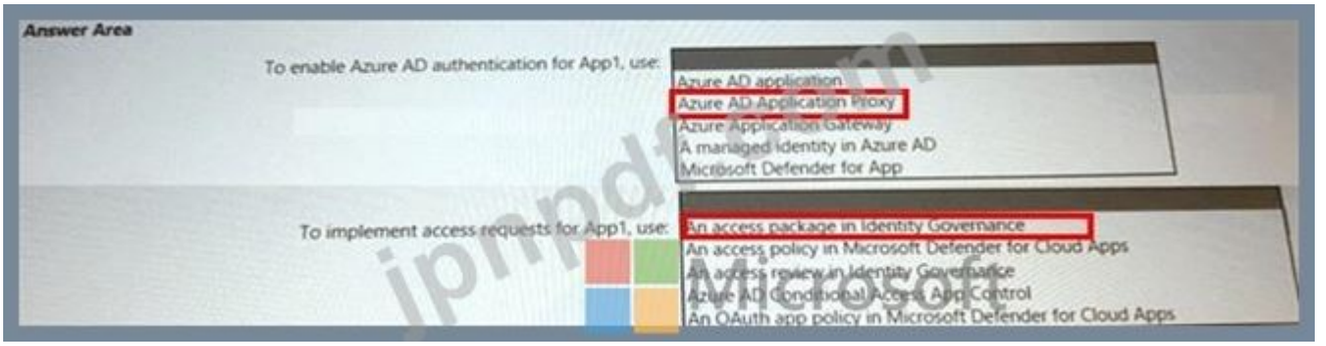
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。

App1 のアクセス セキュリティ アーキテクチャを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。

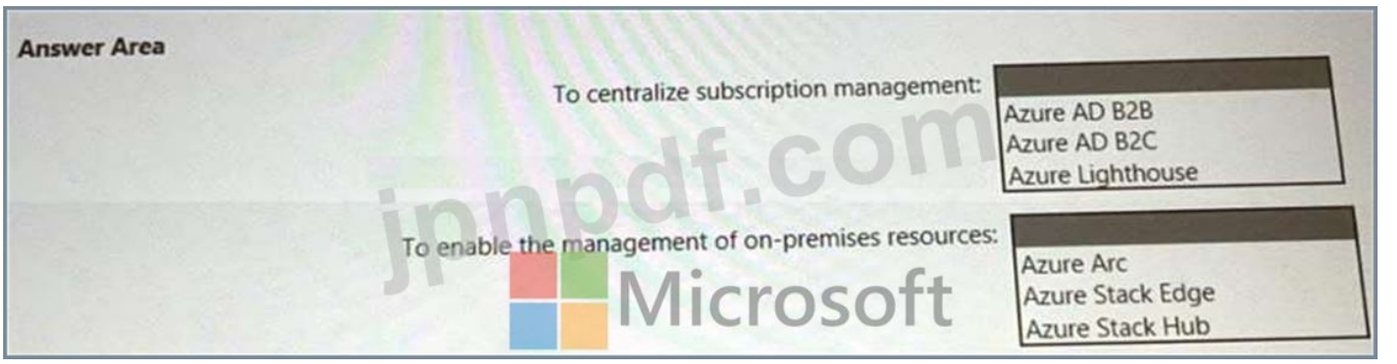
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題**: 50**

ビジネス要件とハイブリッド要件を満たすマルチテナントおよびハイブリッド セキュリティ ソリューションを推奨する必要があります。何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

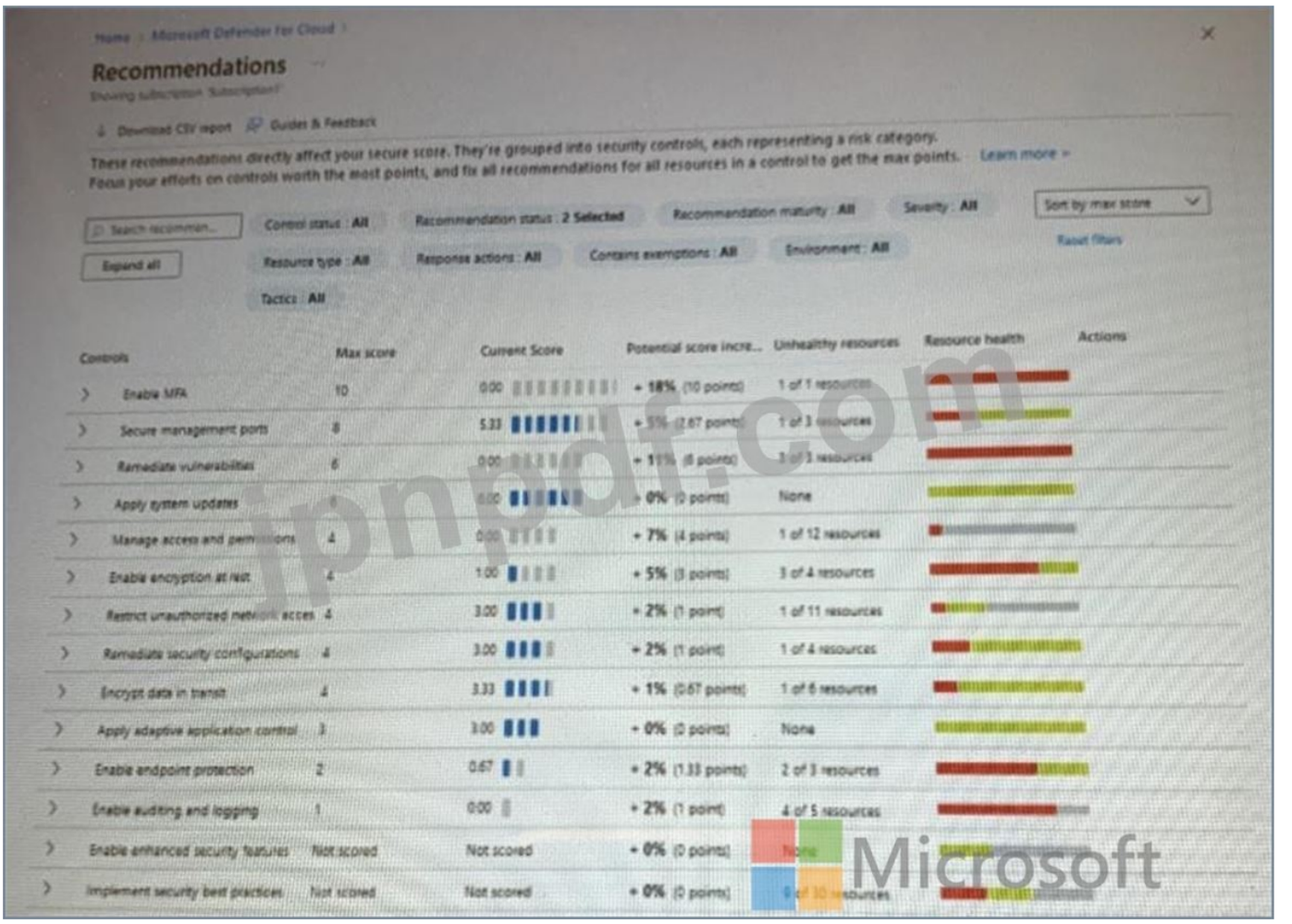
最新問題: **51**

litware.com フォレストを保護するための戦略を推奨する必要があります。ソリューションは ID 要件を満たしている必要があります。推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。ノート; 正しく選択するたびに 1 ポイントの価値があります。

Answer:

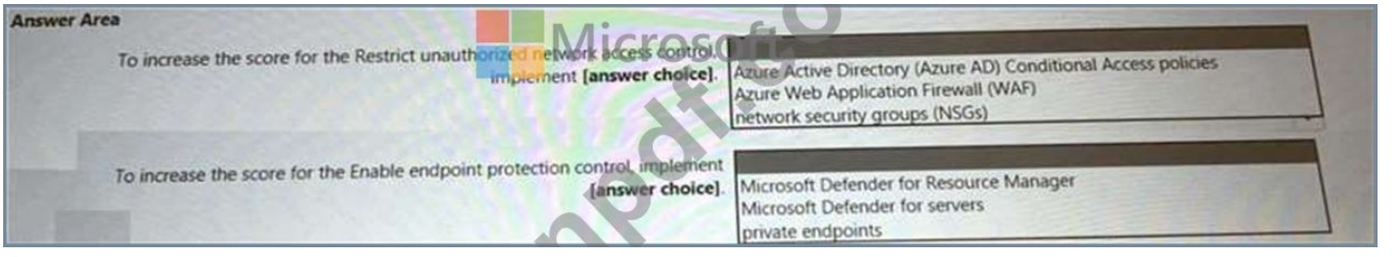
最新問題: **52**

次の図に示すように、Microsoft Defender for Cloud を開きます。



ドロップダウン メニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

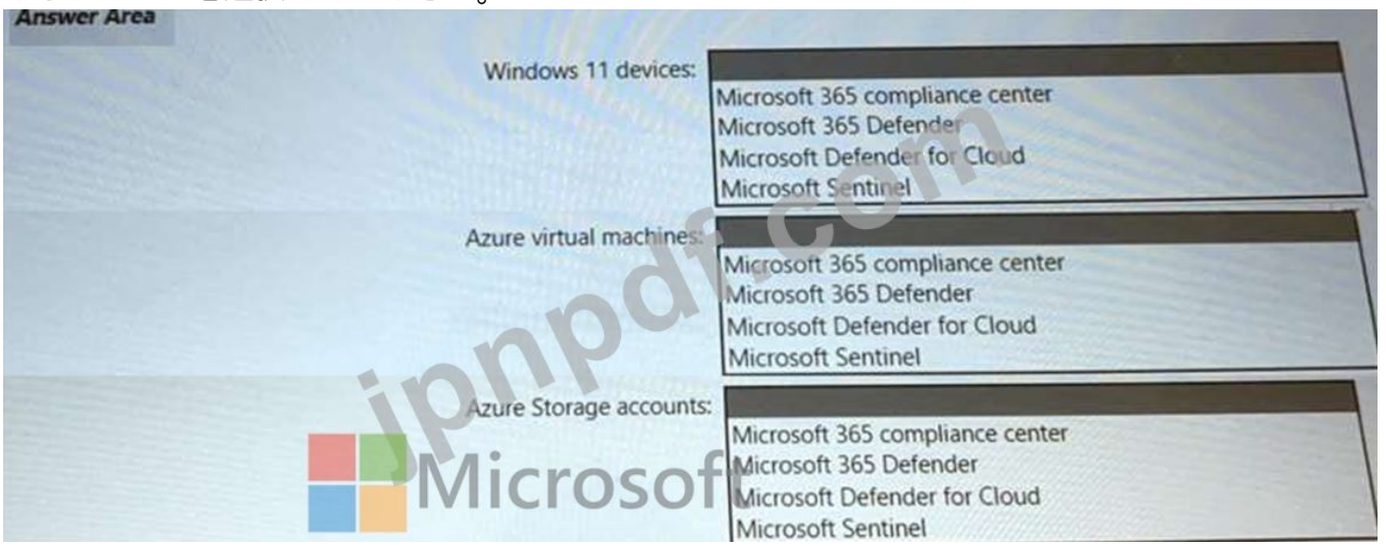
最新問題: **53**

Microsoft 365 E5 サブスクリプションと Azure サブスクリプトを持っている。次のコンポーネントの全体的なセキュリティ体制を強化するには、既存の環境を評価する必要があります。

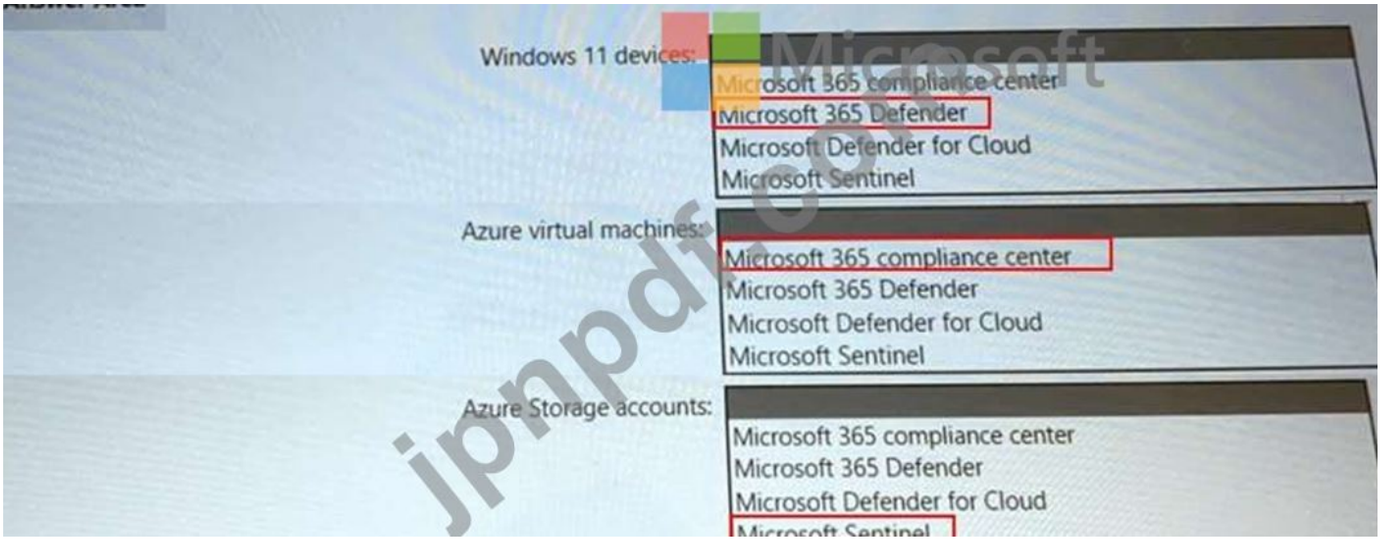
* Microsoft Intune によって管理される Windows 11 デバイス
* Azure ストレージ アカウント

* Azure仮想マシン

コンポーネントを評価するには何を使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。



Answer:



最新問題: **54**

あなたの会社には、オンプレミスの Active Directory ドメイン サービス (AD DS) フォレスト、Microsoft B65 サブスクリプション、および Azure サブスクリプションを含むハイブリッド クラウド インフラストラクチャがあります。

会社のオンプレミス ネットワークには、Kerberos 認証を使用する内部 Web アプリが含まれています。現在、Web アプリにはネットワークからのみアクセスできます。

Windows 11 を実行する個人用デバイスを持っているリモート ユーザーがいます。

リモート ユーザーが Web アプリにアクセスできるようにするソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。

* リモート ユーザーがネットワーク上の他のリソースにアクセスできないようにします。
* Azure Active Directory (Azure AD) 条件付きアクセスをサポートします。
* エンドユーザー エクスペリエンスを簡素化します。

推奨事項には何を含めるべきですか?

A. Azure AD アプリケーション プロキシ
B. Azure 仮想 WAN
C. Microsoft トンネル
D. Microsoft Defender for Endpoint の Web コンテンツ フィルター
Answer: A (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

最新問題**: 55**
あなたの会社にはハイブリッド クラウド インフラストラクチャがあります。
同社は短期間に数人の臨時従業員を雇用する予定だ。臨時従業員は、社内ネットワーク上のアプリケーションやデータにアクセスする必要があります。
会社のセキュリティ ポリシーにより、個人のデバイスを使用して会社のデータやアプリケーションにアクセスすることが禁止されています。
臨時従業員に会社のリソースへのアクセスを提供するソリューションを推奨する必要があります。ソリューションはオンデマンドで拡張できる必要があります。
推奨事項には何を含めるべきですか?
A. オンプレミス アプリケーションをクラウドベースのアプリケーションに移行します。
B. スプリット トンネル構成を採用して VPN インフラストラクチャを再設計します。
C. Microsoft エンドポイント マネージャーと Azure Active Directory (Azure AD) 条件付きアクセスをデプロイします。
D. Azure Virtual Desktop、Azure Active Directory (Azure AD) 条件付きアクセス、および Microsoft Defender for Cloud Apps を展開します。
Answer: D (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop
https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide
https://techcommunity.microsoft.com/t5/security-compliance-and-identity/payment-microsoft-defender-for-cl

最新問題**: 56**
アプリケーションのセキュリティ要件を満たすために、アプリケーションはどの 2 つの認証方法をサポートする必要がありますか? それぞれの正解は完全な解決策を示します。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. セキュリティ アサーション マークアップ言語 (SAML)
B. NTLMv2
C. 証明書ベースの認証
D. ケルベロス
Answer: A,D (メーッセージを残す**)**

説明
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain
トピック 2、Litware, Inc. ケーススタディ 2
概要
リトウェア株式会社 は、ニューヨークとサンフランシスコに主なオフィスを構える金融サービス会社です。リトウェアには
全米に 30 の支社とリモート従業員がいます。リモートの従業員は、VPN を使用してメイン オフィスに接続します。
Litware は、合併と買収により過去 2 年間で大幅に成長しました。買収にはフランスに拠点を置く数社が含まれる。
既存の環境
Litware には、Utvvare.com という名前の Active Directory Domain Services (AD D%) フォレストと同期する Azure Active Directory (Azure AD) テナントがあり、20 の Azure サブスクリプションにリンクされています。Azure AD Connect は、パススルー認証の実装に使用されます。パスワード ハッシュ同期は無効になり、パスワード ライトバックは有効になります。すべての Litware ユーザーは Microsoft 365 E5 ライセンスを持っています。
この環境には、いくつかの AD DS フォレスト、Azure AD テナント、および Litware の子会社に属する数百の Azure サブスクリプションも含まれています。
計画された変更
Litware は次の変更を実装する予定です。
* Azure AD テナントごとに管理グループ階層を作成します。
* Litware の既存の Azure 環境をリファクタリングし、将来のすべての Azure ワークロードをデプロイするためのランディング ゾーン戦略を設計します。
* Azure AD アプリケーション プロキシを実装して、現在 VPN を使用してアクセスされている内部アプリケーションへの安全なアクセスを提供します。
ビジネス要件
Litware は次のビジネス要件を特定します。
* 追加のオンプレミス インフラストラクチャを最小限に抑えます。
* 管理オーバーヘッドに関連する運用コストを最小限に抑えます。
ハイブリッドの要件
Litware では、次のハイブリッド クラウド要件を特定しています。
* Azure からの次のようなオンプレミス リソースの管理を有効にします。
*施行とコンプライアンスの評価には Azure Policy を使用します。
* 変更追跡と資産インベントリを提供します。
* パッチ管理を実装します。

* ゲスト アカウントの維持にかかるオーバーヘッドを発生させずに、一元的なテナント間サブスクリプション管理を提供します。
Microsoft Sentinelの要件
Litware は、Microsoft Sentinel のセキュリティ情報およびイベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAK) 機能を活用する予定です。同社は、Microsoft Sentinel を使用して Security Operations Center (SOQ) を一元化したいと考えています。
アイデンティティ要件
Litware は次の ID 要件を特定します。
* AD DS ユーザー アカウントを直接ターゲットとするブルート フォース攻撃を検出します。
* Litware の Azure AD テナントに漏洩した資格情報の検出を実装します。
* Azure AD ユーザー アカウントをターゲットとしたブルート フォース攻撃によって AD DS ユーザー アカウントがロックアウトされるのを防ぎます。
* Litware の Azure AD テナントにユーザーとグループの委任管理を実装します (サポートを含む)。
* グループのプロパティ、メンバーシップ、およびライセンスの管理 ユーザーのプロパティ、パスワード、およびライセンスの管理
* ビジネスユニットに基づいたユーザー管理の委任。
規制遵守要件
Litware では、次の規制遵守要件を特定しています。
* 米国およびフランスに拠点を置く各子会社が所有するログ、テレメトリ、およびデータを収集する際に、データ常駐に関するコンプライアンスを保証します。
* 組み込みの Azure Policy 定義を活用して、管理された環境全体にわたる法規制への準拠を評価します。
* 最小特権の原則を使用します。
Azure ランディング ゾーンの要件
Litware は、次のランディング ゾーン要件を特定します。
* インターネットに向かうすべてのトラフィックを、専用の Azure サブスクリプションの Azure Firewall 経由でランディング ゾーンからルーティングします。
* ランディング ゾーンを対象とした安全なスコアを提供します。
* 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信していることを確認します。
* データ漏洩の可能性を最小限に抑えます。
* ネットワーク帯域幅を最大化します。
ランディング ゾーン アーキテクチャには、インターネットおよびハイブリッド接続のハブとして機能する専用のサブスクリプションが含まれます。各ランディング ゾーンには次の特徴があります。
* 専用のサブスクリプションで作成されます。
* litware.com の DNS 名前空間を使用します。

アプリケーションのセキュリティ要件
Litware は、次のアプリケーションのセキュリティ要件を特定します。
* Azure AD アプリケーション プロキシを使用してシングル サインオン (SSO) をサポートする内部アプリケーションを特定します。
* Microsoft SharePoint Online および Exchange Online データへのアクセスをリアルタイムで監視および制御します。

最新問題: **57**
Microsoft 365 サブスクリプションをお持ちです
次のアクティビティを監視するには、セキュリティ ソリューションを推奨する必要があります。
* 侵害された可能性のあるユーザー アカウント
* Microsoft SharePoint Online からファイルの一括ダウンロードを実行するユーザー 各アクティビティの推奨事項には何を含める必要がありますか? 答えるには、適切なコンポーネントを正しいアクティビティにドラッグします。各コンポーネントは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 各正解の選択は 1 ポイントの価値があります。

Answer:

最新問題: **58**
50 個の Azure サブスクリプションがあります。
ISO 27001:2013 標準に準拠しているかどうか、サブスクリプション内のリソースを監視する必要があります。このソリューションでは、サブスクリプションの監視対象ポリシー定義のリストを変更するために必要な労力を最小限に抑える必要があります。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. イニシアチブを管理グループに割り当てます。
B. 各サブスクリプションにブループリントを割り当てます。
C. 各サブスクリプションにポリシーを割り当てます。
D. ブループリントを管理グループに割り当てます。

E. 各サブスクリプションにイニシアチブを割り当てます。
F. ポリシーを管理グループに割り当てます。
Answer: D,F (メーッセージを残す**)**
トピック 1、Litware, Inc. ケーススタディ
概要
リトウェア株式会社 は、ニューヨークとサンフランシスコに主なオフィスを構える金融サービス会社です。リトウェアには
全米に 30 の支社とリモート従業員がいます。リモートの従業員は、VPN を使用してメイン オフィスに接続します。
Litware は、合併と買収により過去 2 年間で大幅に成長しました。買収にはフランスに拠点を置く数社が含まれる。
既存の環境
Litware には、Utvvare.com という名前の Active Directory Domain Services (AD D%) フォレストと同期する Azure Active Directory (Azure AD) テナントがあり、20 の Azure サブスクリプションにリンクされています。Azure AD Connect は、パススルー認証の実装に使用されます。パスワード ハッシュ同期は無効になり、パスワード ライトバックは有効になります。すべての Litware ユーザーは Microsoft 365 E5 ライセンスを持っています。
この環境には、いくつかの AD DS フォレスト、Azure AD テナント、および Litware の子会社に属する数百の Azure サブスクリプションも含まれています。
計画された変更
Litware は次の変更を実装する予定です。
* Azure AD テナントごとに管理グループ階層を作成します。
* Litware の既存の Azure 環境をリファクタリングし、将来のすべての Azure ワークロードをデプロイするためのランディング ゾーン戦略を設計します。
* Azure AD アプリケーション プロキシを実装して、現在 VPN を使用してアクセスされている内部アプリケーションへの安全なアクセスを提供します。
ビジネス要件
Litware は次のビジネス要件を特定します。
* 追加のオンプレミス インフラストラクチャを最小限に抑えます。
* 管理オーバーヘッドに関連する運用コストを最小限に抑えます。
ハイブリッドの要件
Litware では、次のハイブリッド クラウド要件を特定しています。
* Azure からの次のようなオンプレミス リソースの管理を有効にします。
*施行とコンプライアンスの評価には Azure Policy を使用します。
* 変更追跡と資産インベントリを提供します。
* パッチ管理を実装します。
* ゲスト アカウントの維持にかかるオーバーヘッドを発生させずに、一元的なテナント間サブスクリプション管理を提供します。
Microsoft Sentinelの要件

Litware は、Microsoft Sentinel のセキュリティ情報およびイベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAK) 機能を活用する予定です。同社は、Microsoft Sentinel を使用して Security Operations Center (SOQ) を一元化したいと考えています。

アイデンティティ要件

Litware は次の ID 要件を特定します。

* AD DS ユーザー アカウントを直接ターゲットとするブルート フォース攻撃を検出します。
* Litware の Azure AD テナントに漏洩した資格情報の検出を実装します。
* Azure AD ユーザー アカウントをターゲットとしたブルート フォース攻撃によって AD DS ユーザー アカウントがロックアウトされるのを防ぎます。
* Litware の Azure AD テナントにユーザーとグループの委任管理を実装します (サポートを含む)。
* グループのプロパティ、メンバーシップ、およびライセンスの管理
* ユーザーのプロパティの管理、
パスワードとライセンス
* ビジネスユニットに基づいたユーザー管理の委任。

規制遵守要件

Litware では、次の規制遵守要件を特定しています。

* 米国およびフランスに拠点を置く各子会社が所有するログ、テレメトリ、およびデータを収集する際に、データ常駐に関するコンプライアンスを保証します。
* 組み込みの Azure Policy 定義を活用して、管理された環境全体にわたる法規制への準拠を評価します。
* 最小特権の原則を使用します。

Azure ランディング ゾーンの要件

Litware は、次のランディング ゾーン要件を特定します。

* インターネットに向かうすべてのトラフィックを、専用の Azure サブスクリプションの Azure Firewall 経由でランディング ゾーンからルーティングします。
* ランディング ゾーンを対象とした安全なスコアを提供します。
* 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信していることを確認します。
* データ漏洩の可能性を最小限に抑えます。
* ネットワーク帯域幅を最大化します。

ランディング ゾーン アーキテクチャには、インターネットおよびハイブリッド接続のハブとして機能する専用のサブスクリプションが含まれます。各ランディング ゾーンには次の特徴があります。

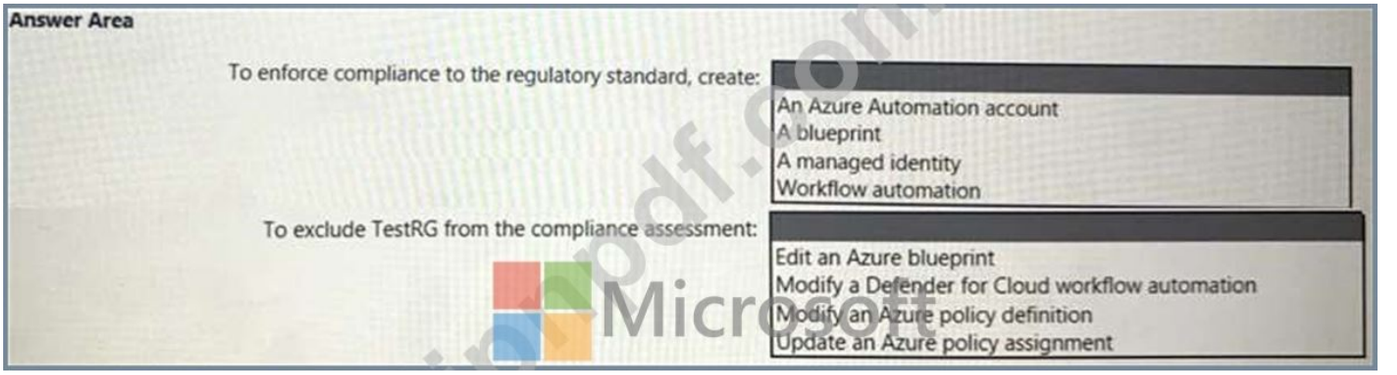
* 専用のサブスクリプションで作成されます。
* litware.com の DNS 名前空間を使用します。

アプリケーションのセキュリティ要件

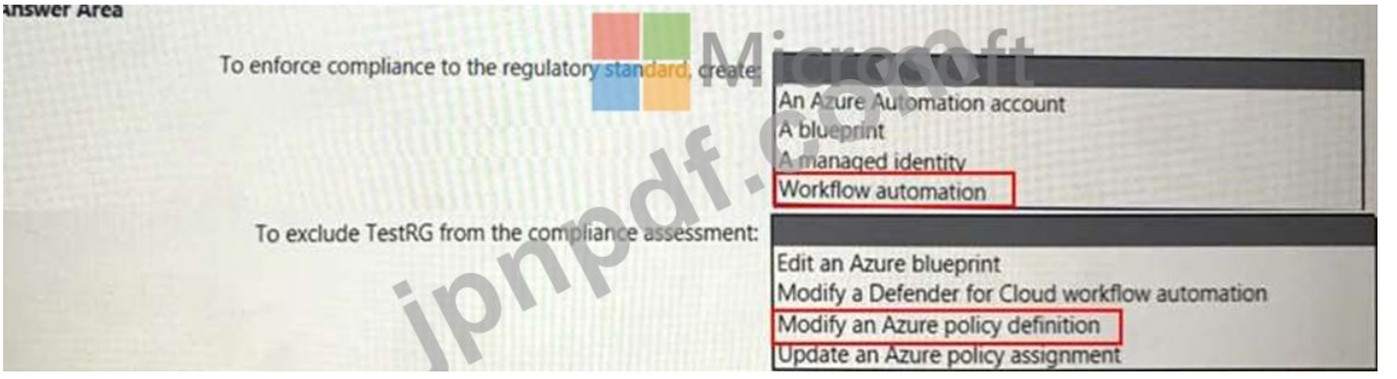
Litware は、次のアプリケーションのセキュリティ要件を特定します。

* Azure AD アプリケーション プロキシを使用してシングル サインオン (SSO) をサポートする内部アプリケーションを特定します。
* Microsoft SharePoint Online および Exchange Online データへのアクセスをリアルタイムで監視および制御します。

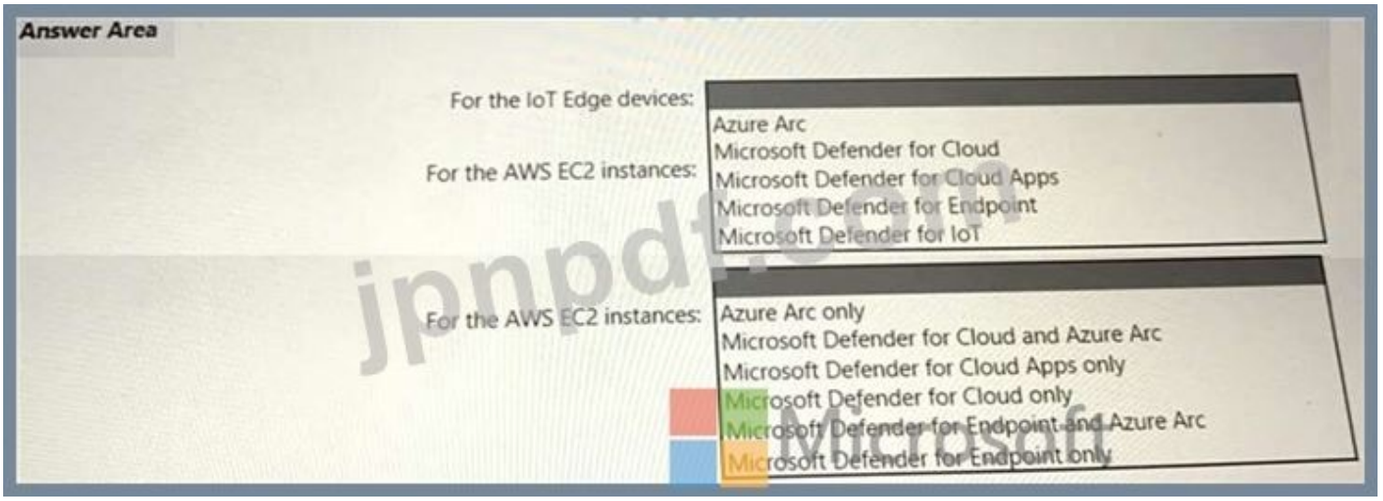
最新問題: **59**
コンプライアンス要件を満たすソリューションを推奨する必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



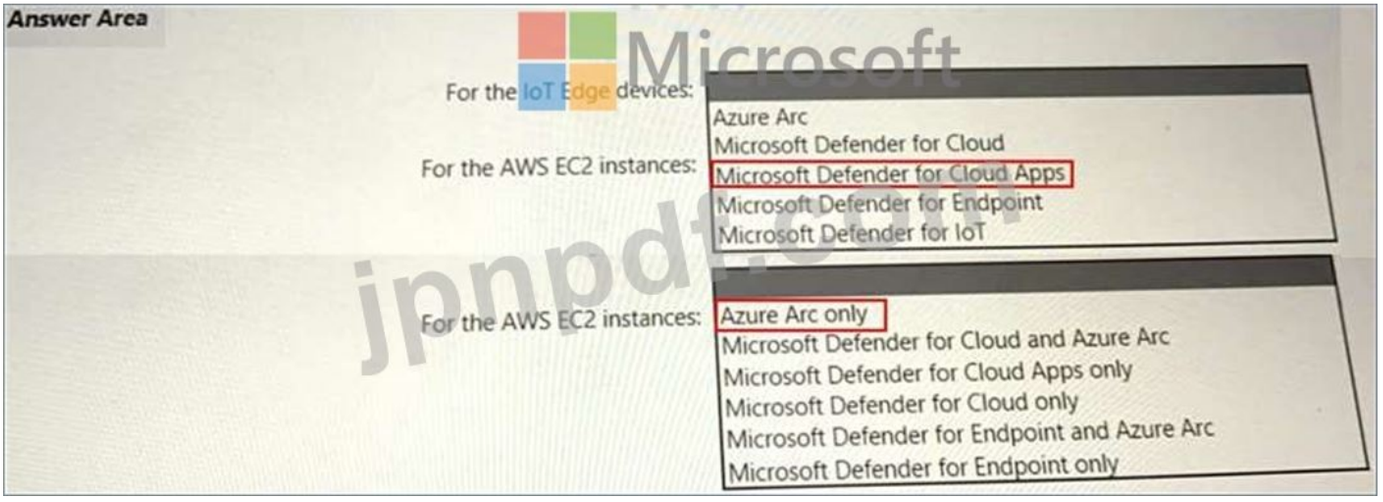
Answer:



最新問題: **60**
あなたの会社には、Microsoft 365 サブスクリプション、Azure サブスクリプション、アマゾン ウェブ サービス (AWS) 実装を含むマルチクラウド環境があります。次のコンポーネントに対してセキュリティ体制管理ソリューションを推奨する必要があります。
* Azure LOT Edge デバイス
* AWS EC2 インスタンス
どのサービスを推奨事項に含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



トピック 2、Fabrikam, Inc

オンプレミス環境

オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

Azure環境

Fabrikam には次の Azure リソースがあります。

* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnetl という名前の仮想ネットワーク
* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ

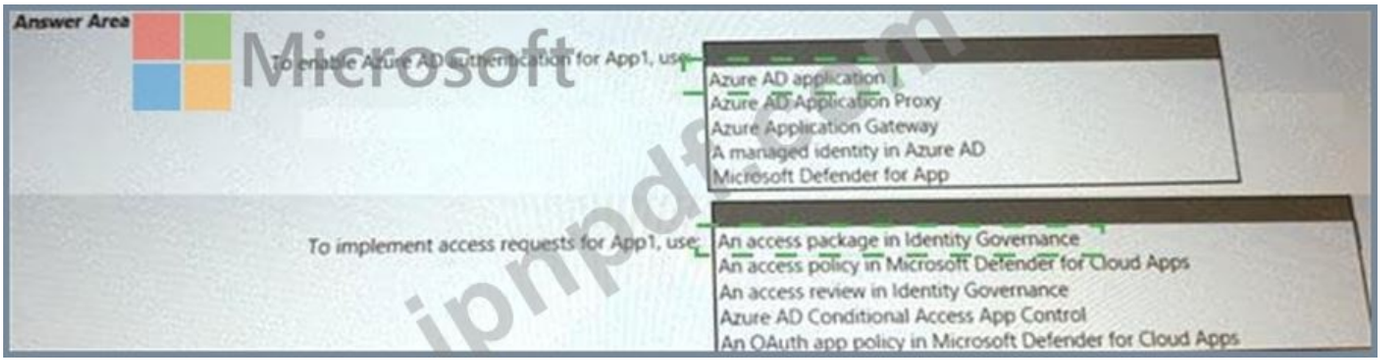
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。
パートナー
Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続します。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。
ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。
コンプライアンスイベント
Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修正されています。
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。
アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。

* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。
* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題**: 61**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャを推奨する必要があります。

推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



説明
ボックス 1 は Azure AD アプリケーションです
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app ボックス 2 は、Identity Governance の Access パッケージです。
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cre

最新問題**: 62**
SharePoint Online と Exchange Online のデータを保護するための戦略を設計する必要があります。ソリューションはアプリケーションのセキュリティ要件を満たしている必要があります。
戦略で活用すべき 2 つのサービスはどれですか? それぞれの正解は、解決策の一部を示しています。
ノート; 正しく選択するたびに 1 ポイントの価値があります。
A. クラウド用 Microsoft Defender
B. Azure AD でのアクセスレビュー

C. エンドポイント用 Microsoft Defender
D. クラウド アプリ向け Microsoft Defender
E. Azure AD 条件付きアクセス
Answer: B,D (メーッセージを残す)

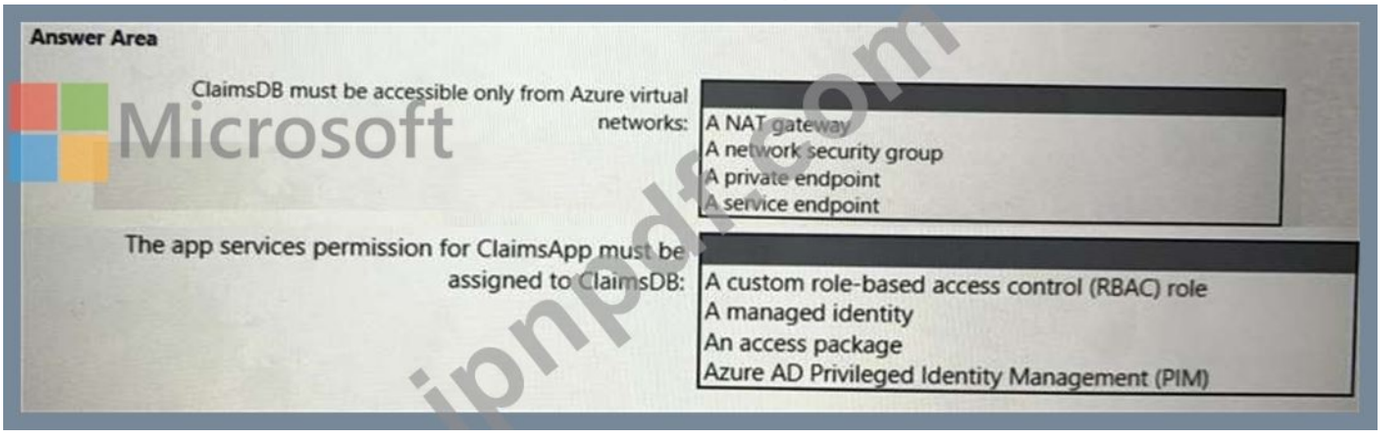
最新問題: **63**
Azure Pipelines と Azure Repos を使用して、継続的インテグレーションと継続的デプロイ (CI/CO) ワークフローを実装します。
Microsoft Cloud Adoption Framework for Azure に基づいて、CI/CD ワークフローの段階を保護するためのベスト プラクティスを推奨する必要があります。
各段階の推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

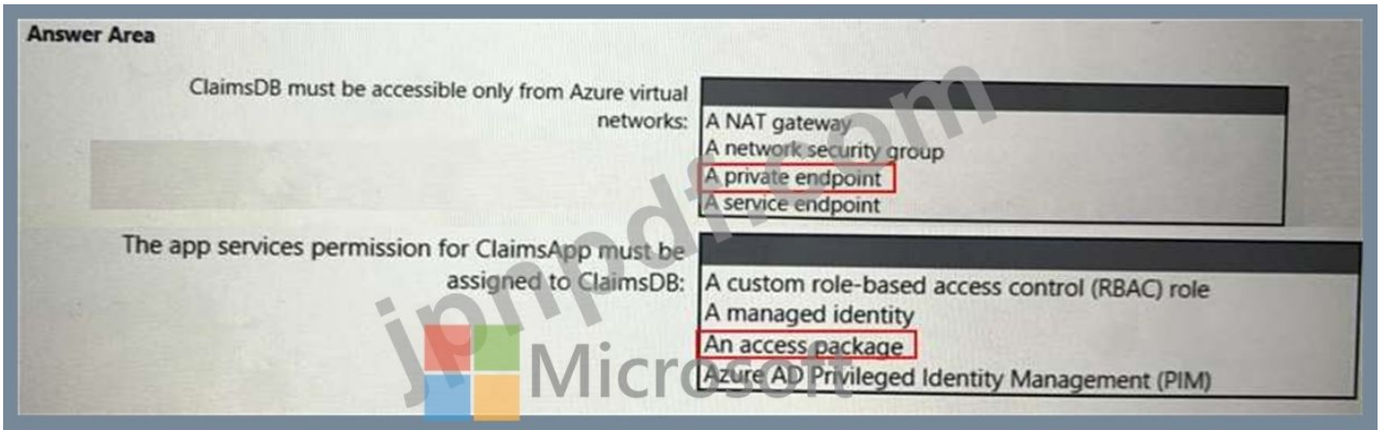
最新問題: **64**
ランディング ゾーンを保護するためのソリューションを推奨する必要があります。ソリューションは、ランディング ゾーンの要件とビジネス要件を満たしている必要があります。
各ランディング ゾーンには何を構成する必要がありますか?
A. Azure DDoS 保護標準
B. Azure プライベート DNS ゾーン
C. クラウド用 Microsoft Defender
D. ExpressRoute ゲートウェイ
Answer: B (メーッセージを残す)
説明
条件の 1 つは、コストを最小限に抑えるというビジネス要件を満たすことです。ExpressRoute は高価です。

ランディングゾーンの要件を考慮すると、
1) 「itware.com の DNS 名前空間を使用する」
2) 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信することを確認します。」

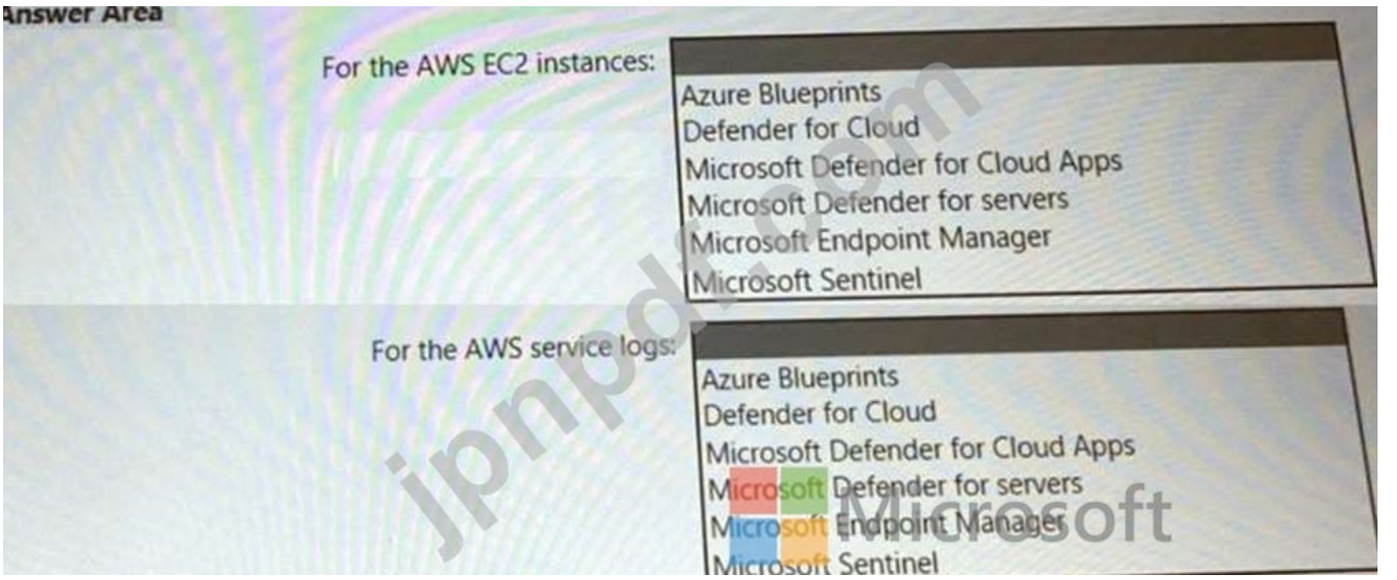
最新問題: **65**
ClaimsDB への接続要件を満たすソリューションを推奨する必要があります。
それぞれの要件に対して何を使用することを推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



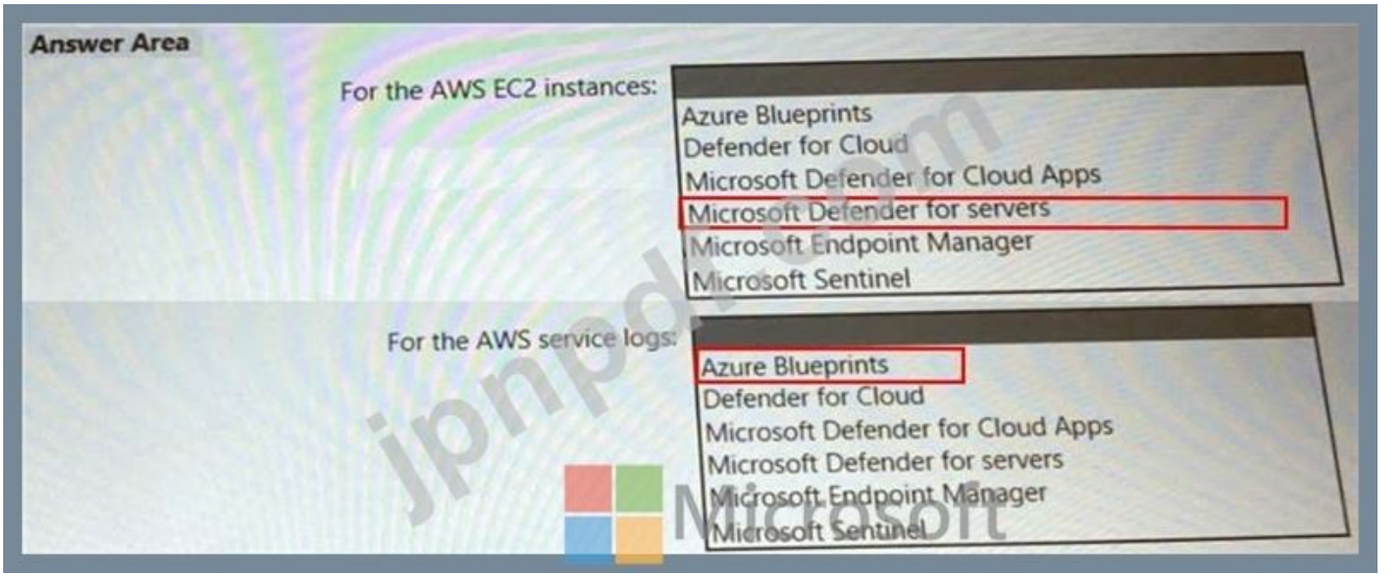
Answer:



最新問題: **66**
AWS の要件を満たすソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 67**

ClaimsApp のセキュリティを評価しています。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

ノート; 正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題: **68**
Microsoft 365 サブスクリプションと Azure サブスクリプションを持つ顧客がいます。
顧客は、Windows、iOS、Android、または macOS のいずれかを実行するデバイスを持っています。Windows デバイスはオンプレミスと Azure にデプロイされます。
すべてのデバイスが顧客のコンプライアンス ルールを満たしているかどうかを評価するセキュリティ ソリューションを設計する必要があります。
ソリューションには何を含めるべきでしょうか?
A. Microsoft 情報保護
B. エンドポイント用 Microsoft Defender
C. マイクロソフト センチネル
D. Microsoft エンドポイント マネージャー
Answer: D (メーッセージを残す**)**
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

最新問題: **69**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。
Azure セキュリティ ベンチマーク V3 レポートを評価しています。
安全な管理ポート制御では、潜在的な 8 ポイントのうち 0 ポイントを持っていることがわかります。
安全な管理ポート制御のスコアを向上させる構成を推奨する必要があります。
解決策: すべての仮想マシンで VMAccess 拡張機能を有効にすることをお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**

https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions アダプティブネットワークの強化: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration

トピック 2、Fabrikam, Inc

オンプレミス環境

オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

Azure環境

Fabrikam には次の Azure リソースがあります。

* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnet1 という名前の仮想ネットワーク
* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。

パートナー

Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。

* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続します。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。

ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。

コンプライアンスイベント

Fabrikam は次のコンプライアンス環境を展開します。

* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修正されています。

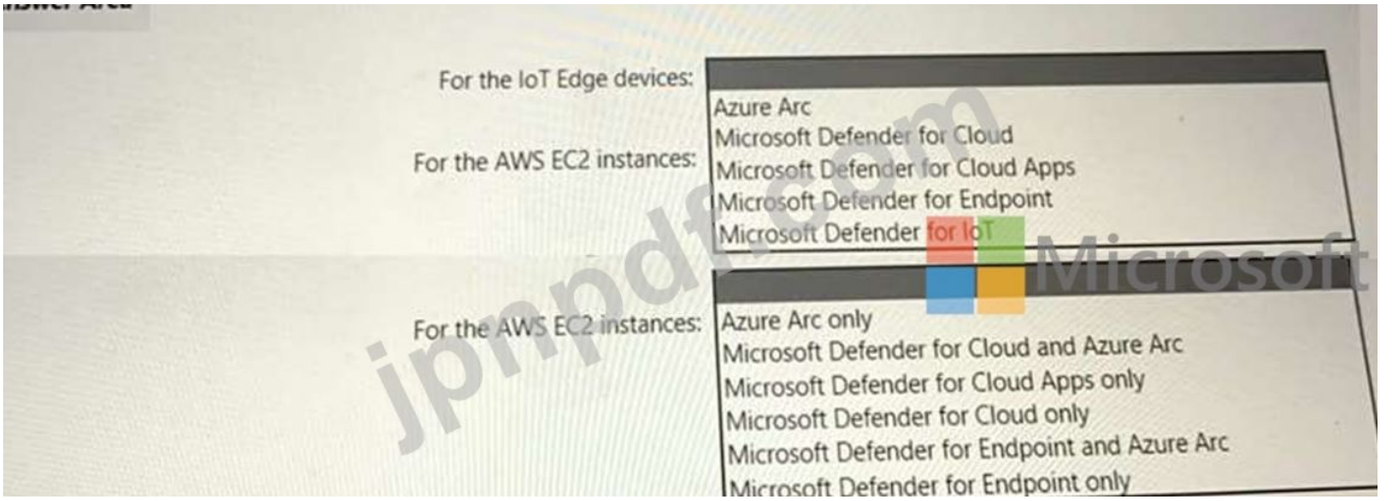
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。
アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。
* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件

Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

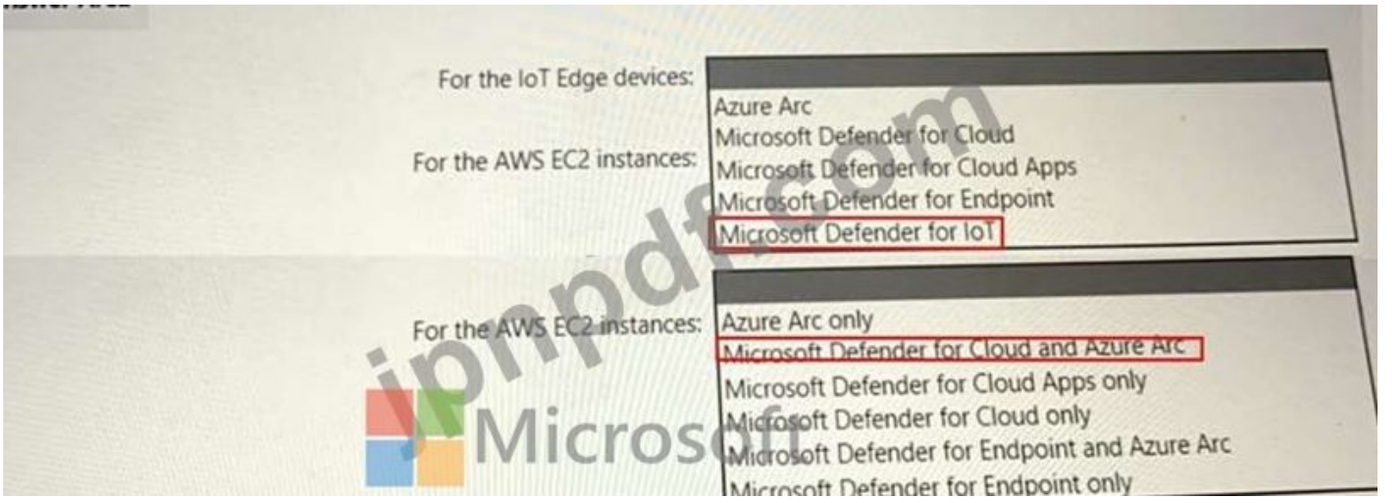
最新問題: **70**
オンプレミス ネットワークには、Angular と Node.js で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行する予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。

Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロトラスト モデルに従う必要があります。解決策: Azure Web アプリケーション ファイアウォール (WAF) を使用して Azure Front Door を実装することをお勧めします。これは目標を達成していますか?
A. いいえ
B. はい
Answer: B (メーッセージを残す**)**

最新問題: **71**
あなたの会社には、Microsoft 365 サブスクリプション、Azure サブスクリプション、アマゾン ウェブ サービス (AWS) 実装を含むマルチクラウド環境があります。次のコンポーネントに対してセキュリティ体制管理ソリューションを推奨する必要があります。
* Azure LOT Edge デバイス
* AWS EC2 インスタンス
どのサービスを推奨事項に含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 72**

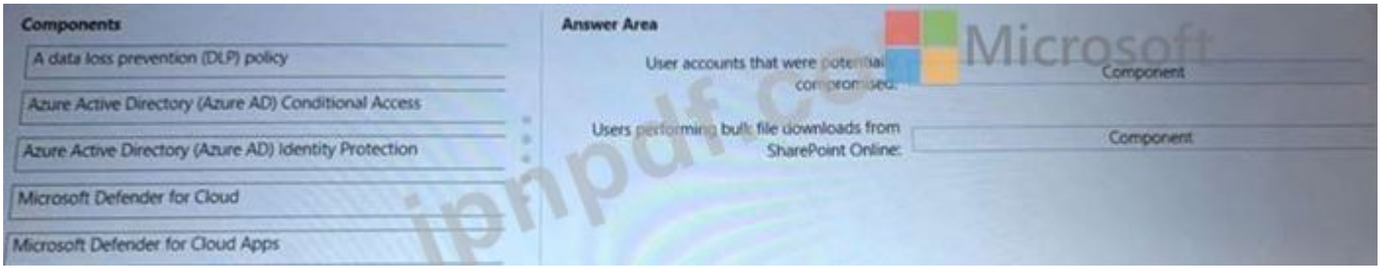
Microsoft 365 サブスクリプションをお持ちです

次のアクティビティを監視するには、セキュリティ ソリューションを推奨する必要があります。

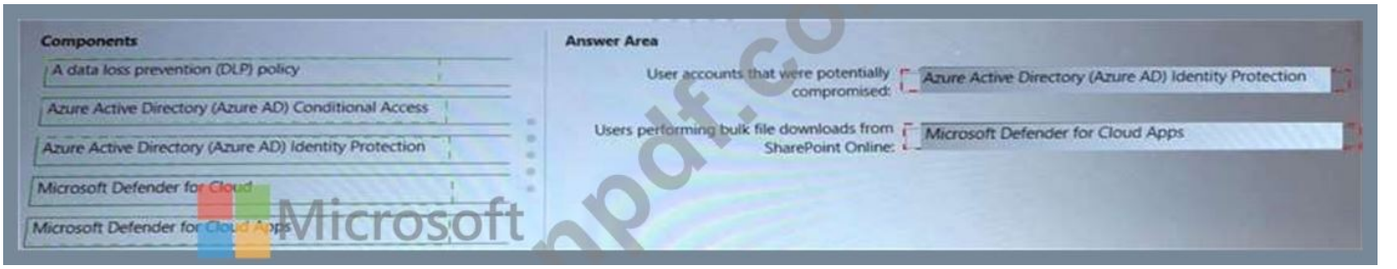
* 侵害された可能性のあるユーザー アカウント

* Microsoft SharePoint Online からファイルの一括ダウンロードを実行するユーザー 各アクティビティの推奨事項には何を含める必要がありますか? 答えるには、適切なコンポーネントを正しいアクティビティにドラッグします。各コンポーネントは 1 回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 各正解の選択は 1 ポイントの価値があります。



Answer:



最新問題: **73**

あなたの会社は、リソースをランサムウェアから保護するために Azure の使用を最適化したいと考えています。

Azure Backup と Azure Storage のどの機能がランサムウェア攻撃に対して最も強力な保護を提供するかを推奨する必要があります。ソリューションは Microsoft セキュリティのベスト プラクティスに従う必要があります。

何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題: **74**

仮想マシンのセキュリティ要件を満たすソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?

A. Azure Bastion ホスト

B. ネットワーク セキュリティ グループ (NSG)

C. ジャストインタイム (JIT) VM アクセス

D. Azure 仮想デスクトップ

Answer: D (メーッセージを残す)

説明

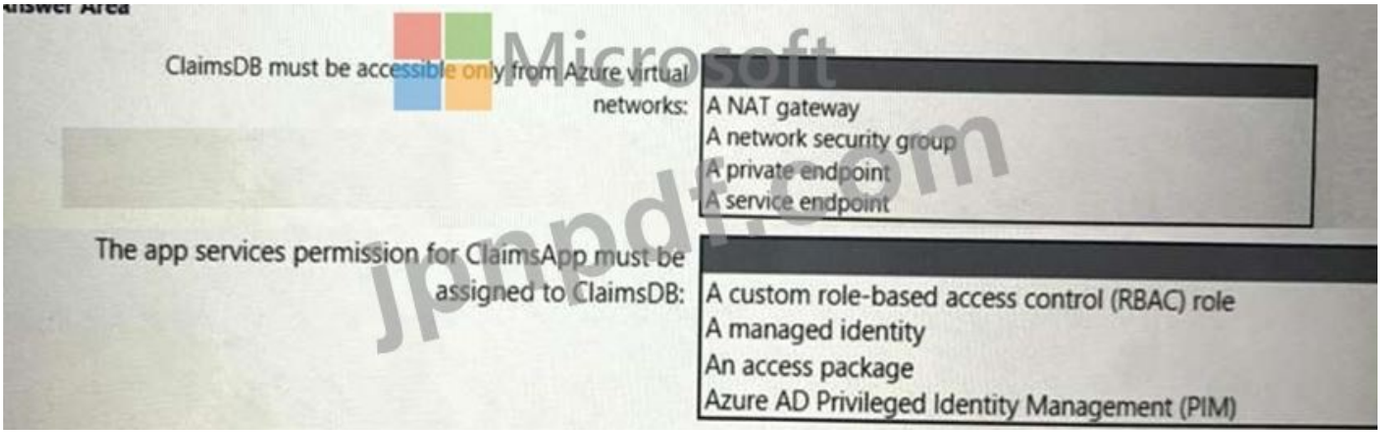
この質問で満たす必要があるセキュリティ要件は、セキュア ホストはカスタム オペレーティング システム イメージからプロビジョニングされる必要がある」です。https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image

最新問題: **75**
セキュリティ アクセス戦略のセキュリティ レベルを計画しています。
どのジョブの役割をどのセキュリティ レベルで構成するかを特定する必要があります。ソリューションは、Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。
各職務にどのセキュリティ レベルを設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

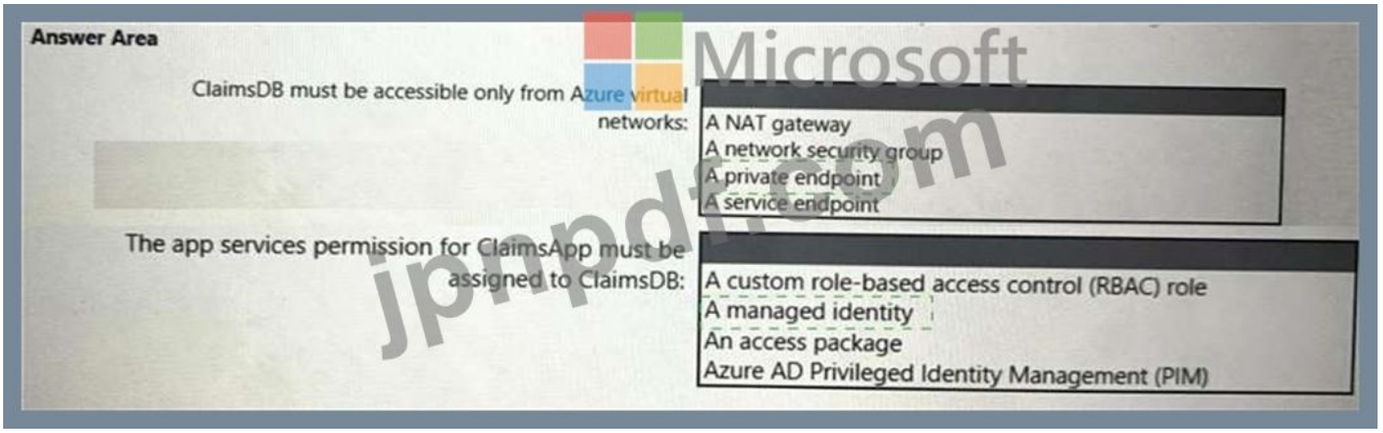
Answer:

最新問題: **76**
ClaimsDB への接続要件を満たすソリューションを推奨する必要があります。
それぞれの要件に対して何を使用することを推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

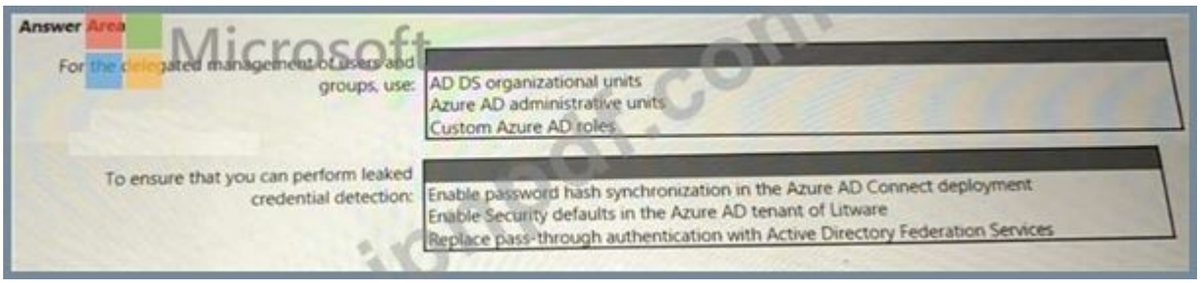


最新問題: **77**

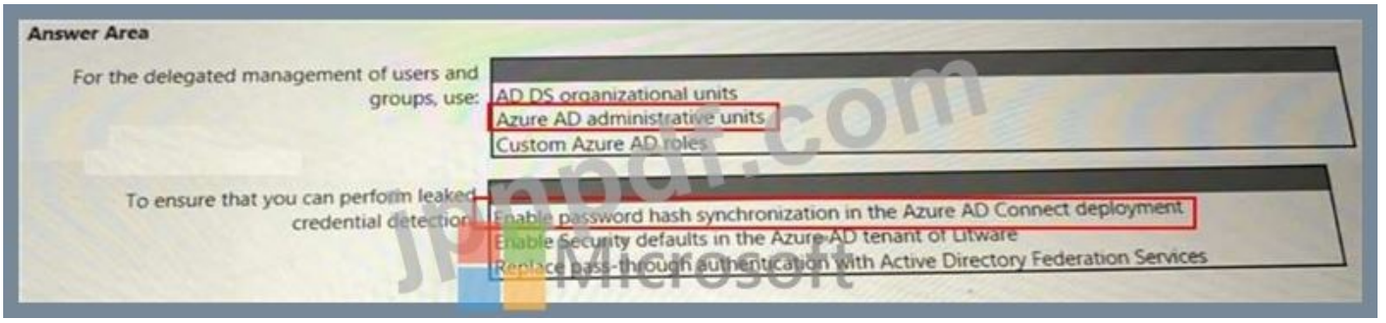
Litware の Azure AD テナントに ID セキュリティ ソリューションを推奨する必要があります。ソリューションは、ID 要件と法規制遵守要件を満たしている必要があります。

何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

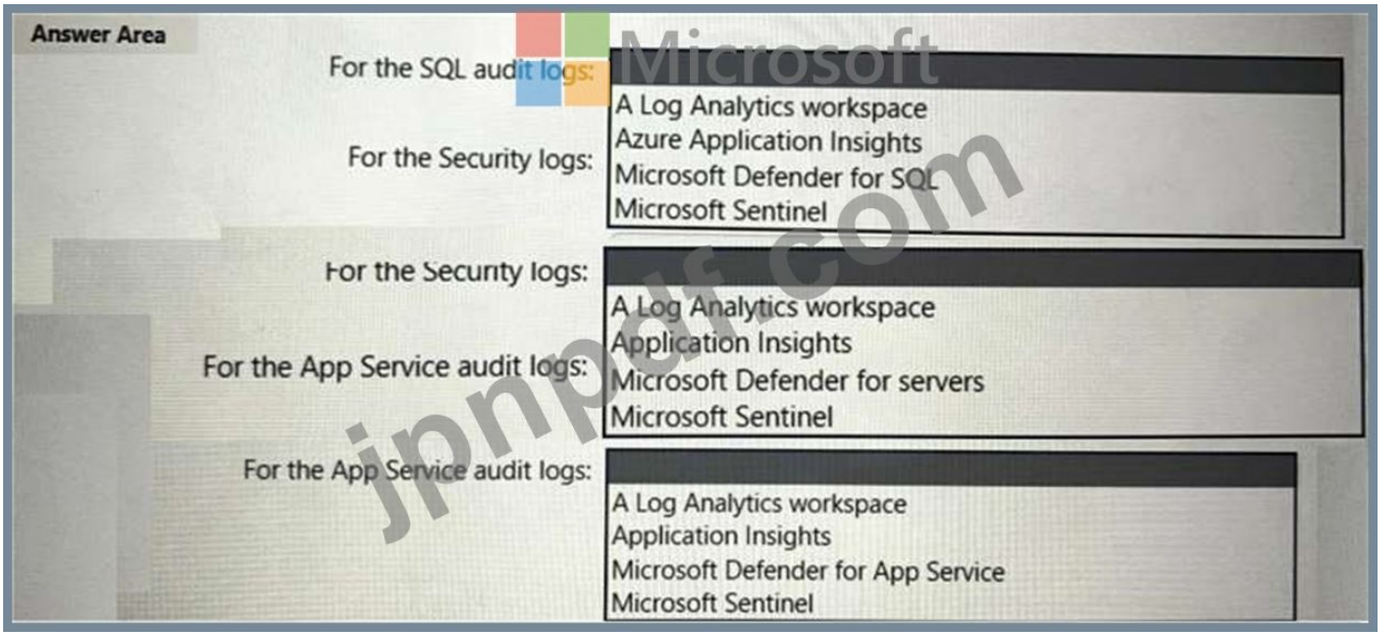


Answer:



最新問題: **78**
あなたの会社には、Microsoft Defender for Cloud のセキュリティが強化された Azure サブスクリプションがあります。
同社は米国政府と契約を締結しました。
NIST 800-53 に準拠するために現在のサブスクリプションを確認する必要があります。
まず何をすべきでしょうか?
A. Defender for Cloud から、セキュリティ スコアの推奨事項を確認します。
B. Microsoft Sentinel から、Microsoft Defender for Cloud データ コネクタを構成します。
C. Defender for Cloud から、監査レポートの Azure セキュリティ ベースラインを確認します。
D. Defender for Cloud から、規制遵守標準を追加します。
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulatory-compliance-standards-are-available-in-defender-for-cloud

最新問題: **79**
次のコンポーネントを含む Azure ランディング ゾーンの監査ソリューションを設計しています。
* Azure SQL データベースの SQL 監査ログ
* Azure 仮想マシンからの Windows セキュリティ ログ
* App Service Web アプリからの Azure App Service 監査ログ
ランディング ゾーンに対して集中ログ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* すべての特権アクセスをログに記録します。
* ログは少なくとも 365 日間保持します。
*コストを最小限に抑えます。
推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

最新問題**: 80**

顧客は、4 つの Azure サブスクリプションにわたる 10 の Azure Kubernetes Service (AKS) リソースに Docker イメージをデプロイしています。あなたは顧客のセキュリティ体制を評価しています。

AKS リソースがセキュリティ スコアの推奨事項から除外されていることがわかります。正確な推奨事項を作成し、安全なスコアを更新する必要があります。

Microsoft Defender for Cloud で推奨すべき 2 つのアクションはどれですか? それぞれの正解は、解決策の一部を示しています。注: 正しく選択するたびに 1 ポイントの価値があります。

A. 自動プロビジョニングを構成します。

B. 法規制順守ポリシーを割り当てます。

C. 在庫を確認します。

D. ワークフローの自動化を追加します。

E. Defender プランを有効にします。

Answer: A,E (メーッセージを残す**)**

説明

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages

https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

最新問題**: 81**

あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。

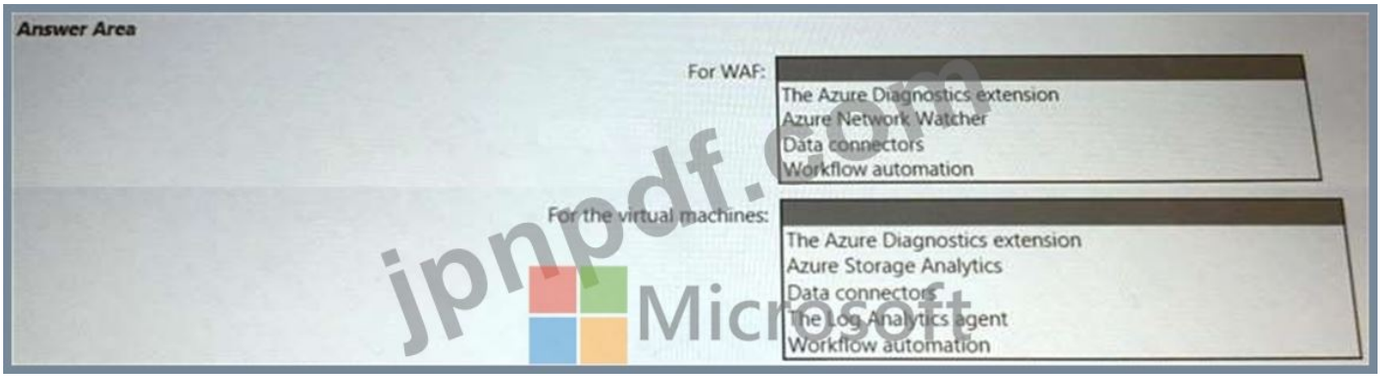
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。

* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。

* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。

ソリューションには何を含めるべきでしょうか? 回答するには、回答領域で適切なオプションを選択してください。ノート：

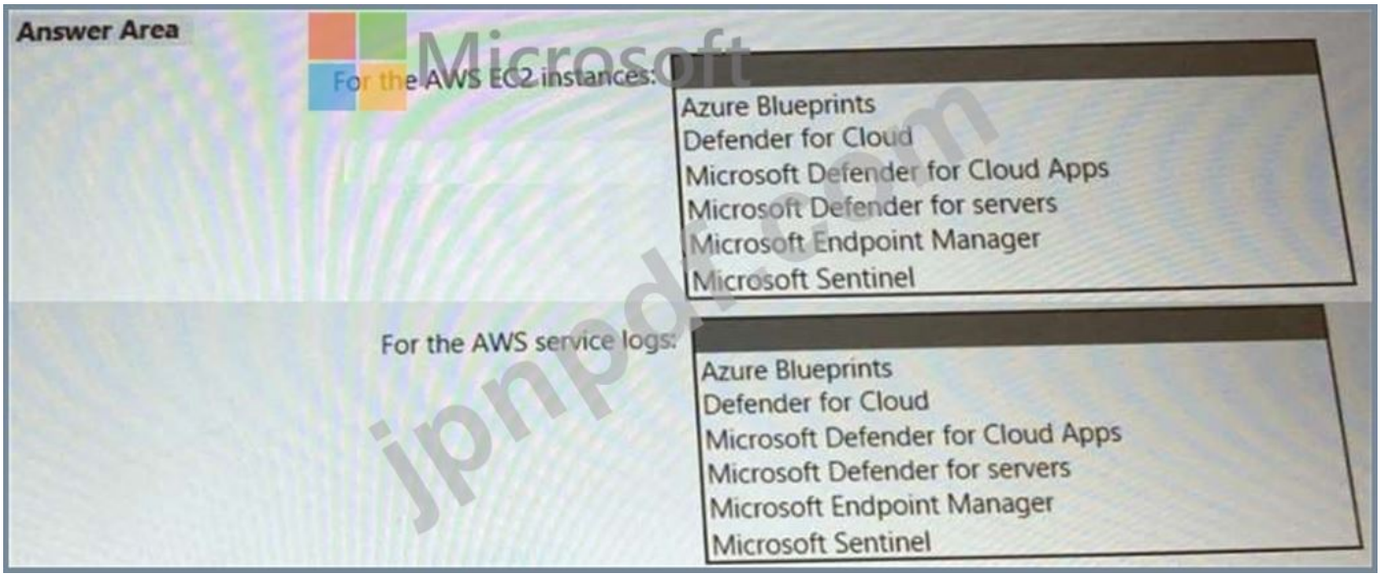
正しく選択するたびに 1 ポイントの価値があります。



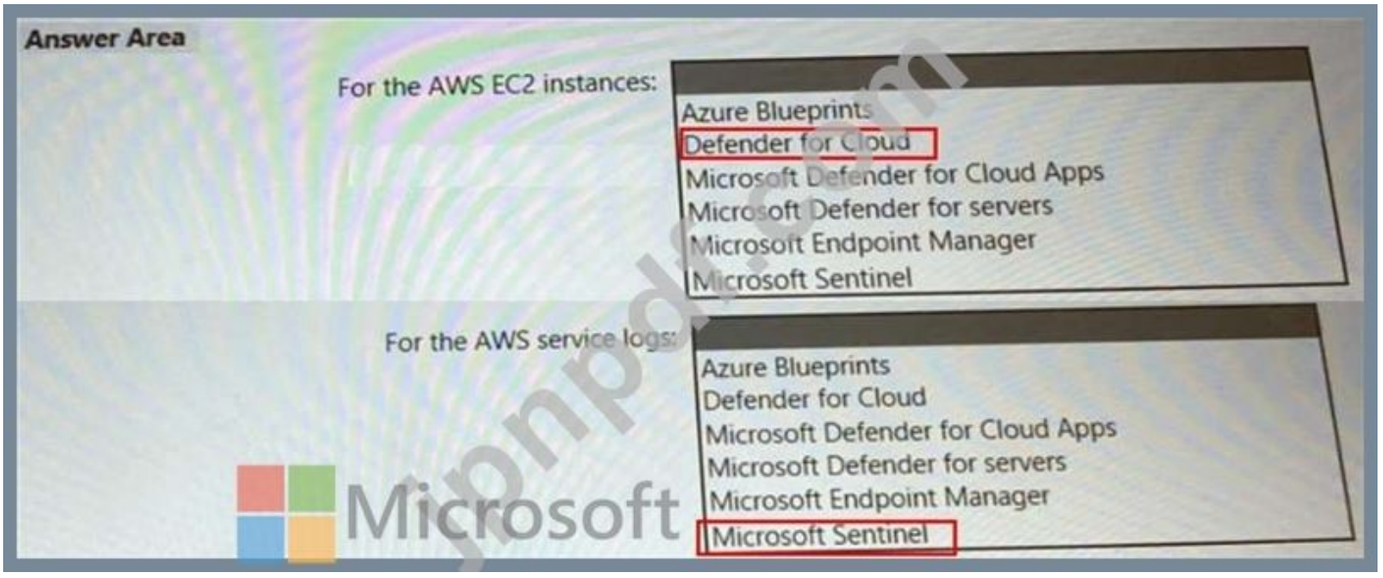
Answer:

最新問題: **82**
アプリケーションのセキュリティ要件を満たすために、アプリケーションはどの 2 つの認証方法をサポートする必要がありますか? それぞれの正解は完全な解決策を示します。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. セキュリティ アサーション マークアップ言語 (SAML)
B. NTLMv2
C. 証明書ベースの認証
D. ケルベロス
Answer: A,D (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

最新問題: **83**
AWS の要件を満たすソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: **84**

いくつかのレガシー アプリケーションを含むオンプレミス ネットワークがあります。アプリケーションは、既存のディレクトリ サービスに対して LDAP クエリを実行します。オンプレミスのインフラストラクチャをクラウドのみのインフラストラクチャに移行しています。

レガシー アプリケーションをサポートするインフラストラクチャ用の ID ソリューションを推奨する必要があります。ソリューションでは、インフラストラクチャを維持するための管理労力を最小限に抑える必要があります。

どの ID サービスを推奨事項に含めるべきですか?

A. Azure Active Directory ドメイン サービス (Azure AD DS)

B. Azure Active Directory (Azure AD) B2C

C. Azure Active Directory (Azure AD)

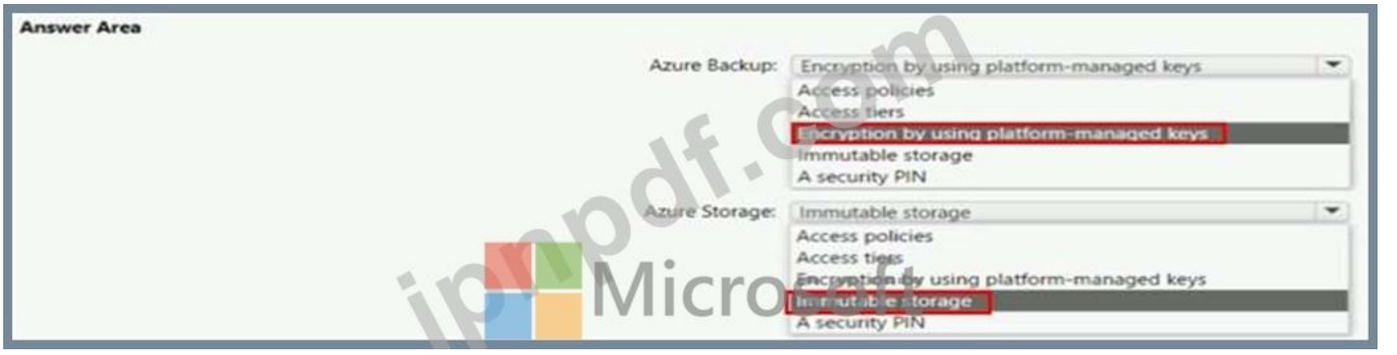
D. Active Directory ドメイン サービス (AD DS)

Answer: (解答を表示する**)**

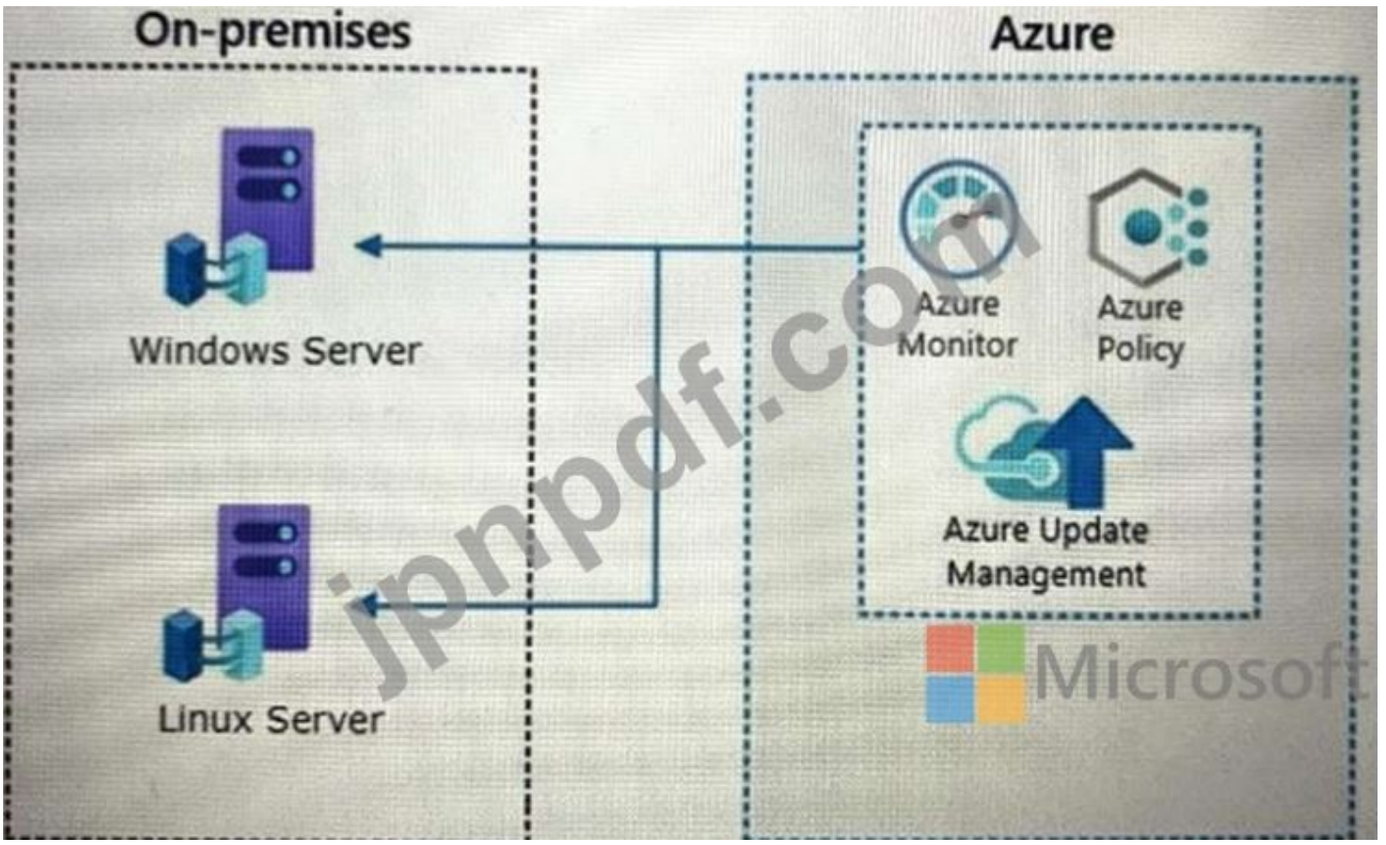
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

最新問題: **85**
あなたの会社は、リソースをランサムウェアから保護するために Azure の使用を最適化したいと考えています。
Azure Backup と Azure Storage のどの機能がランサムウェア攻撃に対して最も強力な保護を提供するかを推奨する必要があります。ソリューションは Microsoft セキュリティのベスト プラクティスに従う必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題: **86**
あなたの会社にはハイブリッド クラウド インフラストラクチャがあります。
データとアプリケーションはクラウド環境間で定期的に移動されます。
同社のオンプレミス ネットワークは、次の図に示すように管理されています。



注意 正しい選択はそれぞれ 1 ポイントの価値があります。

A. Azure VPN ゲートウェイ

B. オンプレミス データ ゲートウェイ

C. アズールバスティオン

D. Azure Policy のゲスト構成

E. アズールアーク

Answer: B,E (メーッセージを残す**)**

最新問題**: 87**

あなたの会社はシアトルにオンプレミス ネットワークと Azure サブスクリプションを持っています。オンプレミス ネットワークにはリモート デスクトップ サーバーが含まれています。

同社はフランスのサードパーティ開発会社と契約して、リソースを開発し、Azure サブスクリプションでホストされている仮想マシンにデプロイします。

現在、同社はリモート デスクトップ サーバーへの RDP 接続を確立しています。企業は、リモート デスクトップ接続から、リモート デスクトップ サーバーにインストールされているカスタム管理ツールを使用して、Azure でホストされている仮想マシンにアクセスできます。リモート デスクトップ サーバーへのすべてのトラフィックはファイアウォールによってキャプチャされ、ファイアウォールはフランスからサーバーへの特定の接続のみを許可します。

ゼロトラスト モデルに基づいた最新のセキュリティ ソリューションを推奨する必要があります。

このソリューションでは、開発者の待ち時間を最小限に抑える必要があります。

どの 3 つのアクションをお勧めしますか? それぞれの正解は、解決策の一部を示しています。

注: 正しく選択するたびに 1 ポイントの価値があります。

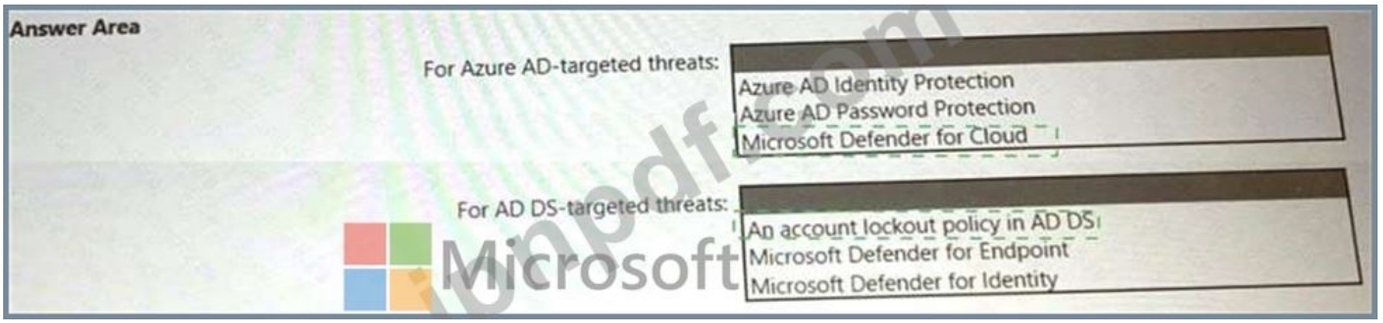
A. IP アドレス範囲の特定の論理グループのみからのアクセスを許可するようにネットワーク セキュリティ グループ (NSG) を構成します。
B. Azure Firewall を実装して、ホスト プールの送信アクセスを制限します。
C. 多要素認証 (MFA) と名前付き場所を使用して Azure Active Directory (Azure AD) 条件付きアクセスを構成します。
D. リモート デスクトップ サーバーから Azure Virtual Desktop に移行します。
E. リモート デスクトップ サーバーをフランスにある Azure リージョンにデプロイします。
Answer: B,C,D (メーッセージを残す)
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

最新問題**: 88**
Azure リソースの保存データの暗号化標準を設計している場合、保存データが AES-256 キーを使用して暗号化されるようにするための推奨事項を提供する必要があります。ソリューションは、暗号化キーの毎月のローテーションをサポートする必要があります。
解決策: Azure Storage の BLOB コンテナーの場合は、カスタマー マネージド キー (CMK) を使用した暗号化をお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
Answer: A (メーッセージを残す)

最新問題**: 89**
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。アマゾン ウェブ サービス (AWS) が実装されています。
Azure のセキュリティ戦略を AWS の実装に拡張することを計画しています。このソリューションでは Azure Arc は使用されません。AWS リソースのセキュリティを提供するために使用できる 3 つのサービスはどれですか? それぞれの正解は完全な解決策を示します。注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure ポリシー
B. サーバー用 Microsoft Defender
C. コンテナー用 Microsoft Defender
D. Azure Active Directory (Azure AD) 条件付きアクセス
E. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Answer: C,D (メーッセージを残す)

最新問題**: 90**
litware.com フォレストを保護するための戦略を推奨する必要があります。ソリューションは ID 要件を満たしている必要があります。推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。ノート; 正しく選択するたびに 1 ポイントの価値があります。

Answer:



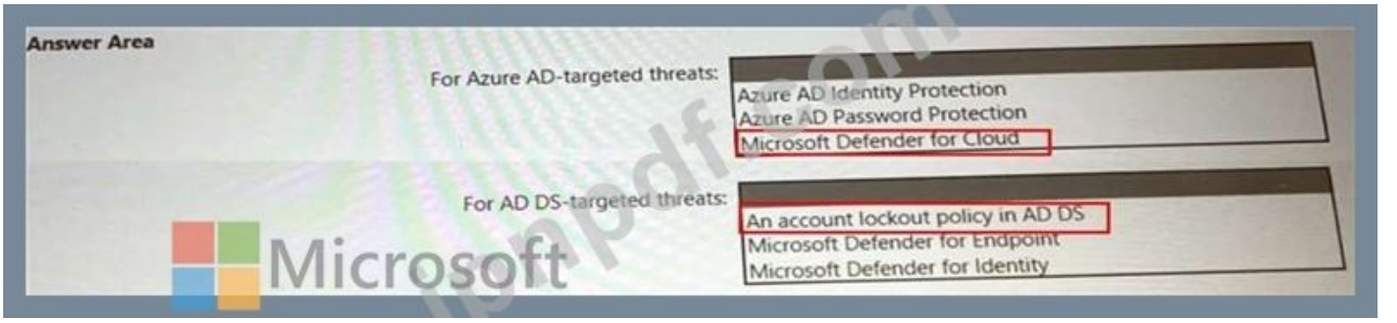
最新問題**: 91**
顧客は、Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを含むハイブリッド クラウド インフラストラクチャを所有しています。
境界ネットワーク内のすべてのオンプレミス サーバーは、インターネットに直接接続できません。
この顧客は最近、ランサムウェア攻撃から回復しました。
顧客は Microsoft Sentinel の導入を計画しています。
次の要件を満たす構成を推奨する必要があります。
* セキュリティ運用チームがセキュリティ ログと操作ログにアクセスできることを確認してください。
* IT 運用チームが、境界ネットワーク内のサーバーのイベント ログを含む運用ログのみにアクセスできるようにします。
推奨事項に含めることができる 2 つの構成はどれですか? それぞれの正解は完全な解決策を示します。注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure Active Directory (Azure AD) 条件付きアクセス ポリシー
B. リソースベースのロールベースのアクセス制御 (RBAC)
C. Log Analytics エージェントを使用するカスタム コレクター
D. Azure Monitor エージェント
Answer: B,D (メーッセージを残す)

最新問題: 92
オンプレミス ネットワークには、Angular と Nodejs で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行する予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。

Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロトラスト モデルに従う必要があります。
解決策: Web アプリとデータベース層のプライベート エンドポイントを作成することをお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
Answer: A (メーッセージを残す)

最新問題: 93
litware.com フォレストを保護するための戦略を推奨する必要があります。ソリューションは ID 要件を満たしている必要があります。推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。ノート; 正しく選択するたびに 1 ポイントの価値があります。

Answer:



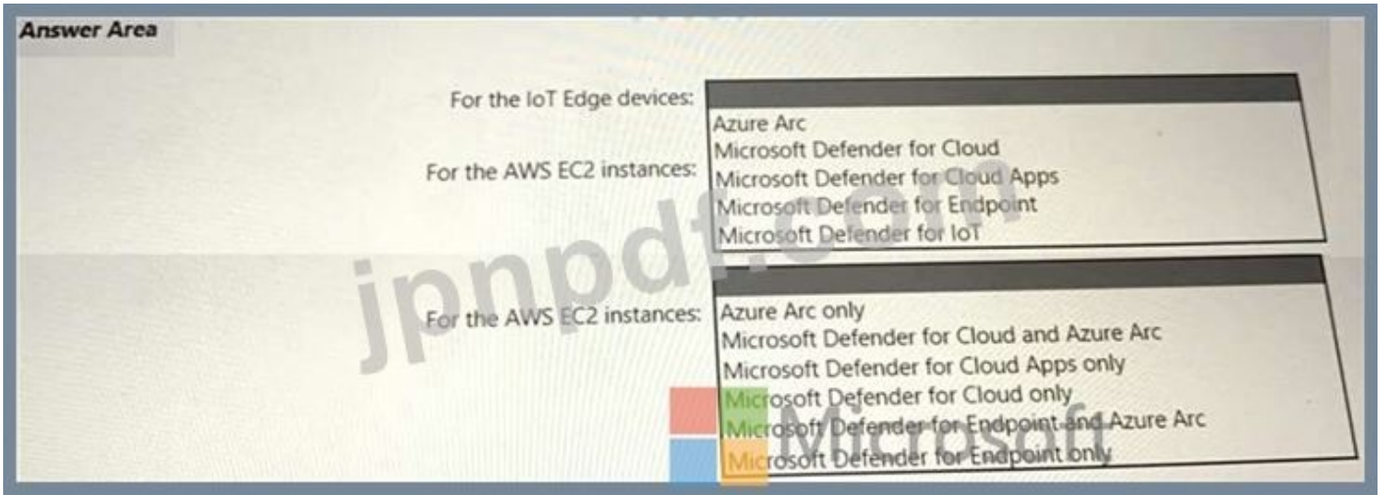
最新問題: **94**

あなたの会社には、Microsoft 365 サブスクリプション、Azure サブスクリプション、アマゾン ウェブ サービス (AWS) 実装を含むマルチクラウド環境があります。次のコンポーネントに対してセキュリティ体制管理ソリューションを推奨する必要があります。

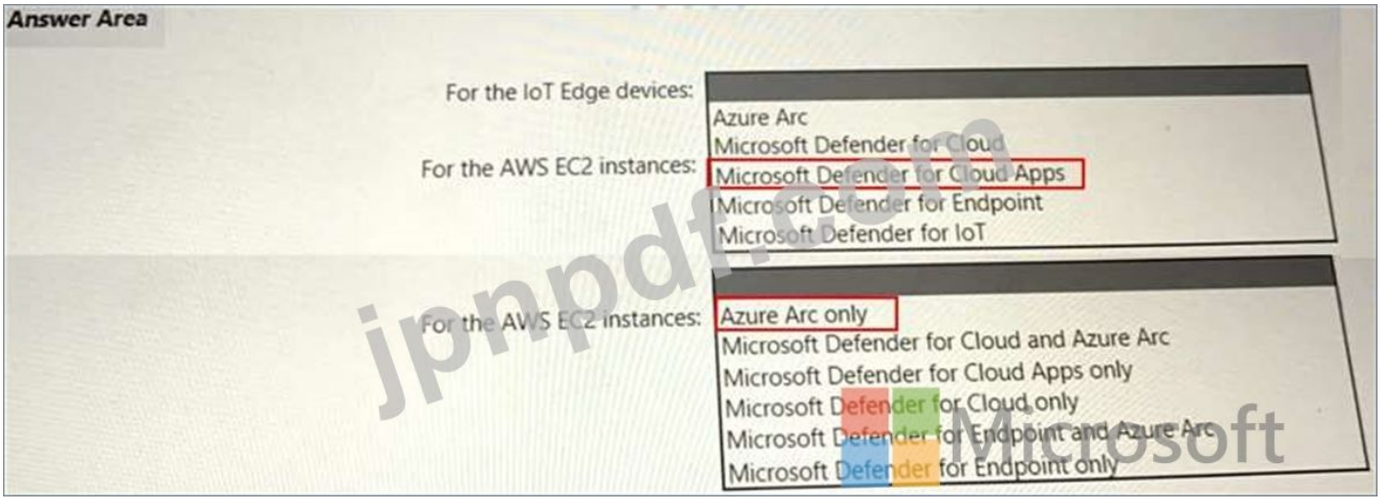
* Azure LOT Edge デバイス
* AWS EC2 インスタンス

どのサービスを推奨事項に含めるべきですか? 回答するには、回答内の適切なオプションを選択してください。

ａ．注正しく選択するたびに 1 ポイントの価値があります。

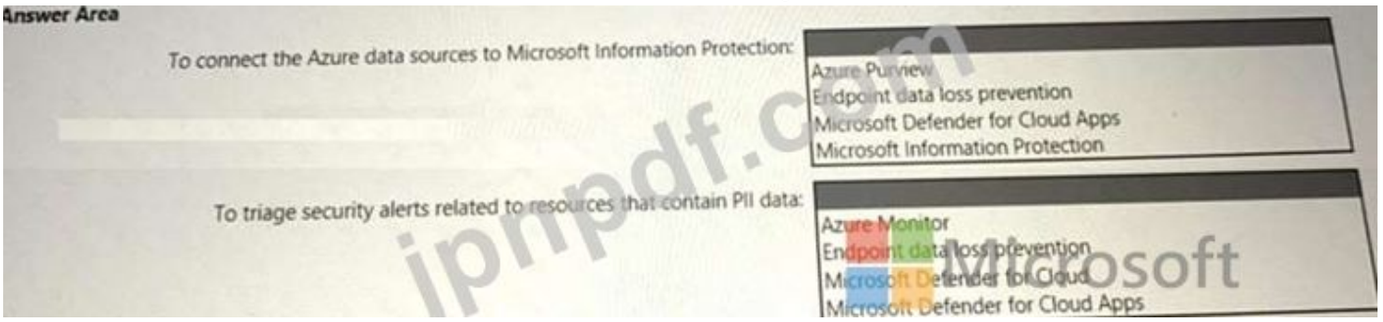


Answer:



最新問題: **95**

あなたの会社はデータを Azure に移行しています。データには個人を特定できる情報 (PII) が含まれています。同社は、Azure の PII データ ストアに Microsoft Information Protection を使用する予定です。Azure リソース内でリスクにさらされている PLL データを検出するソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

最新問題: **96**
あなたの会社にはハイブリッド クラウド インフラストラクチャがあります。
同社は短期間に数人の臨時従業員を雇用する予定だ。臨時従業員は、社内ネットワーク上のアプリケーションやデータにアクセスする必要があります。
会社のセキュリティ ポリシーにより、個人のデバイスを使用して会社のデータやアプリケーションにアクセスすることが禁止されています。
臨時従業員に会社のリソースへのアクセスを提供するソリューションを推奨する必要があります。ソリューションはオンデマンドで拡張できる必要があります。
推奨事項には何を含めるべきですか?
A. オンプレミス アプリケーションをクラウドベースのアプリケーションに移行します。
B. Microsoft エンドポイント マネージャーと Azure Active Directory (Azure AD) 条件付きアクセスをデプロイします。
C. Azure Virtual Desktop、Azure Active Directory (Azure AD) 条件付きアクセス、および Microsoft Defender for Cloud Apps を展開します。
D. スプリット トンネル構成を採用して VPN インフラストラクチャを再設計します。
Answer: (解答を表示する**)**

最新問題: **97**

Azure Automation アカウントで Runbook のセキュリティを設計しています。Runbook はデータを Azure Data Lake Storage Gen2 にコピーします。
コピー プロセスのコンポーネントを保護するソリューションを推奨する必要があります。
各コンポーネントの推奨事項には何を含める必要がありますか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しい選択はそれぞれ 1 ポイントの価値があります。

Answer:

最新問題: **98**
あなたの会社は、Microsoft セキュリティのベスト プラクティスに基づいて、Microsoft Defender for Endpoint の使用を最適化し、ランサムウェアからリソースを保護したいと考えています。
Microsoft セキュリティのベスト プラクティスの Microsoft Detection and Response Team (DART) のアプローチに基づいて、侵害されたコンピューターに対する侵害後の対応計画を準備する必要があります。
対応計画には何を含めるべきですか?
A. ユーザーの分離
B. アプリケーションの分離
C. フォルダーへのアクセスが制御されます
D. メモリスキャン
E. マシンの隔離
Answer: E (メーッセージを残す**)**

最新問題: **99**
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。アマゾン ウェブ サービス (AWS) が実装されています。
Azure のセキュリティ戦略を AWS の実装に拡張することを計画しています。このソリューションでは Azure Arc は使用されません。AWS リソースのセキュリティを提供するために使用できる

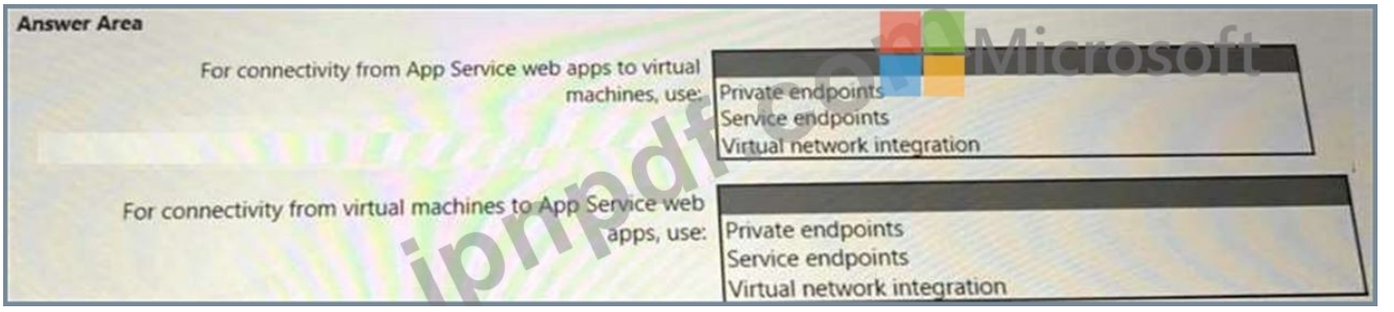
3 つのサービスはどれですか? それぞれの正解は完全な解決策を示します。注: 正しく選択するたびに 1 ポイントの価値があります。

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) 条件付きアクセス
C. サーバー用 Microsoft Defender
D. Azure ポリシー
E. コンテナー用 Microsoft Defender
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=aws-eks

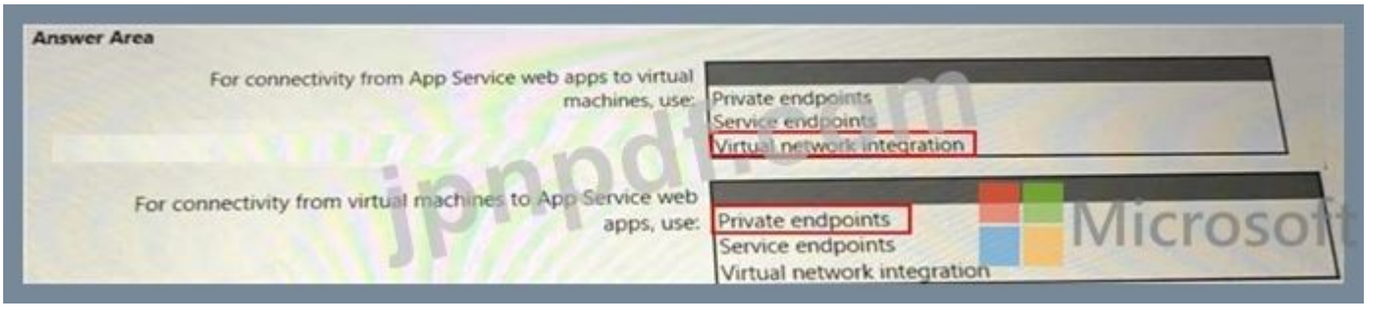
最新問題: **100**
Microsoft クラウド環境の場合、Microsoft Cybersecurity Reference Architectures (MCRA) に基づいてセキュリティ アーキテクチャを設計しています。次の攻撃チェーンの外部脅威から保護する必要があります。
* 攻撃者は外部 Web サイトにデータを流出させようとします。
* 攻撃者は、ドメインに参加しているコンピューター間で横方向の移動を試みます。
各脅威の推奨事項には何を含める必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

Answer:

最新問題: **101**
App Service Web アプリ接続の戦略を推奨する必要があります。ソリューションはランディング ゾーンの要件を満たしている必要があります。何を勧めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注意 正しい選択はそれぞれ 1 ポイントの価値があります。



Answer:



最新問題: **102**

オンプレミス ネットワークには、Angular と Nodejs で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行する予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。

Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロ トラスト モデルに従う必要があります。

解決策: 資格情報を保存するには、Azure Key Vault を実装することをお勧めします。

A. いいえ

B. はい

Answer: A (メーッセージを残す)

最新問題: **103**

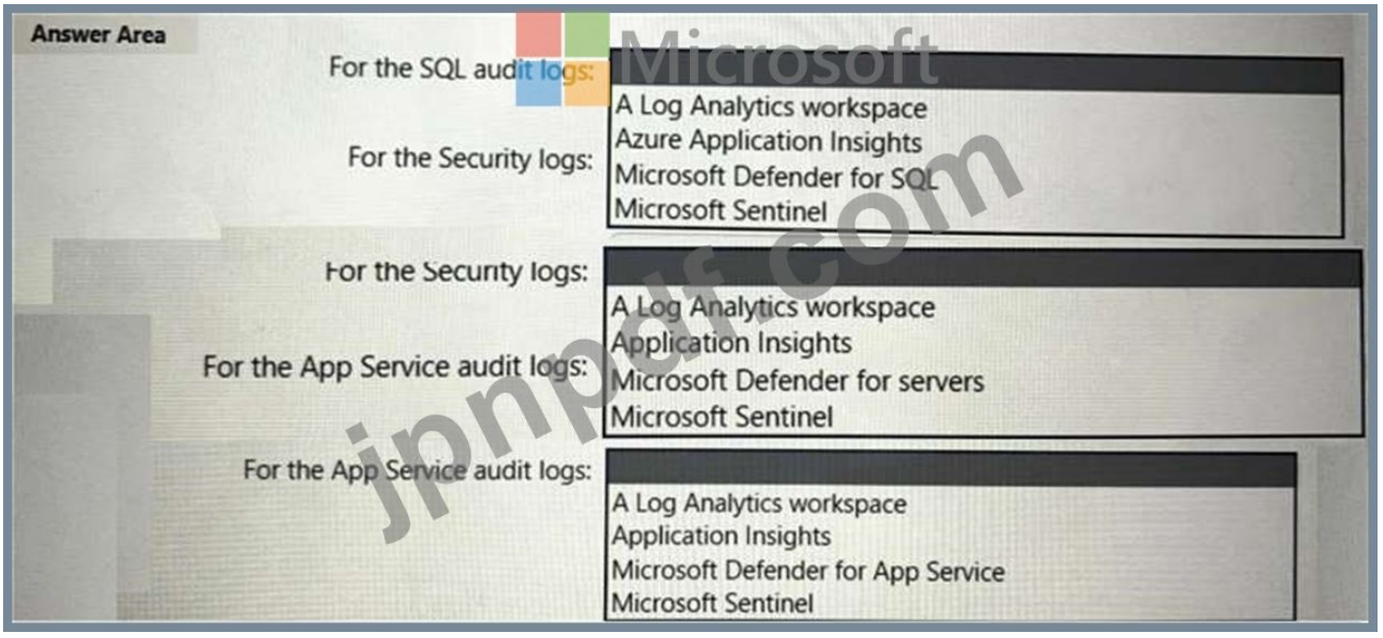
あなたの会社は、すべてのオンプレミス仮想マシンを Azure に移行することを計画しています。ネットワーク エンジニアは、次の表に示す Azure 仮想ネットワーク設計を提案します。

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

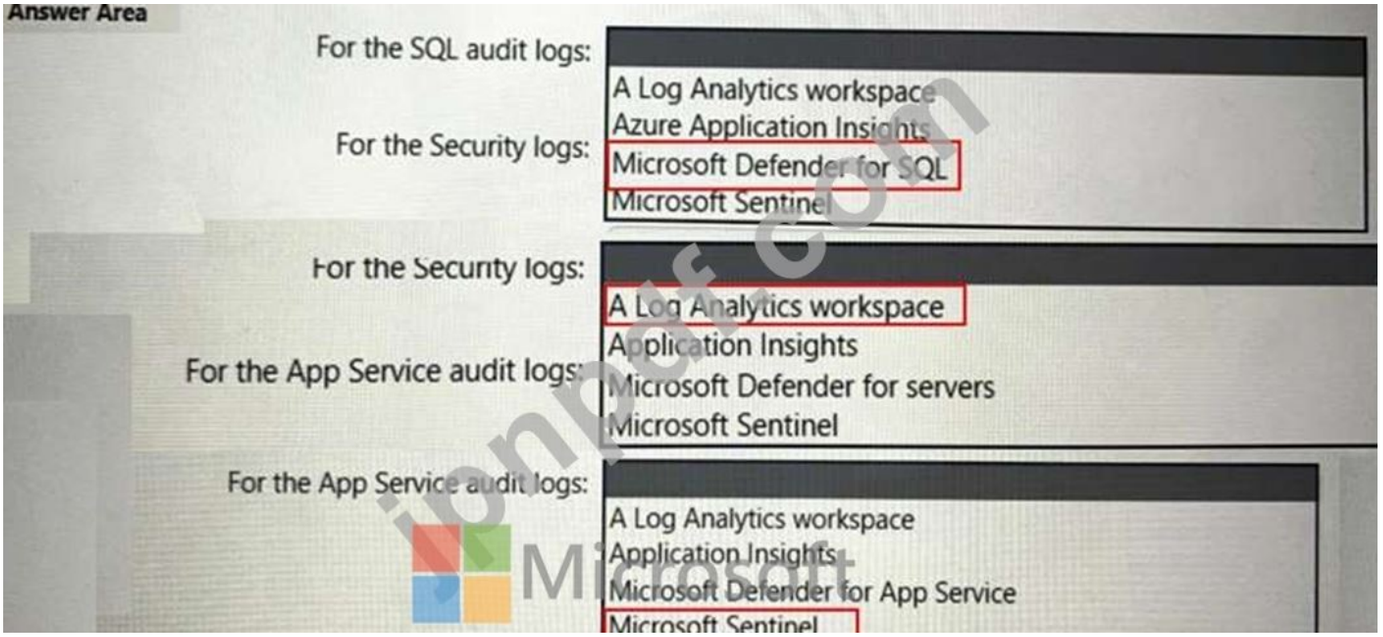
すべての仮想マシンへの安全なリモート アクセスを提供するには、Azure Bastion デプロイを推奨する必要があります。仮想ネットワーク設計に基づいて、Azure Bastion サブネットはいくつ必要ですか?

A. 3
B. 1
C. 2
D. 5
E. 4
Answer: B (メーッセージを残す**)**

最新問題**: 104**
次のコンポーネントを含む Azure ランディング ゾーンの監査ソリューションを設計しています。
* Azure SQL データベースの SQL 監査ログ
* Azure 仮想マシンからの Windows セキュリティ ログ
* App Service Web アプリからの Azure App Service 監査ログ
ランディング ゾーンに対して集中ログ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* すべての特権アクセスをログに記録します。
* ログは少なくとも 365 日間保持します。
*コストを最小限に抑えます。
推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: **105**

あなたは、Azure Front Door インスタンスを通じて Azure App Service Web アプリへのアクセスを提供するためのセキュリティ戦略を設計しています。

Web アプリが Front Door インスタンスを介したアクセスのみを許可するようにするソリューションを推奨する必要があります。

解決策: Front Door インスタンスのバックエンド IP アドレスからのトラフィックを許可するアクセス制限を推奨します。

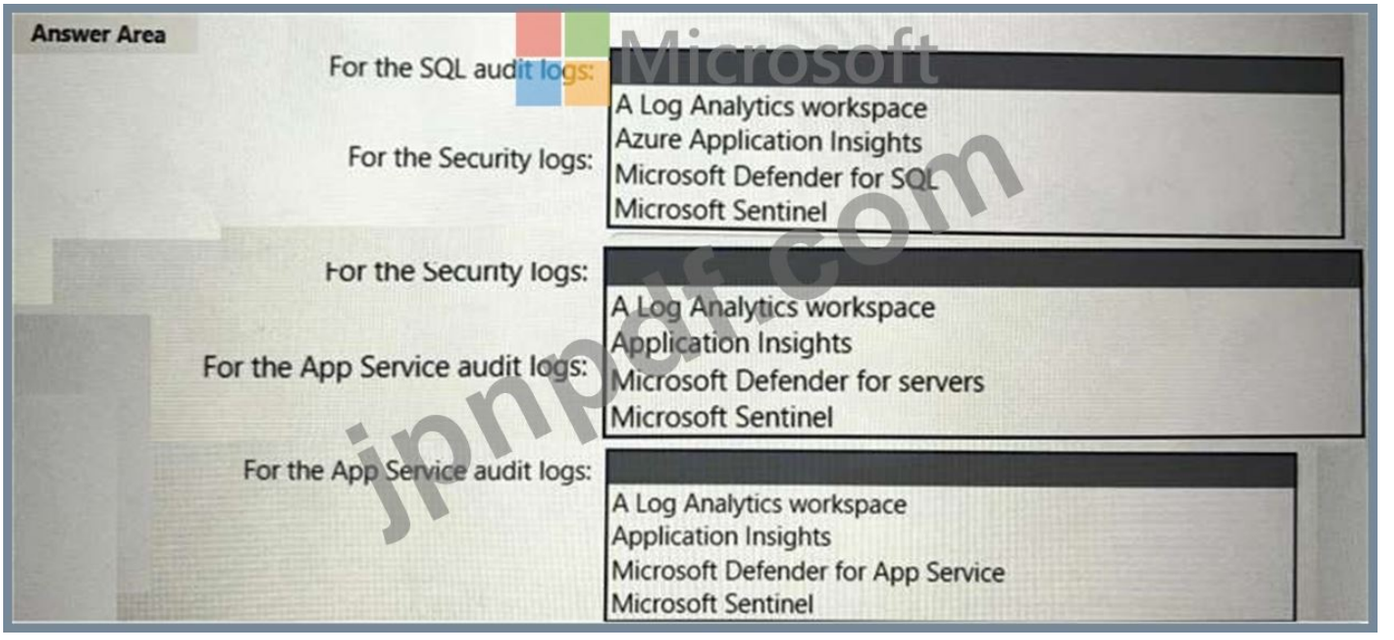
これは目標を達成していますか?

A. いいえ

B. はい

Answer: (解答を表示する**)**

最新問題: **106**
次のコンポーネントを含む Azure ランディング ゾーンの監査ソリューションを設計しています。
* Azure SQL データベースの SQL 監査ログ
* Azure 仮想マシンからの Windows セキュリティ ログ
* App Service Web アプリからの Azure App Service 監査ログ
ランディング ゾーンに対して集中ログ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* すべての特権アクセスをログに記録します。
* ログは少なくとも 365 日間保持します。
*コストを最小限に抑えます。
推奨事項には何を含めるべきですか? 回答するには、回答内の適切なオプションを選択してください。
ａ．注正しく選択するたびに 1 ポイントの価値があります。



Answer:

最新問題: **107**
アプリケーションのセキュリティ要件を満たすために、アプリケーションはどの 2 つの認証方法をサポートする必要がありますか? それぞれの正解は完全な解決策を示します。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. セキュリティ アサーション マークアップ言語 (SAML)
B. NTLMv2
C. 証明書ベースの認証
D. ケルベロス
Answer: (解答を表示する**)**
トピック 1、Litware, Inc.
既存の環境
Litware には、Utvvare.com という名前の Active Directory Domain Services (AD D%) フォレストと同期する Azure Active Directory (Azure AD) テナントがあり、20 の Azure サブスクリプションにリンクされています。Azure AD Connect は、パススルー認証の実装に使用されます。パスワード ハッシュ同期は無効になり、パスワード ライトバックは有効になります。すべての Litware ユーザーは Microsoft 365 E5 ライセンスを持っています。
この環境には、いくつかの AD DS フォレスト、Azure AD テナント、および Litware の子会社に属する数百の Azure サブスクリプションも含まれています。
計画された変更
Litware は次の変更を実装する予定です。
* Azure AD テナントごとに管理グループ階層を作成します。
* Litware の既存の Azure 環境をリファクタリングし、将来のすべての Azure ワークロードをデプロイするためのランディング ゾーン戦略を設計します。
* Azure AD アプリケーション プロキシを実装して、現在 VPN を使用してアクセスされている内部アプリケーションへの安全なアクセスを提供します。
ビジネス要件
Litware は次のビジネス要件を特定します。
* 追加のオンプレミス インフラストラクチャを最小限に抑えます。
* 管理オーバーヘッドに関連する運用コストを最小限に抑えます。
ハイブリッドの要件
Litware では、次のハイブリッド クラウド要件を特定しています。
* Azure からの次のようなオンプレミス リソースの管理を有効にします。

* 施行とコンプライアンスの評価には Azure Policy を使用します。
* 変更追跡と資産インベントリを提供します。
* パッチ管理を実装します。
* ゲスト アカウントの維持にかかるオーバーヘッドを発生させずに、一元的なテナント間サブスクリプション管理を提供します。

Microsoft Sentinelの要件

Litware は、Microsoft Sentinel のセキュリティ情報およびイベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAK) 機能を活用する予定です。同社は、Microsoft Sentinel を使用して Security Operations Center (SOQ) を一元化したいと考えています。

アイデンティティ要件

Litware は次の ID 要件を特定します。
* AD DS ユーザー アカウントを直接ターゲットとするブルート フォース攻撃を検出します。
* Litware の Azure AD テナントに漏洩した資格情報の検出を実装します。
* Azure AD ユーザー アカウントをターゲットとしたブルート フォース攻撃によって AD DS ユーザー アカウントがロックアウトされるのを防ぎます。
* Litware の Azure AD テナントにユーザーとグループの委任管理を実装します (サポートを含む)。
* グループのプロパティ、メンバーシップ、ライセンスの管理、ユーザーのプロパティ、パスワード、ライセンスの管理
* ビジネスユニットに基づいたユーザー管理の委任。

規制遵守要件

Litware では、次の規制遵守要件を特定しています。
* 米国およびフランスに拠点を置く各子会社が所有するログ、テレメトリ、およびデータを収集する際に、データ常駐に関するコンプライアンスを保証します。
* 組み込みの Azure Policy 定義を活用して、管理された環境全体にわたる法規制への準拠を評価します。
* 最小特権の原則を使用します。

Azure ランディング ゾーンの要件

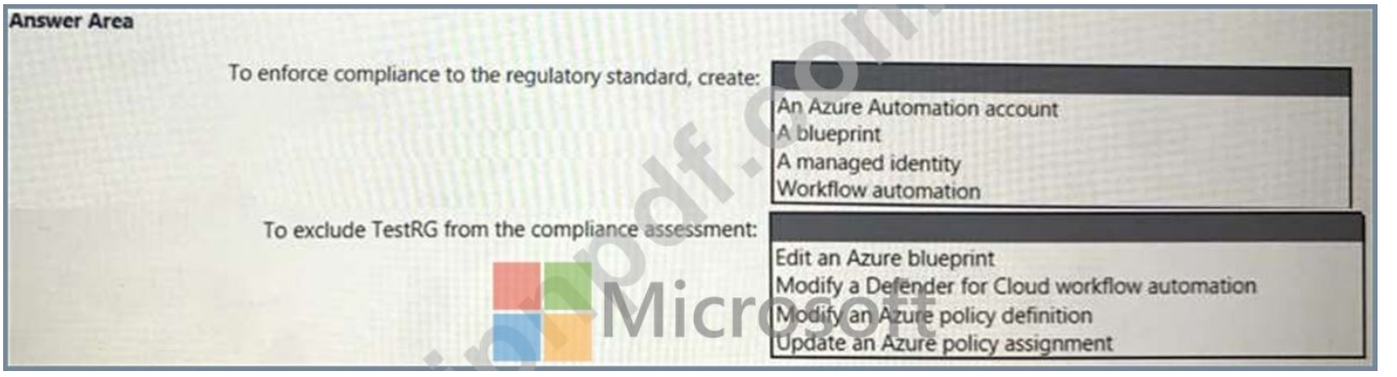
Litware は、次のランディング ゾーン要件を特定します。
* インターネットに向かうすべてのトラフィックを、専用の Azure サブスクリプションの Azure Firewall 経由でランディング ゾーンからルーティングします。
* ランディング ゾーンを対象とした安全なスコアを提供します。
* 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信していることを確認します。
* データ漏洩の可能性を最小限に抑えます。
* ネットワーク帯域幅を最大化します。

ランディング ゾーン アーキテクチャには、インターネットおよびハイブリッド接続のハブとして機能する専用のサブスクリプションが含まれます。各ランディング ゾーンには次の特徴があります。
* 専用のサブスクリプションで作成されます。
* litware.com の DNS 名前空間を使用します。
アプリケーションのセキュリティ要件
Litware は、次のアプリケーションのセキュリティ要件を特定します。
* Azure AD アプリケーション プロキシを使用してシングル サインオン (SSO) をサポートする内部アプリケーションを特定します。
* Microsoft SharePoint Online および Exchange Online データへのアクセスをリアルタイムで監視および制御します。

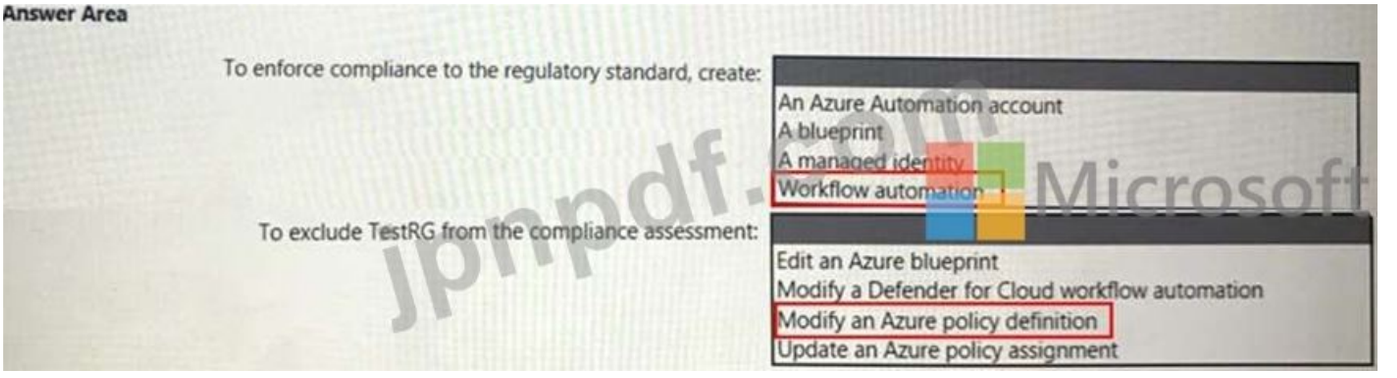
最新問題: **108**
Microsoft 365 E5 サブスクリプションをお持ちです。
あなたは、100 万を超えるドキュメントを含む Microsoft SharePoint Online サイトの機密データを保護するソリューションを設計しています。
個人識別情報 (PII) の共有を防ぐソリューションを推奨する必要があります。
推奨事項に含めるべき 2 つのコンポーネントはどれですか? それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. データ損失防止 (DLP) ポリシー
B. 機密ラベルポリシー
C. 保持ラベルポリシー
D. 電子情報開示ケース
Answer: (解答を表示する**)**
Office 365 のデータ損失防止。データ損失防止 (DLP) は、機密情報を保護し、不用意な開示を防ぐのに役立ちます。組織外への漏洩を防止したい機密情報の例には、財務データや、クレジット カード番号、社会保障番号、健康記録などの個人識別情報 (PII) が含まれます。データ損失防止 (DLP) ポリシーを使用すると、Office 365 全体で機密情報を識別、監視し、自動的に保護できます。
Microsoft Purview Information Protection の機密ラベルを使用すると、ユーザーの生産性や共同作業能力を妨げることなく、組織のデータを分類して保護できます。より広範な情報保護スキームへの統合を計画します。OME との共存に加えて、秘密度ラベルは Microsoft Purview データ損失防止 (DLP) や Microsoft Defender for Cloud Apps などの機能と併用できます。
https://motionwave.com.au/keeper-your-confidential-data-secure-with-microsoft-office-365/
https://docs.microsoft.com/en-us/microsoft-365/solutions/information- protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

最新問題: **109**
コンプライアンス要件を満たすソリューションを推奨する必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



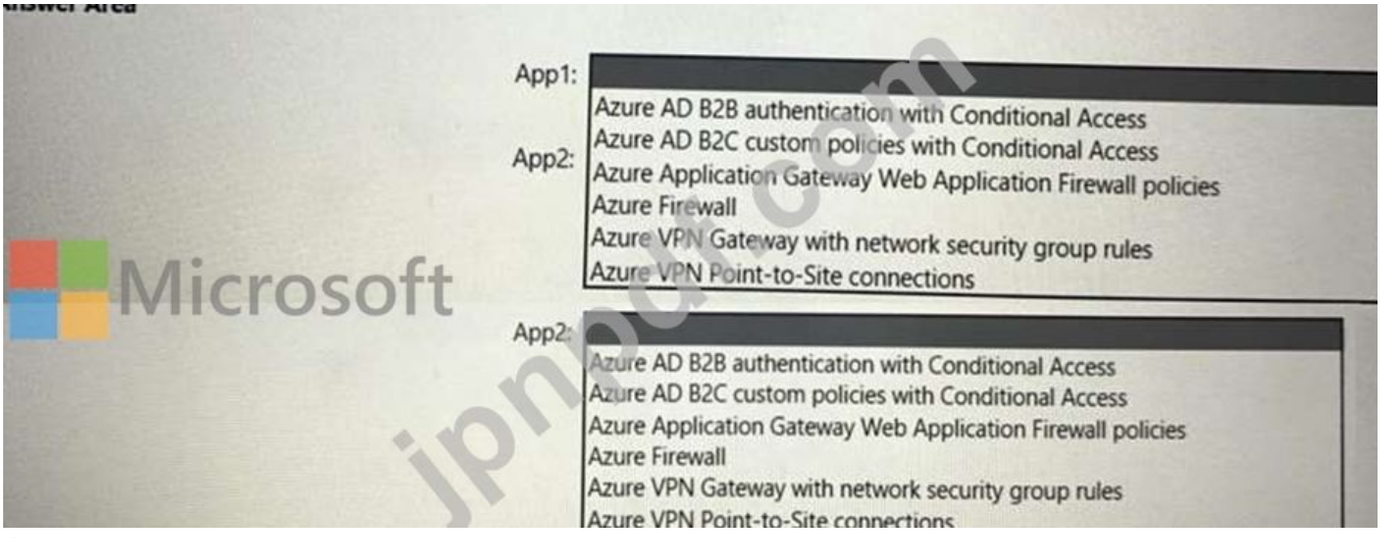
最新問題**: 110**

ハイブリッド クラウド インフラストラクチャがあります。

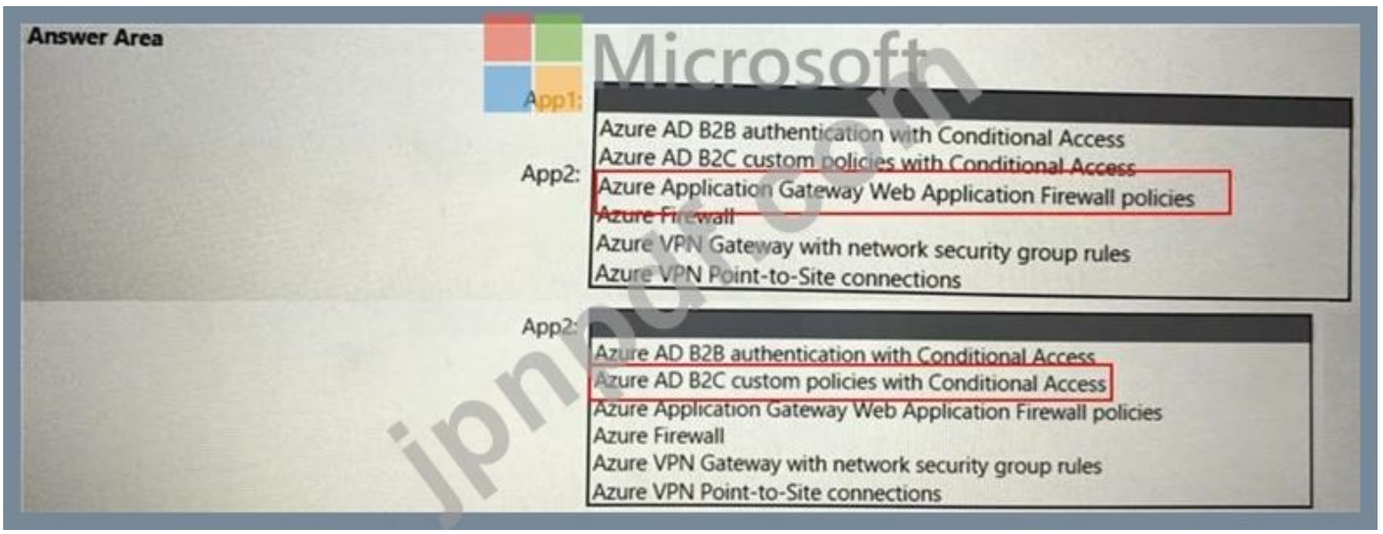
次の表に示す Azure アプリケーションをデプロイする予定です。

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

各アプリの要件を満たすには何を使用する必要がありますか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題**: 111**

セキュリティ アクセス戦略のセキュリティ レベルを計画しています。

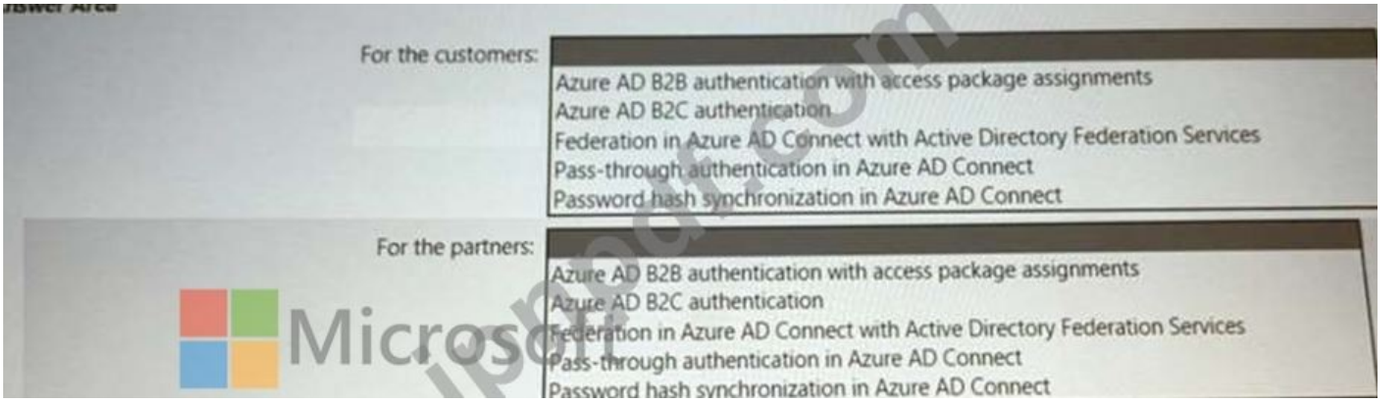
どのジョブの役割をどのセキュリティ レベルで構成するかを特定する必要があります。ソリューションは、Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。

各職務にどのセキュリティ レベルを設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

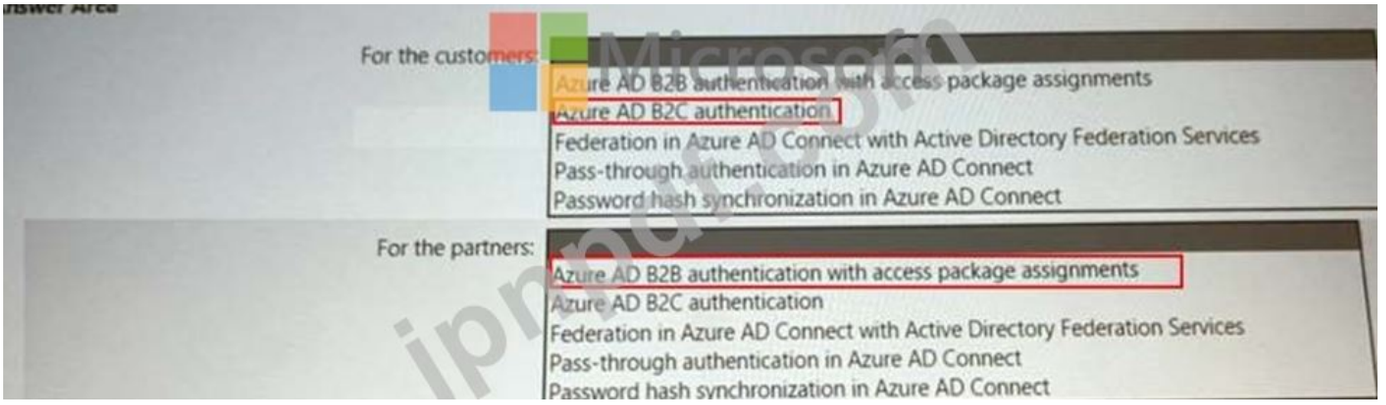
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

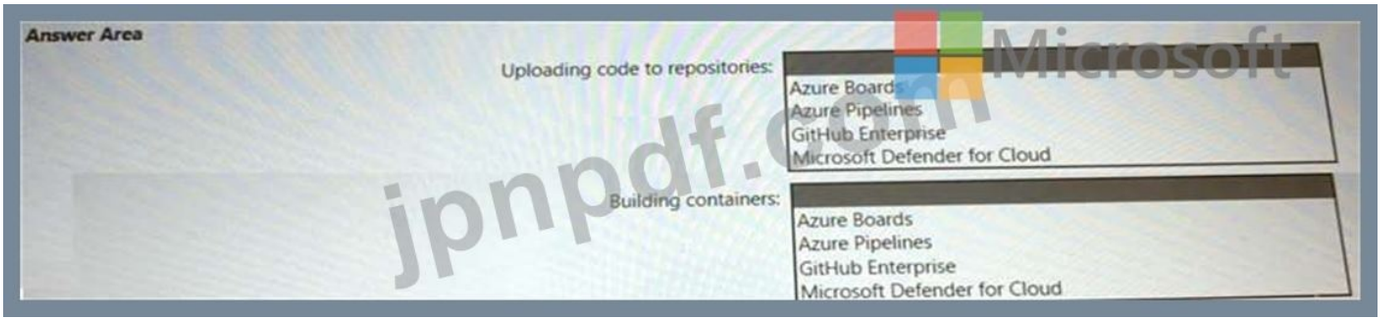
最新問題: **112**
あなたの会社には Microsoft 365 E5 サブスクリプション、Azure サブスクリプション、オンプレミス アプリケーション、および Active Directory ドメイン サービス (AD DSV) があります。次の要件を満たす ID セキュリティ戦略を推奨する必要があります。
* 顧客が Facebook 資格情報を使用して Azure App Service Web サイトへの認証を行えることを保証します
* パートナー企業が、割り当てられているプロジェクトの Microsoft SharePoint Online サイトにアクセスできるようにします。ソリューションでは、追加のインフラストラクチャ コンポーネントを展開する必要性を最小限に抑える必要があります。推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



最新問題: **113**
あなたの会社には、コンテナー化された Web アプリをデプロイするために使用される Azure App Service プランがあります。Web アプリを App Service プランにデプロイするための安全な DevOps 戦略を設計しています。コード スキャン ツールを安全なソフトウェア開発ライフサイクルに統合する戦略を推奨する必要があります。コードは次の 2 つのフェーズでスキャンする必要があります。
コードをリポジトリにアップロードする コンテナを構築する
各フェーズのコード スキャンをどこに統合する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。



Answer:

最新問題: **114**

あなたの会社は、すべてのオンプレミス仮想マシンを Azure に移行することを計画しています。ネットワーク エンジニアは、次の表に示す Azure 仮想ネットワーク設計を提案します。

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

すべての仮想マシンへの安全なリモート アクセスを提供するには、Azure Bastion デプロイを推奨する必要があります。仮想ネットワーク設計に基づいて、Azure Bastion サブネットはいくつ必要ですか?

A. 1

B. 2

C. 3

D. 4

E. 5

Answer: B (メーッセージを残す**)**

説明

https://docs.microsoft.com/en-us/azure/bastion/vnet-peering

https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

最新問題: **115**

Microsoft 365 サブスクリプションと Azure サブスクリプションをお持ちです。Microsoft 365 Defender と Microsoft Defender for Cloud が有効になっています。

Azure サブスクリプションには Microsoft Sentinel ワークスペースが含まれています。Microsoft Sentinel データ コネクタは、Microsoft 365、Microsoft 365 Defender、Defender for Cloud、および Azure 用に構成されています。

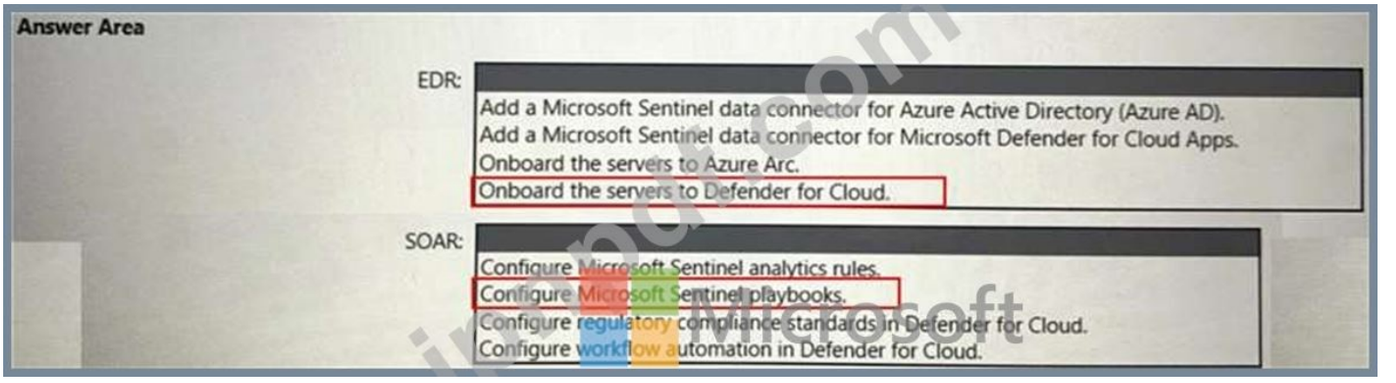
Windows Server を実行する Azure 仮想マシンをデプロイする予定です。

Microsoft Sentinel の拡張検出と応答 (EDR) およびセキュリティ オーケストレーション、自動化、および応答 (SOAR) 機能を有効にする必要があります。

各機能を有効にすることをどのように推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



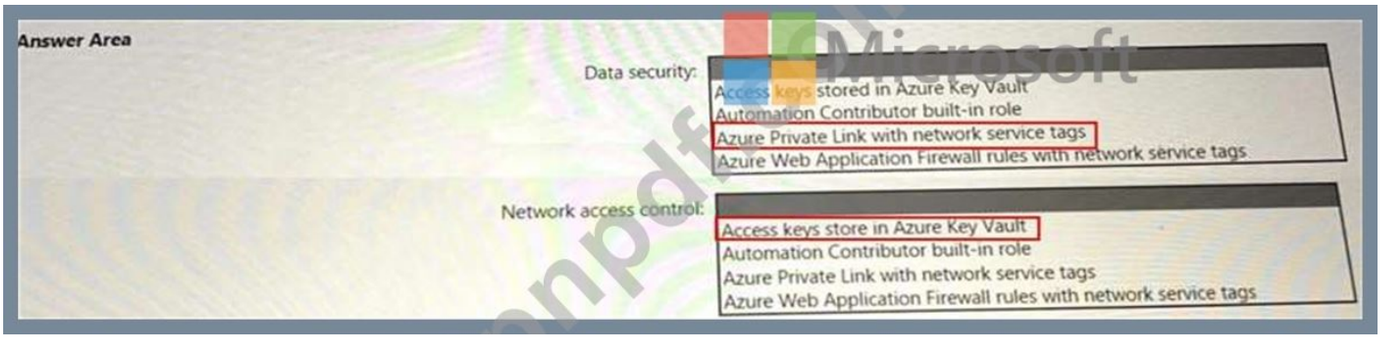
最新問題: **116**

Azure Automation アカウントで Runbook のセキュリティを設計しています。Runbook はデータを Azure Data Lake Storage Gen2 にコピーします。

コピー プロセスのコンポーネントを保護するソリューションを推奨する必要があります。

各コンポーネントの推奨事項には何を含める必要がありますか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



最新問題**: 117**

あなたの会社は Microsoft 365 E5 ライセンスと Azure サブスクリプションを持っています。

同社は、次の場所に保存されている機密データに自動的にラベルを付けることを計画しています。

* Microsoft SharePoint Online
* Microsoft Exchange Online
*マイクロソフトチーム

機密データを特定して保護するための戦略を推奨する必要があります。

機密ラベル ポリシーにはどの範囲を推奨する必要がありますか? 答えるには、適切なスコープを正しい場所にドラッグします。各スコープは、1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。

注: 正しく選択するたびに 1 ポイントの価値があります。

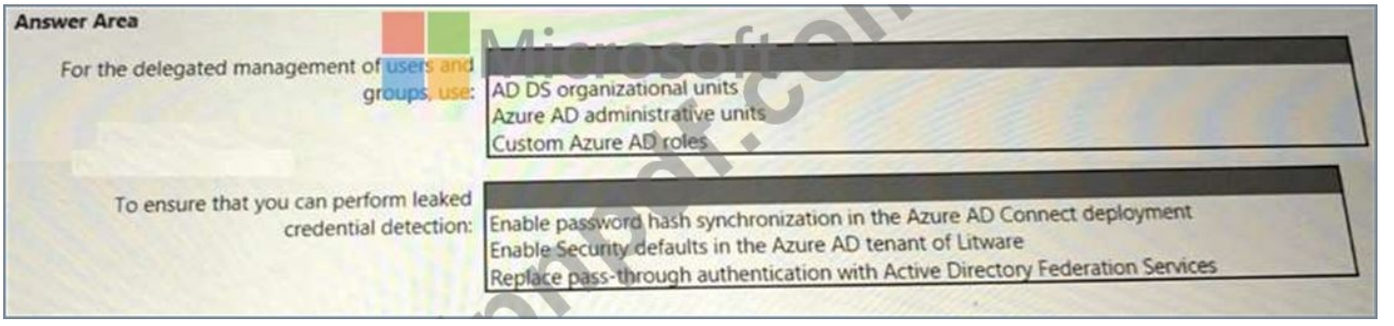
Answer:

最新問題: **118**
Azure Storage を使用する Azure サブスクリプション。
同社は特定の BLOB をベンダーと共有する予定です。BLOB を公に公開せずに、特定の BLOB への安全なアクセスをベンダーに提供するソリューションを推奨する必要があります。アクセスは t \me-Vim\ted である必要があります。推奨事項には何を含めるべきですか?
A. 共有アクセス署名 (SAS) を作成します。
B. アクセスキーの接続文字列を共有します。
C. プライベートリンク接続を設定します。
D. カスタマー マネージド キー (CMK) を使用して暗号化を構成する
Answer: (解答を表示する**)**
トピック 2、Fabrikam, Inc
オンプレミス環境
オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Azure環境
Fabrikam には次の Azure リソースがあります。
* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnetl という名前の仮想ネットワーク
* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。
パートナー
Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続します。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。

ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。
コンプライアンスイベント
Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修正されています。
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。
アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。
* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件

Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題**: 119**
Litware の Azure AD テナントに ID セキュリティ ソリューションを推奨する必要があります。ソリューションは、ID 要件と法規制遵守要件を満たしている必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer: