

Microsoft SC-100 トレーニング サンプル、SC-100 ファンデーション



2026年PassTestの最新SC-100 PDFダンプおよびSC-100試験エンジンの無料共有: <https://drive.google.com/open?id=1g8SuaAnYfw6kcuVond0tgctqAx4UawO0>

どのようにして短時間で試験に合格し、証明書を取得できますか？ SC-100試験トレントは、目標を達成するための最良の選択です。お客様のニーズに応じて、当社の製品は多くの専門家によって改訂されました。SC-100試験問題集のほとんどの機能は、お客様がより多くの時間を節約し、お客様をリラックスさせるのに役立ちます。SC-100テストクイズを使用することを選択した場合、短時間でSC-100試験に合格することは非常に簡単です。SC-100試験問題の勉強に20~30時間費やすだけです。他のことをする自由時間が増えます。

Microsoft SC-100試験を受けるには、候補者はサイバーセキュリティの概念、Microsoft Security Technologiesの経験、およびセキュリティ運用の知識を十分に理解する必要があります。また、Microsoft Technologiesを使用してサイバーセキュリティソリューションの設計、実装、および維持の経験が必要です。

Microsoft SC-100試験は、サイバーセキュリティでのキャリアを追求したいと考えており、業界で認識された認定でスキルと知識を検証したい人に最適です。この試験は、すでにサイバーセキュリティに取り組んでおり、Microsoft Security TechnologiesとSolutionsの知識とスキルを向上させたい専門家にも適しています。Microsoft SC-100試験に合格することにより、個人はMicrosoft Security Technologiesを使用して安全なソリューションを設計および実装する能力を実証できます。

マイクロソフトSC-100（マイクロソフトサイバーセキュリティアーキテクト）試験は、サイバーセキュリティアーキテクトの知識とスキルを評価するために設計されています。この試験は、サイバーセキュリティのキャリアを追求し、この分野のスキルと知識を検証したい人々を対象としています。マイクロソフトSC-100試験は、ITとサイバーセキュリティのバックグラウンドを持ち、この分野のスキルと知識を向上させたい人々に適しています。

>> Microsoft SC-100 トレーニング サンプル <<

SC-100 ファンデーション & SC-100 試験勉強書

SC-100認定を取得することは、学生、教師、主婦など、さまざまな分野の多くの人々にますます一般的になっていることがわかっています。全員がSC-100認定を取得することが望まれます。私たちのSC-100試験ダンプ問題は、短時間で認定を取得するために最善を尽くすために非常に必要です。SC-100 Exam Braindumpsは、試験に合格する手を差し伸べます。SC-100 Exam Torrentは、認定を取得するための最良の学習ツールです。

Microsoft Cybersecurity Architect 認定 SC-100 試験問題 (Q101-Q106):

質問 # 101

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

* Prevent the need to enable ports 3389 and 22 from the internet.

* Only provide permission to connect the virtual machines when required.

* Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- **A. Enable Just Enough Administration (JEA).**
- B. Configure Azure VPN Gateway.
- **C. Configure Azure Bastion.**
- D. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
- E. Enable just-in-time (JIT) VM access.

正解: A、C

解説:

Topic 1, Litware, inc.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named Utvware.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses. The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

* Create a management group hierarchy for each Azure AD tenant.

* Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

* Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

* Minimize any additional on-premises infrastructure.

* Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

* Enable the management of on-premises resources from Azure, including the following:

* Use Azure Policy for enforcement and compliance evaluation.

* Provide change tracking and asset inventory.

* Implement patch management.

* Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

* Detect brute force attacks that directly target AD DS user accounts.

* Implement leaked credential detection in the Azure AD tenant of Litware.

* Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.

* Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:

* The management of group properties, membership, and licensing

* The management of user properties, passwords, and licensing

* The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

* Insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.

* Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.

* Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

* Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

* Provide a secure score scoped to the landing zone.

- * Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
- * Minimize the possibility of data exfiltration.
- * Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

- * Be created in a dedicated subscription.
- * Use a DNS namespace of litware.com.

Application Security Requirements

Litware identifies the following application security requirements:

- * Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
- * Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

質問 # 102

Your company is exploring migrating data into Azure; they would like to have a central authentication solution when accessing the data; they have chosen Azure Active Directory.

Which two storage types natively support Active Directory authentication?

- **A. Azure Storage blob containers**
- B. Azure File Share
- **C. Azure Data Lake Storage Gen2**
- D. Azure Data Box

正解: A、C

解説:

Option D is correct Because Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to blob data.

Option B is correct Because Azure Data Lake Storage Gen2 (ADLS Gen2) accounts support using OAuth 2.0 with an Azure Active Directory (Azure AD).

Option C is incorrect because To support AD DS authentication over SMB for Azure File Share; you need to register your storage account with AD DS.

Option A is incorrect because Azure Data Box is a device used to move large amounts of data to Azure; this process is known as seeding.

References:

<https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory>

<https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access>

質問 # 103

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines. You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines.

What should recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

正解:

解説:

Explanation:

質問 # 104

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation?

- **A. Onboard the virtual machines to Microsoft Defender for Endpoint.**
- B. Enable the Qualys scanner in Defender for Cloud.
- C. Onboard the virtual machines to Azure Arc.
- D. Create a device compliance policy in Microsoft Endpoint Manager.

正解: A

解説:

Topic 1, Fabrikam, Inc

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com

Azure Environment

Fabrikam has the following Azure resources:

- * An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabrikam.com
- * A single Azure subscription named Sub1
- * A virtual network named Vnet1 in the East US Azure region
- * A virtual network named Vnet2 in the West Europe Azure region
- * An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAF) enabled
- * A Microsoft Sentinel workspace
- * An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- * 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- * A resource group named TestRG that is used for testing purposes only
- * An Azure Virtual Desktop host pool that contains personal assigned session hosts. All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-

- * An Azure AD tenant named contoso.onmicrosoft.com
- * An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- * Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- * Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- * Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- * ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- * Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com
- * ClaimsApp will access data in ClaimsDB.
- * ClaimsDB must be accessible only from Azure virtual networks.
- * The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- * Azure DevTest labs will be used by developers for testing.
- * All the application code must be stored in GitHub Enterprise.
- * Azure Pipelines will be used to manage application deployments.
- * All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- * Internet-accessible applications must prevent connections that originate in North Korea.
- * Only members of a group named InfraSec must be allowed to configure network security groups (NSGs) and instances of Azure Firewall, WAF, and Front Door in Sub1.
- * Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- * Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- * Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers;

- * Every month, the membership of the ContosoDevelopers group must be verified.
- * The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- * The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

質問 # 105

Your company has an office in Seattle.

The company has two Azure virtual machine scale sets hosted on different virtual networks.

The company plans to contract developers in India.

You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

- * Prevent exposing the public IP addresses of the virtual machines.
- * Provide the ability to connect without using a VPN.
- * Minimize costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enable just-in-time VM access on the virtual machines.
- B. Deploy Azure Bastion to each virtual network.
- C. Create NAT rules and network rules in Azure Firewall.
- D. Create a hub and spoke network by using virtual network peering.
- E. Deploy Azure Bastion to one virtual network.

正解: C、D

質問 # 106

.....

市場の他の教育プラットフォームと比較して、PassTestはより信頼性が高く、非常に効率的です。これは、SC-100試験に合格したい受験者に高い合格率SC-100の教材を提供し、すべてのお客様が最初の試行でSC-100試験に合格しています。ウェブサイトでSC-100試験に合格するには、20~30時間かかります。それは本当に他のことをするために多くの時間とエネルギーを節約するのを助けることができる非常に効率的な試験ツールです。

SC-100ファンデーション: <https://www.passtest.jp/Microsoft/SC-100-shiken.html>

- SC-100試験の準備方法 | 実用的なSC-100トレーリングサンプル試験 | 100%合格率のMicrosoft Cybersecurity Architectファンデーション □ “SC-100”を無料でダウンロード ➡ www.it-passports.com □ ウェブサイトを入力するだけSC-100的中関連問題
- 効果的なMicrosoft SC-100トレーリングサンプル - 合格スムーズSC-100ファンデーション | 信頼できるSC-100試験勉強書 □ (www.goshiken.com) に移動し、 □ SC-100 □ を検索して、無料でダウンロード可能な試験資料を探しますSC-100試験問題
- SC-100無料ダウンロード □ SC-100無料ダウンロード □ SC-100予想試験 □ 「 www.goshiken.com 」は、 (SC-100) を無料でダウンロードするのに最適なサイトですSC-100無料ダウンロード
- SC-100試験の準備方法 | 実用的なSC-100トレーリングサンプル試験 | 100%合格率のMicrosoft Cybersecurity Architectファンデーション □ [www.goshiken.com] は、 ▶ SC-100 ◀ を無料でダウンロードするのに最適なサイトですSC-100一発合格
- SC-100日本語版参考書 □ SC-100試験問題 □ SC-100無料ダウンロード □ 時間限定無料で使える ▶ SC-100 ◀ の試験問題は ➡ www.japancert.com □ サイトで検索SC-100試験概要
- SC-100予想試験 □ SC-100シュミレーション問題集 □ SC-100試験勉強書 □ ウェブサイト▶ www.goshiken.com ◀ から ➡ SC-100 □ を開いて検索し、無料でダウンロードしてくださいSC-100予想試験
- Microsoft SC-100 Exam | SC-100トレーリングサンプル - SC-100試験製品の無料ダウンロード □ □ www.passtest.jp □ を開いて ⇒ SC-100 ◀ を検索し、試験資料を無料でダウンロードしてくださいSC-100予想試験
- SC-100問題例 □ SC-100問題と解答 □ SC-100無料ダウンロード □ □ ⇒ www.goshiken.com ◀ を入力して ➡ SC-100 □ を検索し、無料でダウンロードしてくださいSC-100資格勉強

