

F5CAB1日本語版参考書、F5CAB1難易度



無料でクラウドストレージから最新のCertShiken F5CAB1 PDFダンプをダウンロードする：https://drive.google.com/open?id=1wAQbiJFSYAovUm4dQu0Uhb6gcYsgba_

IT業種が新しい業種で、経済発展を促進するチェーンですから、極めて重要な存在だということを良く知っています。CertShikenの F5のF5CAB1試験トレーニング資料は高度に認証されたIT領域の専門家の経験と創造を含めているものです。その権威性は言うまでもありません。あなたはCertShikenの学習教材を購入した後、私たちは一年間で無料更新サービスを提供することができます。

F5 F5CAB1 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• BIG IP 管理 コントロールプレーン管理：このセクションでは、システム管理者のスキルを評価し、BIG IP が構成・管理されるコントロールプレーンの管理について学習します。ユーザーアカウント、ロール、デバイス設定、構成管理の操作、そして日常的な管理タスクのためのグラフィカルインターフェースとコマンドラインの使用が含まれます。
トピック 2	• BIG IP管理データプレーン概念：このセクションでは、ネットワーク管理者のスキルを評価し、BIG IPがデータプレーン上のアプリケーショントラフィックをどのように処理するかを網羅します。トラフィックフロー、主要なデータバスコンポーネント、ロードバランシングの基本概念、セキュリティおよびパフォーマンス機能がユーザートラフィックに与える影響などについて理解を深めます。
トピック 3	• BIG IP管理 インストール、初期設定、アップグレード：この試験セクションでは、システム管理者のスキルを評価し、BIG IPシステムの導入と保守に関するライフサイクルタスクを網羅します。プラットフォームのインストール、初期セットアップの実行、ライセンスの適用、基本的なネットワーク設定、ソフトウェアのアップグレードとホットフィックスの計画と実行などが含まれます。
トピック 4	• BIG IP管理データプレーン構成：このセクションでは、システム管理者のスキルを評価し、データプレーンの動作を制御するBIG IPオブジェクトの構成について学習します。設計要件に従ってアプリケーションが確実に効率的に配信されるように、仮想サーバー、プール、ノード、モニター、プロファイルの設定に重点を置きます。
トピック 5	• BIG IP 管理サポートとトラブルシューティング：この試験セクションでは、ネットワーク管理者のスキルを評価し、BIG IP の運用に影響を与える一般的な問題の特定と解決方法を網羅します。ログ、統計、診断ツール、基本的なトラブルシューティング手法を用いて、正常なトラフィックフローを回復し、安定したアプリケーション配信を維持することに重点が置かれます。

F5 F5CAB1試験の準備方法 | 権威のあるF5CAB1日本語版参考書試験 | 更新するBIG-IP Administration Install, Initial Configuration, and Upgrade 難易度

F5CAB1試験問題の継続的な刷新により、当社は大きな市場シェアを占めています。強力な研究センターを構築し、F5CAB1トレーニングガイドでより良い仕事をするために強力なチームを所有しています。F5これまで、F5CAB1学習教材に関する多くの特許を取得しています。一方で、当社は改修の恩恵を受けています。お客様は当社の製品を選択する可能性が高くなります。一方、私たちが投資したお金は有意義なものであり、F5CAB1試験の新しい学習スタイルを刷新するのに役立ちます。

F5 BIG-IP Administration Install, Initial Configuration, and Upgrade 認定 F5CAB1 試験問題 (Q34-Q39):

質問 # 34

The Configuration Utility of a BIG-IP device is currently accessible via its management IP 10.53.1.245 from all VLANs.

The BIG-IP Administrator needs to restrict access so only hosts from the 10.0.0.0/24 subnet can access the Configuration Utility. Which TMSH command accomplishes this?

- A. (tmsh)# modify /ltn httpd allow replace-all-with {10.0.0.0/24}
- **B. (tmsh)# modify /sys httpd allow replace-all-with {10.0.0.0/24}**
- C. (tmsh)# create /net acl MGMT.HTTP rule add { (permit tcp 10.0.0.0 0.0.0.255 host 10.53.1.245 http) }
- D. (tmsh)# create /net acl MGMT.HTTP rule add { (permit tcp 10.0.0.0/24 10.53.1.245 http) (deny ip any any http) }

正解: B

解説:

BIG-IP controls access to the web-based Configuration Utility (TMUI) through the /sys httpd allowlist. This parameter specifies which client IPs or subnets may initiate HTTP/HTTPS connections to the management interface.

To restrict TMUI access to only the 10.0.0.0/24 subnet:

* The correct method is to modify the HTTPD allow list so that it contains only this subnet.

* This requires replacing the entire current list with the new subnet using:

modify /sys httpd allow replace-all-with {10.0.0.0/24}

This ensures that only clients within 10.0.0.0/24 can reach the Configuration Utility.

Why the other options are incorrect:

* Options A and C create network ACL objects under /net acl, which apply to data-plane traffic, not management-plane TMUI access. TMUI access is not controlled by LTM ACLs but by the HTTPD allow directive.

* Option B is incorrect syntax and references /ltn httpd, which is not the proper object; the correct hierarchy is /sys httpd.

Thus, only modifying the /sys httpd allowlist achieves the required restriction.

質問 # 35

The BIG-IP Administrator wants to manage the newly built F5 system through an in-band Self-IP.

The administrator has configured a VLAN and Self-IP and can ping the IP from their workstation, but cannot access the system via SSH or HTTPS.

What port lockdown settings should the BIG-IP Administrator use to allow management access on the Self-IP?

(Choose two.)

- **A. The Self-IP port lockdown behavior could be adjusted to Allow Management**

- B. The Self-IP port lockdown behavior could be adjusted to Allow All
- **C. The Self-IP port lockdown behavior could be adjusted to Allow Mgmt**
- D. The Self-IP port lockdown behavior could be adjusted to Allow Default

正解: A、C

解説:

Self-IPs include a security feature called Port Lockdown, which restricts which services respond on that Self-IP.

By default, Self-IPs block management access (SSH and HTTPS/TMUI), meaning an administrator cannot manage the device through in-band Self-IPs unless explicitly allowed.

Allow Mgmt / Allow Management

These settings enable only the management services required for administrative access, specifically:

* SSH (22)

* HTTPS/TMUI (443)

These options allow secure administration without opening unnecessary ports.

Why these are correct:

- * They provide only the essential access for management.
- * They follow F5 security best practices when using in-band admin access.
- * They do not expose all services, reducing the attack surface.

Why the other options are incorrect:

A). Allow Default

- * This allows only a minimal set of system-required ports (e.g., failover, config sync), not SSH or HTTPS.
- * Administrator access would still fail.

B). Allow All

- * Opens all ports on the Self-IP, which is not secure.
- * Exposes services that should remain restricted.

Therefore, Allow Mgmt / Allow Management are the correct choices.

質問 # 36

A BIG-IP Administrator is using Secure Copy Protocol (SCP) to transfer a TMOS image to the BIG-IP system in preparation for an upgrade.

To what directory should the file be transferred?

- A. /var/images/
- B. /local/images/
- **C. /shared/images/**

正解: C

解説:

BIG-IP systems require all ISO images (base TMOS images and HotFix images) to be stored in a specific directory used for software installation:

/shared/images/

This directory:

- * Is the only supported location from which the BIG-IP software installation system validates and installs ISO files
- * Is accessible by both the GUI and TMSH installers
- * Has adequate storage space allocated specifically for images
- * Is part of the shared partition that persists across reboots

When transferring images via SCP, the administrator must copy them directly into /shared/images/ so that:

- * The GUI (System # Software Management # Available Images) can detect the image
- * TMSH install software image commands can reference it

Other directories such as /local/images/ or /var/images/ are not valid storage paths for software images.

質問 # 37

Refer to the exhibit.

An organization has purchased a BIG-IP license that includes all available modules but has chosen to provision only the modules they require.

The exhibit displays the current resource allocation from the System # Resource Provisioning page.

Based on the information provided, which F5 modules have been provisioned?

- A. LTM, DNS, APM
- B. LTM, APM
- C. TMM, DNS, APS
- D. DNS, APM

正解: A

解説:

The exhibit shows the Current Resource Allocation for:

- * CPU
- * Disk
- * Memory

In particular, the Memory Allocation bar displays the modules that are currently provisioned.

Memory is the most reliable indicator because BIG-IP allocates memory only to modules that are actively provisioned.

From the exhibit:

- * MGMT(Management) - always present
- * TMM(Traffic Management Microkernel) - indicates LTM is provisioned
- * GTM- this label indicates that the DNS module is provisioned (GTM = Global Traffic Manager, now called DNS)
- * APM- explicitly shown, indicating Access Policy Manager is provisioned

Therefore, the provisioned modules are:

- * LTM(implied by TMM allocation)
- * DNS/GTM
- * APM

This matches Option C: LTM, DNS, APM.

質問 # 38

A BIG-IP Administrator needs to purchase new licenses for a BIG-IP appliance.

The administrator needs to know:

- * Whether a module is licensed
- * The memory requirement for that module

Where should the administrator view this information in the System menu?

- A. Resource Provisioning
- B. Configuration Device
- C. Software Management
- D. Configuration OVSDB

正解: A

解説:

To understand:

- * Which modules are licensed
- * Which modules are provisioned
- * The resource requirements(CPU / RAM) of each module

The administrator uses:

System Resource Provisioning

This page displays:

- * All modules present in the license
- * Whether they are enabled or disabled
- * Required memory to activate each module
- * CPU and disk allocation information
- * Provisioning level options (None / Minimal / Nominal / Dedicated)

This is the exact location where BIG-IP administrators evaluate module capacity before enabling or purchasing licensing upgrades.

Why the other options are incorrect:

A). Configuration OVSDB

- * Used for network virtualization integrations, not licenses or modules.

B). Software Management

- * Used for software image installation, not licensing.

* Displays hostname, failover settings, device properties - not module resource requirements. Thus, module licensing and memory requirement data are found under Resource Provisioning.

• • • • •

F5CAB1難易度: <https://www.certshiken.com/F5CAB1-shiken.html>

- P.S. CertShikenがGoogle Driveで共有している無料かつ新しいF5CAB1ダンプ: <https://drive.google.com/open?id=17wAObiJFSYAovUm4dQu0Uhb6gcYsgba>