



BIG-IP LTM

簡単セットアップガイド (v14.1 対応)

F5 Networks Japan

目次

1.	はじめに	4
1.1.	LTM 動作概要	4
2.	L3 構成:スタンドアローン	5
2.1.	L3 構成:スタンドアローンイメージ	5
2.2.	L3 構成:スタンドアローンのネットワークサンプル	6
3.	初期設定	7
3.1.	管理ポートへの GUI アクセス	7
4.	ネットワーク設定	12
4.1.	VLAN の作成	12
4.2.	Self IP の設定	14
4.3.	ルーティングの設定	15
4.3.1.	デフォルトゲートウェイの設定	15
4.3.2.	サーバへのルーティング設定	16
5.	ロードバランシング設定	17
5.1.	HTTP (Port:80) のロードバランシング設定	17
5.1.1.	Pool の作成	17
5.1.2.	HTTP(80)の Virtual Server の作成	19
5.1.3.	クライアントからの HTTP アクセス	20
5.2.	パーシステンス設定	21
5.2.1.	送信元 IP アドレスによるパーシスタンス	21
5.2.2.	クライアントからの HTTP アクセス	21
5.2.3.	Cookie によるパーシスタンス	21
5.2.4.	クライアントからの HTTP アクセス	21
5.3.	HTTPS (Port:443) のロードバランシング設定: [パターン A] 簡易的な設定方法	22
5.3.1.	HTTPS パーチャルサーバの設定	22
5.3.2.	クライアントからの HTTPS アクセス	23
5.4.	HTTPS (Port:443) のロードバランシング設定: [パターン B] 認証局発行の証明書の利用	24
5.4.1.	サーバ証明書の準備	24
5.4.2.	秘密鍵とサーバ証明書のインポート	25
5.4.3.	クライアント PC の設定	29
5.4.3.1.	認証局の証明書のインポート	29
5.4.3.2.	クライアント PC の hosts ファイルの編集	34
5.4.4.	クライアントからの HTTPS アクセス	36
6.	iRules の使い方	37
6.1.	User-Agent を取得する	37
6.1.1.	User-Agent ヘッダによる制御	37
6.1.2.	BIG-IP への SSH アクセス	40
6.1.3.	User-Agent をログ上で確認	41
6.2.	User-Agent 毎にアクセス先 Pool Member を変える	41
7.	UCS の取得	43
8.	コンフィグの初期化(全消去)	45
8.1.	BIG-IP への SSH アクセス	45
8.2.	コンフィグの初期化	45
9.	UCS のリストア	46
10.	QKview の取得	50
11.	L3 構成:冗長化	52
11.1.	L3 構成:冗長化イメージ	52
11.2.	L3 構成:冗長化のネットワークサンプル	53
11.3.	Active 機(bigXXX.f5jp.local)の設定	54
11.3.1.	HA VLAN の設定	54
11.3.2.	HA VLAN の IP 設定	54
11.3.3.	Device の設定	55
11.3.4.	時刻同期(NTP)設定	57
11.4.	Standby 機(bigYYY.f5jp.local)の設定	59

11.4.1.	VLAN 設定	59
11.4.2.	Self-IP 設定	59
11.4.3.	Device 設定	60
11.4.4.	NTP 設定	60
11.5.	デバイストラスト設定 (Active 機(bigXXX.f5jp.local)側から実施)	61
11.6.	デバイスグループの設定	64
11.7.	トラフィックグループの設定	65
11.7.1.	トラフィックグループの確認	65
11.7.2.	Floating IP の設定	66
11.7.3.	Virtual Server と Traffic-Group の紐付け(確認)	67
11.7.4.	Traffic Group に紐付けられたオブジェクトの確認	67
11.8.	ConfigSync	68
11.9.	Traffic-group-1 の Active/Standby の切替え	69
11.9.1.	Traffic-group-1 の Active/Standby の切替え	69
11.9.2.	クライアントからの接続確認	70
12.	コマンドラインによる設定	71
12.1.	コンフィグの初期化(全消去)	71
12.2.	初期設定	72
12.3.	ネットワークの設定	72
12.4.	Pool と Virtual Server の設定	73
12.4.1.	HTTP(80)用 Pool と VS	73
12.4.2.	SSH 用 VS	75
12.5.	コンフィグの保存	75
12.6.	冗長化設定	76
12.6.1.	1号機(XXX)での設定	76
12.6.2.	2号機(YYY)の設定	77
12.6.3.	再び1号機(XXX)からの実行	77
12.7.	[参考]root のパスワード変更	78
12.8.	show コマンドのサンプル	79
12.8.1.	コネクションテーブルの確認	79
12.8.2.	ハードウェアに関わる情報(CPU の詳細やシリアル番号等)の確認	80
12.8.3.	各パーティションの OS の確認	80
12.8.4.	現在利用中の OS バージョンの確認	80
12.8.5.	Virtual Server の状態確認	80
13.	おわりに	81

1. はじめに

本セットアップガイドにて BIG-IP Local Traffic Manager (以下、LTM) の設定方法についてご案内します。

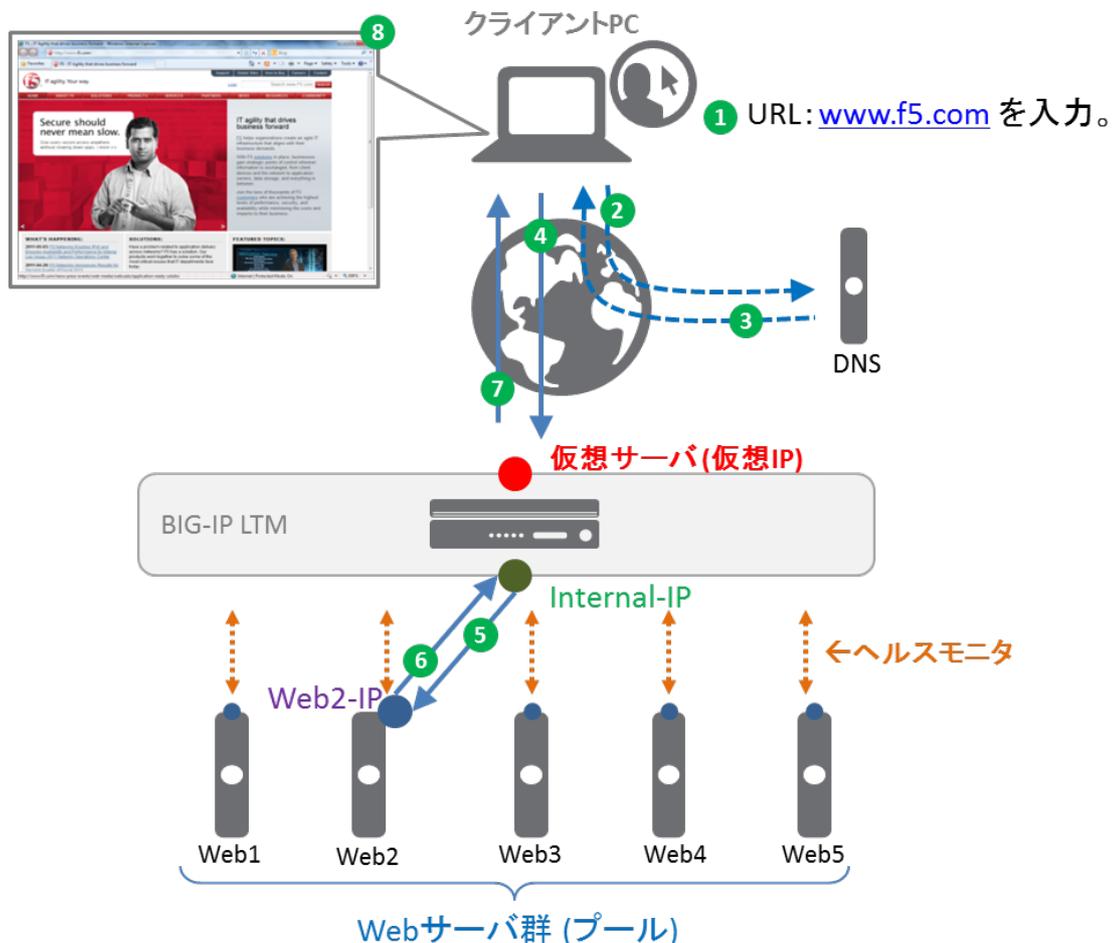
BIG-IP LTM はサーバ負荷分散をはじめとして SSL のオフロードやコンテンツスイッチング、また圧縮やキャッシュなど多彩な機能を搭載し、アプリケーションサービスの可用性を高め快適なユーザエクスペリエンスを提供するのに役立ちます。

本ガイドでは、BIG-IP LTM をご購入いただいてすぐに使い始められるように、サーバ負荷分散を実現するのに必要となる典型的なセットアップ手法を豊富なスクリーンショットを交えて解説します。

これにより、ネットワークを構成し、クライアントーサーバ間での簡単な WEB の負荷分散環境を構築することができますので、セットアップ時の手引きとしてご活用ください。また、管理用のマネージメント IP アドレスは設定済みである前提としております。

1.1. LTM 動作概要

LTM は以下のような流れで動作します。

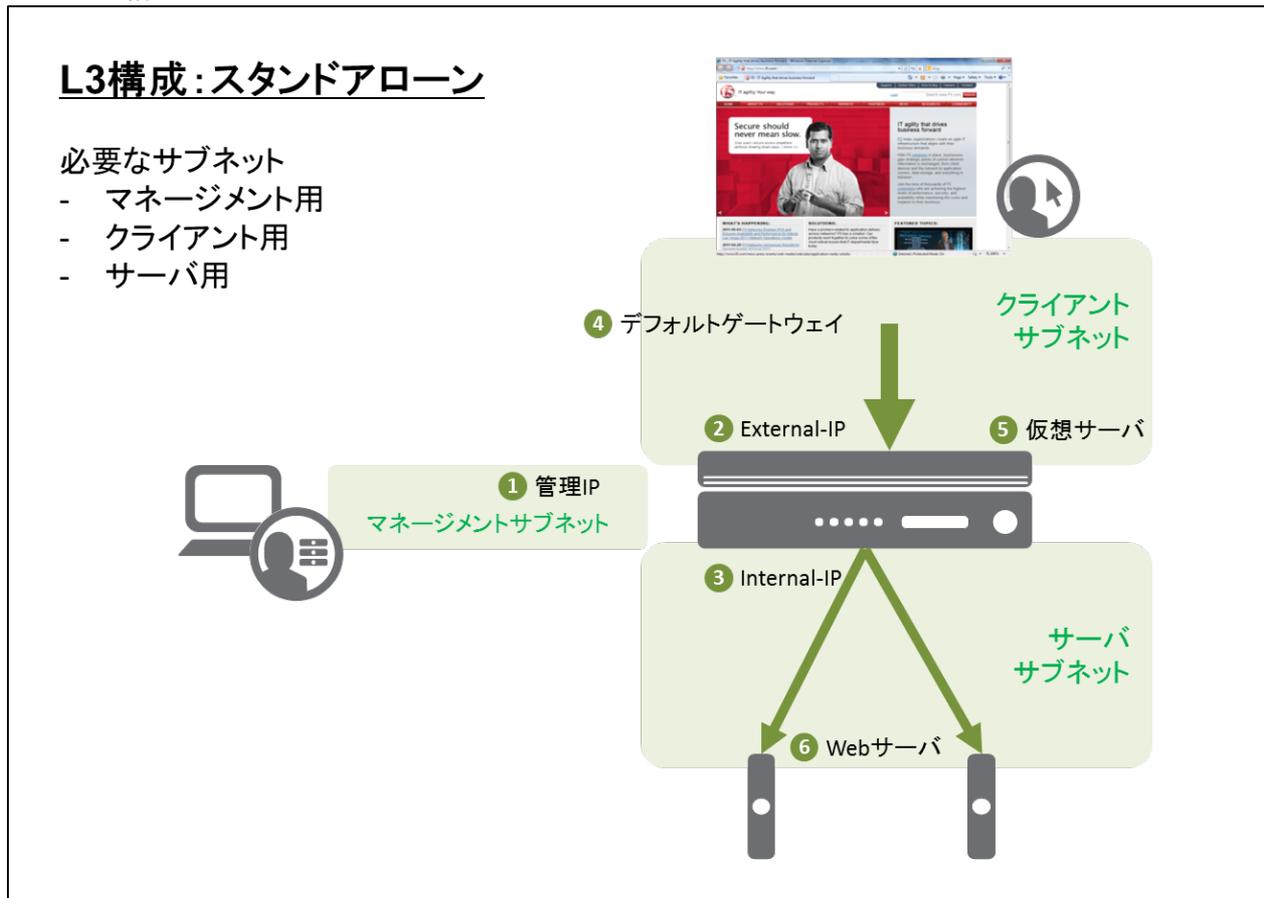


○ BIG-IP LTM は、Web サーバ群に対して、定期的なヘルスマonitoringにて稼働監視を行っている。

- ① クライアントが Web ブラウザに、URL: www.f5.com を入力。
- ② クライアント PC は、www.f5.com の IP アドレスを解決するために、DNS クエリを送信。
- ③ DNS サーバから www.f5.com の IP アドレスを得る。
- ④ Web ブラウザは、その IP アドレス(仮想サーバ)宛に HTTP リクエストを送信。
- ⑤ BIG-IP LTM は、Web サーバ群から 1 台(この例では Web2)を選び、宛先アドレスを変換し、HTTP リクエストを転送。
- ⑥ Web サーバ(Web2)は、その HTTP リクエストに対する HTTP レスポンスを送信。
- ⑦ その HTTP レスポンスを受けとった BIG-IP LTM は、送信元アドレス変換を行い、その HTTP レスポンスをクライアント PC へ転送。
- ⑧ www.f5.com の Web 画面が表示される。

2. L3 構成:スタンドアローン

2.1. L3 構成:スタンドアローンイメージ



上図①～⑥の IP アドレスが必要になりますので、あらかじめご用意ください。

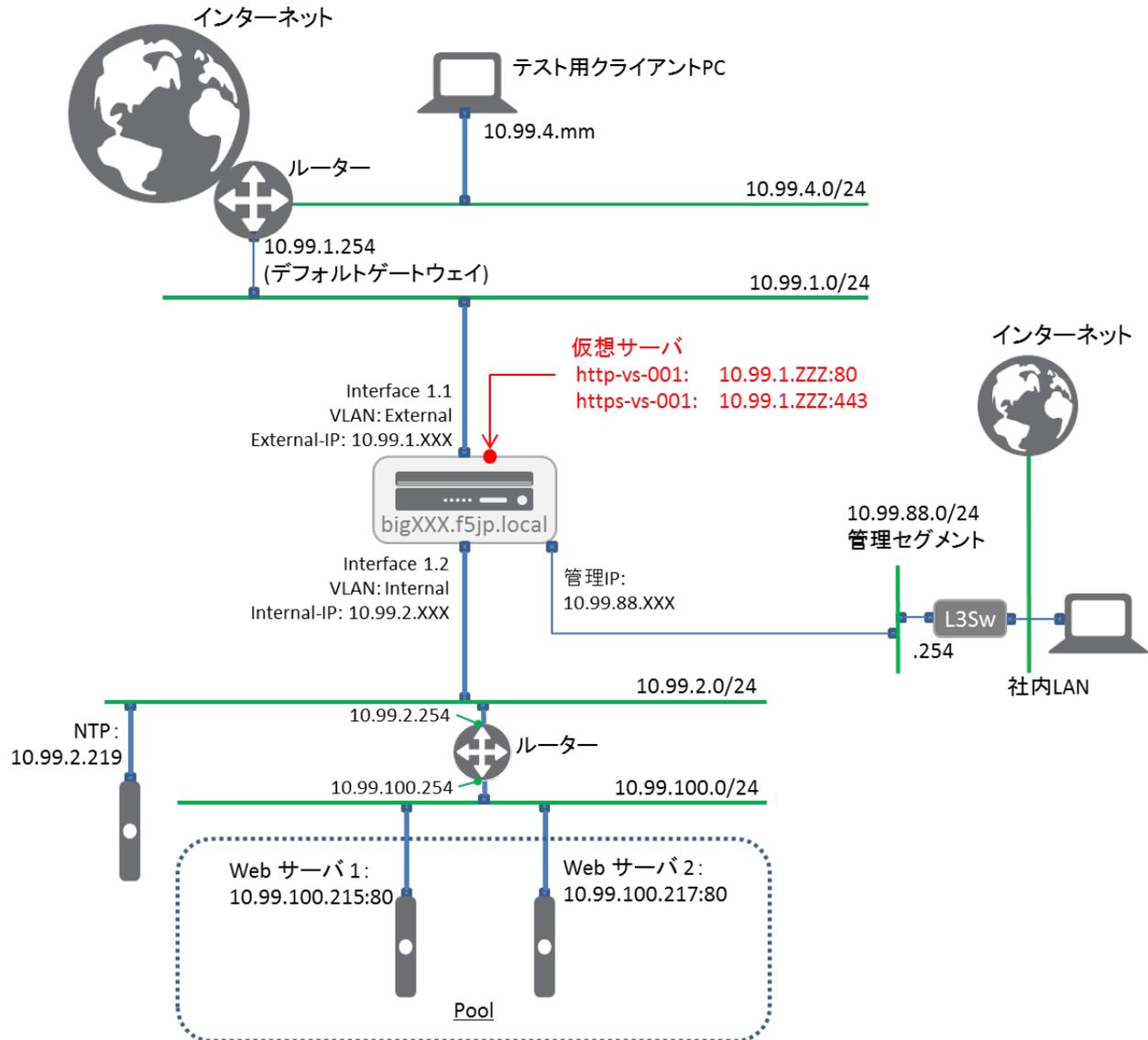
なお、工場出荷時には①⑦⑧は以下がプリセットされております。

- ① 192.168.1.245/24
- ⑦ default
- ⑧ admin

項目	名前(サンプル)	値(サンプル)
- ホスト名	bigXXX.f5jp.local	
① 管理 IP	---	10.99.88.XXX/24
② External インタフェース	external	10.99.1.XXX
③ Internal インタフェース	internal	10.99.2.XXX
④ デフォルトゲートウェイ		10.99.1.254
⑤ 仮想サーバアドレス	http-vs-001 https-vs001	10.99.1.ZZZ:80 10.99.1.ZZZ:443
⑥ Web サーバ 1 のアドレス:ポート	---	10.99.100.215:80
Web サーバ 2 のアドレス:ポート	---	10.99.100.217:80
⑦ CLI パスワード	---	ID/Password : root/default
⑧ GUI パスワード	---	ID/Password : admin/admin

2.2. L3 構成: スタンドアロンのネットワークサンプル

まずは、冗長化しない状態の L3 構成を想定して、1 台のみ設定していきます。



BIG-IP の Virtual Server は 10.99.1.ZZZ:80 と 10.99.1.ZZZ:443 の 2 つを設定します。

プールメンバーは、以下 2 つです。

10.99.100.215:80
10.99.100.217:80

BIG-IP のデフォルトゲートウェイは、インターネット方向を想定したルーター: 10.99.1.254 に設定します。

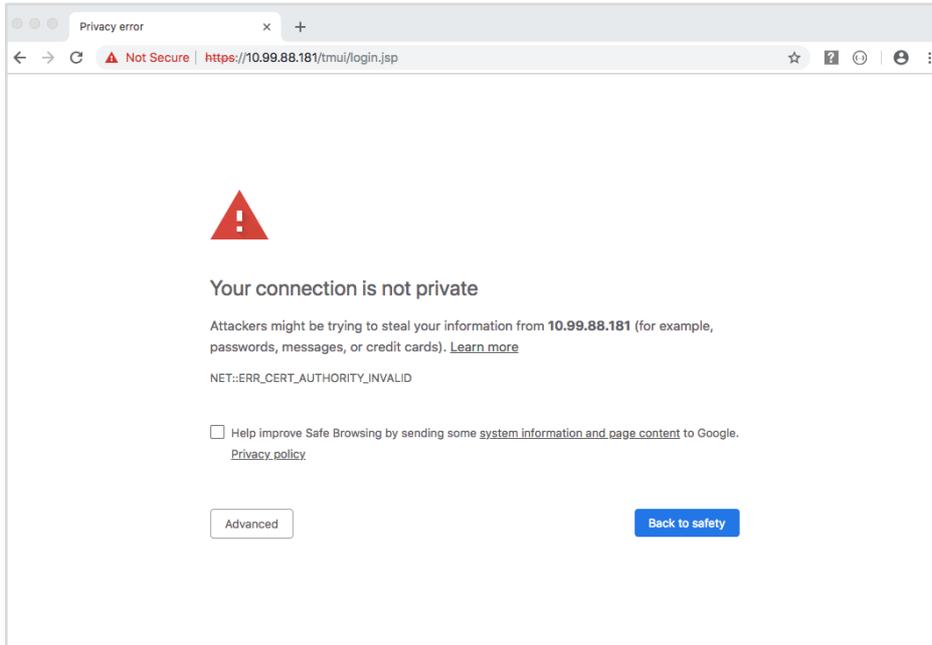
Web サーバのデフォルトゲートウェイは、BIG-IP の Internal インタフェース宛(10.99.2.XXX)に設定します。

動作確認は、テスト用に設置した PC(図中の「テスト用クライアント」)から行うこととします。

3. 初期設定

3.1. 管理ポートへの GUI アクセス

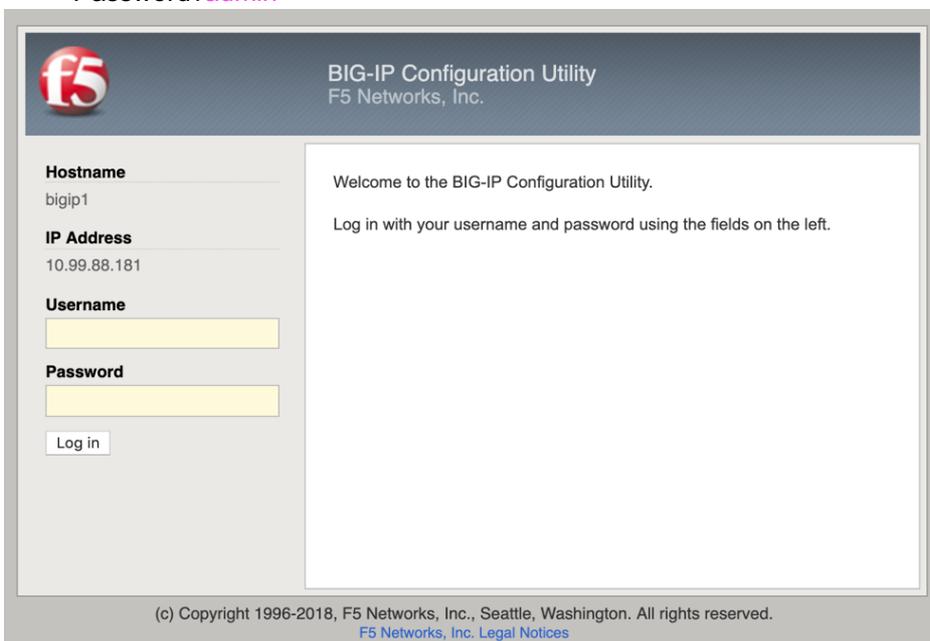
- (1) 管理用 PC から、設定した BIG-IP の管理 IP アドレスへ、HTTPS でアクセスします。デフォルトの証明書は、正式に取得した証明書ではないため、以下のような画面が現れますが、「続行する」を選択してください。



- (2) ログイン画面が現れますので、以下のデフォルトの ID と Password でログインしてください。

ID: **admin**

Password: **admin**



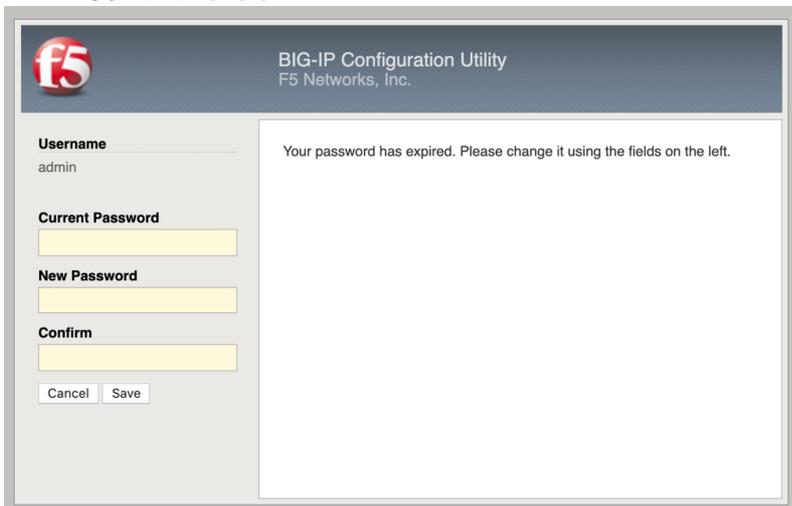
- (3) バージョン 14.0 より、デフォルトで BIG-IP のセキュアパスワードポリシーが有効となっています。パスワードポリシーを変更しない限り、v13.0 以前のデフォルトパスワードは利用できません。

F5LAB では以下のように設定し、Save ボタンを押します。

Current Password: **admin**

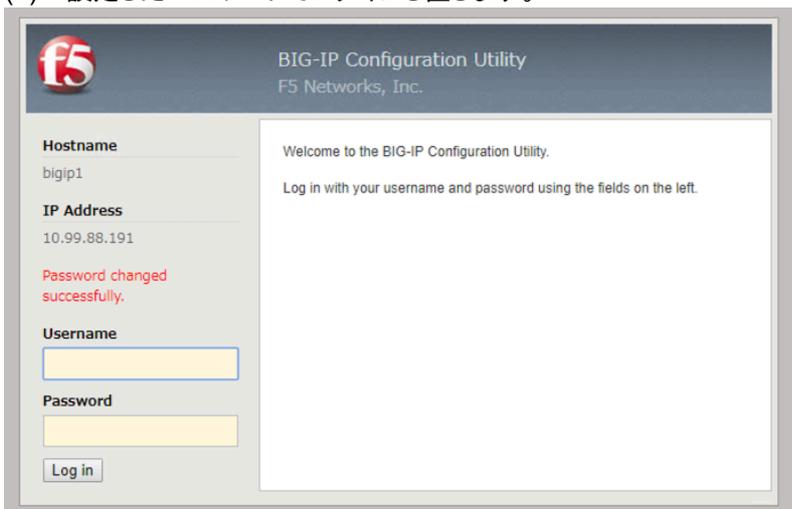
New Password: **ilovef5**

Confirm: **ilovef5**



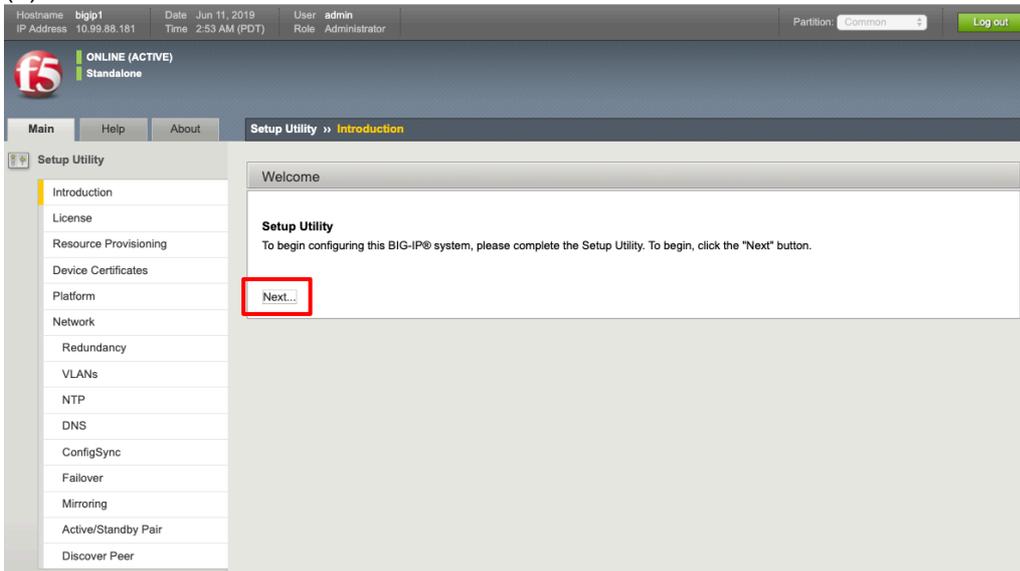
The screenshot shows the 'BIG-IP Configuration Utility' interface. On the left, there are input fields for 'Username' (admin), 'Current Password', 'New Password', and 'Confirm'. Below these fields are 'Cancel' and 'Save' buttons. On the right, a message states: 'Your password has expired. Please change it using the fields on the left.'

- (4) 設定したパスワードでログインし直します。



The screenshot shows the 'BIG-IP Configuration Utility' login screen. On the left, there are fields for 'Hostname' (bigip1), 'IP Address' (10.99.88.191), 'Username', and 'Password'. A red message says 'Password changed successfully.' Below the fields is a 'Log in' button. On the right, a message says: 'Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left.'

- (5) 「Next」ボタンを押します。



The screenshot shows the main menu of the 'BIG-IP Configuration Utility'. At the top, there is a status bar with 'Hostname: bigip1', 'Date: Jun 11, 2019', 'Time: 2:53 AM (PDT)', 'User: admin', 'Role: Administrator', 'Partition: Common', and a 'Log out' button. Below this is a navigation bar with 'Main', 'Help', and 'About' tabs. The 'Setup Utility' section is active, showing a 'Welcome' message and a 'Next...' button highlighted with a red box. The 'Next...' button is located in the 'Setup Utility' section, which also contains a message: 'To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.'

(6) ライセンス画面が出ます。「Next」ボタンを押します。(ライセンスが BIG-IQ License Manager で管理されている場合は、Next ボタンは押せませんので、Resource Provisioning をクリックして下さい。)

~中略~

ライセンスが BIG-IQ License Manager で管理されている場合は、Next ボタンは押せませんので、Resource Provisioning をクリックして下さい。

(7) プロビジョニング画面がでますが、デフォルトで LTM が選択されているので、そのまま「Next」ボタンを押します。

Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1264
Carrier Grade NAT (CGNAT)	Disabled	Licensed	0	0
Local Traffic (LTM)	Nominal	Licensed	0	2400
Application Security (ASM)	None	Licensed	20	1492
Fraud Protection Service (FPS)	None	N/A	12	544
Global Traffic (DNS)	None	Licensed	0	148
Link Controller (LC)	None	Unlicensed	0	148
Access Policy (APM)	None	Licensed	12	494
Application Visibility and Reporting (AVR)	None	Licensed	16	576
Policy Enforcement (PEM)	None	Unlicensed	16	1223
Advanced Firewall (AFM)	None	Licensed	16	1058
Application Acceleration Manager (AAM)	None	Unlicensed	32	2050
Secure Web Gateway (SWG)	None	Time limited module expires after: Jan 25, 2019	24	4096
iRules Language Extensions (iRulesLX)	None	Licensed	0	748
URLDB Minimal (URLDB)	None	Time limited module expires after: Jan 25, 2019	36	2048

(8) SSL 証明書の確認がなされますが、デフォルトのまま、「Next」ボタンを押します。

Hostname: bigip1, Date: Jun 11, 2019, User: admin, Role: Administrator, Partition: Common, Log out

ONLINE (ACTIVE) Standalone

Setup Utility » Device Certificates

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- Fingerprint
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

General Properties

Name	server.crt
Certificate Subject(s)	localhost.localdomain, MyCompany

Certificate Properties

Public Key Type	RSA
Public Key Size	2048 bits
Expires	May 27 2029 10:28:27 GMT
Version	3
Serial Number	a1:96:8f:4d:d6:55:1f:08
Fingerprint	SHA256/2B:45:66:8B:8D:6B:1D:EB:1F:4E:7A:E5:9C:F2:C2:6F:17:0F:79:1F:11:06:0D:A3:B3:51:22:EF:BE:EB:45:C2
Subject	Common Name: localhost.localdomain Organization: MyCompany Division: MyOrg Locality: Seattle State Or Province: WA Country: --
Issuer	Self
Email	root@localhost.localdomain
Subject Alternative Name	

Back Renew... Import... **Next...**

(9) ホスト名、タイムゾーン、Root のパスワードを設定します。「Next」ボタンを押します。

Hostname: bigip1, Date: Jun 11, 2019, User: admin, Role: Administrator, Partition: Common, Log out

ONLINE (ACTIVE) Standalone

Activation Complete
Configure your platform.

Setup Utility » Platform

Setup Utility

- Introduction
- License
- Resource Provisioning
- Device Certificates
- Platform
- Network
- Redundancy
- VLANs
- NTP
- DNS
- ConfigSync
- Failover
- Mirroring
- Active/Standby Pair
- Discover Peer

General Properties

Management Port 1 Configuration: Automatic (DHCP) Manual

Management Port 1: IP Address/prefix: 10.99.88.181, Network Mask: 255.255.255.0 (/24), Management Route: 10.99.88.90

Management Port 2: IP Address/prefix: , Network Mask: , Management Route: Select...

Host Name: big181.f5jp.local **ホスト名を FQDN で指定**

Host IP Address: Use Management Port IP Address

Time Zone: Japan **タイムゾーンを指定**

User Administration

Root Account: Disable login
Password:, Confirm:

SSH Access: Enabled

SSH IP Allow: * All Addresses

Back **Next...**

Root ユーザのパスワードを指定 ilovef5

(10)この後、Standard Network Configuration の「Next」を押すことでウィザード形式にて冗長化も含めた設定が可能ですが、ここではスタンドアローン構成にするため、Advanced Network Configuration の「Finished」ボタンを押します。

The screenshot shows the Fortinet Configuration Utility interface. At the top, there is a status bar with the following information: Hostname: big181.f5.jp.local, IP Address: 10.99.88.181, Date: Jun 11, 2019, Time: 7:22 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. Below the status bar, there is a navigation menu with tabs for Main, Help, and About. The current page is titled "Setup Utility » Network". On the left side, there is a "Setup Utility" sidebar with a list of configuration options: Introduction, License, Resource Provisioning, Device Certificates, Platform, Network (highlighted), Redundancy, VLANs, NTP, DNS, ConfigSync, Failover, Mirroring, Active/Standby Pair, and Discover Peer. The main content area is titled "Standard Network Configuration" and contains the following text: "Create a standard network configuration by configuring these features:" followed by a list of features: Redundancy, VLANs, NTP, DNS, Config Sync, Failover, Mirroring, and Peer Device Discovery (for Redundant Configurations). Below this list is a "Next..." button. Underneath, there is a section titled "Advanced Network Configuration" with the text: "Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility." The "Finished" button is highlighted with a red box.

4. ネットワーク設定

VLAN や VLAN インタフェースへの IP 設定（Self-IP 設定）およびルーティング設定を行います。

4.1. VLAN の作成

まず、VLAN を作成します。「Network」 → 「VLAN」で表示された画面の右上にある「Create」ボタンを押します。

(1) External VLAN を設定します。

The screenshot shows the f5 network configuration interface for creating a new VLAN. The interface is in Japanese and includes a top status bar with system information, a left sidebar with navigation options, and a main configuration area. The 'VLANs' menu item in the sidebar is highlighted with a red box. The main configuration area is titled 'New VLAN...' and contains several sections: 'General Properties' with a 'Name' field set to 'external' (highlighted with a red box and a red annotation '名前(任意)を指定'), 'Resources' with an 'Interfaces' list containing '1.1 (untagged)' (highlighted with a red box and a red annotation 'Interface: 1.1、Tagging: Untagged を選択し、Add をクリック'), 'Configuration: Basic' with 'Source Check' and 'MTU' fields, and 'sFlow' with 'Polling Interval' and 'Sampling Rate' fields. At the bottom, there are 'Cancel', 'Repeat', and 'Finished' buttons, with 'Finished' highlighted by a red box.

(2) Internal VLAN を設定します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 1:16 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » VLANs : VLAN List » New VLAN...

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
Network

Interfaces
Routes
Self IPs
Packet Filters
Quick Configuration
Trunks
Tunnels
Route Domains
VLANs

General Properties

Name: internal 名前(任意)を指定

Description:

Tag:

Resources

Interfaces

Interface: 1.1
Tagging: Untagged
Add
1.2 (untagged) Interface:1.2 を、
Tagging:Untagged を選択し、
Add をクリック

Edit Delete

Configuration: Basic

Source Check

MTU: 1500

sFlow

Polling Interval: Default
Sampling Rate: Default

Cancel Repeat **Finished**

(3) 設定後は、以下の状態になります。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 1:20 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » VLANs : VLAN List

VLAN List VLAN Groups

* Search Create...

<input checked="" type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	external		4094	1.1		Common
<input type="checkbox"/>	internal		4093	1.2		Common

Delete...

4.2. Self IP の設定

BIG-IP に設定した VLAN それぞれに対して、IP アドレスを設定していきます。

この IP アドレスのことを“Self IP”と呼びます。

「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押します。

(1) External VLAN の Self IP を設定します。

The screenshot shows the 'New Self IP...' configuration page in the BIG-IP web interface. The configuration table is as follows:

Field	Value	Annotation
Name	external-ip	名前(任意)
IP Address	10.99.1.181 10.99.1.XXX (F5 ラボの場合)	IP アドレス
Netmask	255.255.255.0	サブネットマスク
VLAN / Tunnel	external	VLAN を設定
Port Lockdown	Allow None	このアドレス上でのサービス (SSH/GUI アクセス等) を拒否
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)	
Service Policy	None	

Buttons: Cancel, Repeat, Finished

Left sidebar: Network > Self IPs

(2) Internal VLAN の Self IP を設定します。

The screenshot shows the 'New Self IP...' configuration page in the BIG-IP web interface. The configuration table is as follows:

Field	Value	Annotation
Name	internal-ip	名前(任意)
IP Address	10.99.2.181 10.99.2.XXX (F5 ラボの場合)	IP アドレス
Netmask	255.255.255.0	サブネットマスク
VLAN / Tunnel	internal	VLAN を設定
Port Lockdown	Allow Default	このアドレス上でのサービス (SSH/GUI アクセス等) を許可
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)	
Service Policy	None	

Buttons: Cancel, Repeat, Finished

Left sidebar: Network > Self IPs

(3) 一覧では、以下のような状態になります。

The screenshot shows the F5 configuration interface. At the top, it displays system information: Hostname (big181.f5jp.local), IP Address (10.99.88.181), Date (Jun 27, 2019), Time (1:25 PM (JST)), User (admin), and Role (Administrator). The interface is in the 'Network >> Self IPs' section. A table titled 'Self IP List' is shown with the following data:

Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
external-ip		10.99.1.181	255.255.255.0	external	traffic-group-local-only	Common
internal-ip		10.99.2.181	255.255.255.0	internal	traffic-group-local-only	Common

4.3. ルーティングの設定

4.3.1. デフォルトゲートウェイの設定

(1) 「Network」 → 「Routes」で表示された画面の右上にある「Add」ボタンを押します。以下の通り入力し、「Finished」を押します。

The screenshot shows the F5 configuration interface in the 'Network >> Routes >> New Route...' section. The 'Properties' dialog box is open with the following fields and values:

- Name: Default-GW (Red box with note: 任意の名称を入力)
- Description: (Empty)
- Destination: 0.0.0.0 (Red box with note: 左記の通りに入力)
- Netmask: 0.0.0.0 (Red box with note: 左記の通りに入力)
- Resource: Use Gateway...
- Gateway Address: IP Address (dropdown), 10.99.1.254 (Red box with note: ゲートウェイのアドレスを入力)
- MTU: (Empty)

At the bottom of the dialog, there are buttons for 'Cancel', 'Repeat', and 'Finished' (highlighted with a red box).

4.3.2. サーバへのルーティング設定

(1) BIG-IP からオフィス内サーバ: 10.99.100.0/24 へ到達するためのルーティングも同様に設定します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 12:44 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » Routes » New Route...

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
Network

Properties

Name	Server-Route	任意の名称を入力
Description		
Destination	10.99.100.0	左記の通りに入力
Netmask	255.255.255.0	
Resource	Use Gateway...	
Gateway Address	IP Address 10.99.2.254	ゲートウェイのアドレスを入力
MTU		

Cancel Repeat **Finished**

(2) 設定後は、以下の状態になります。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 12:46 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » Routes

Route List

Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
Default-GW		Default IPv4		Partition Default Route Domain	Gateway	10.99.1.254	Common
Server-Route		10.99.100.0	255.255.255.0	Partition Default Route Domain	Gateway	10.99.2.254	Common

Delete...

5. ロードバランシング設定

5.1. HTTP (Port:80)のロードバランシング設定

5.1.1. Pool の作成

まず、Pool から作成します。Pool は、ロードバランス対象の複数サーバの集合を指します。

(1) 「Local Traffic」 → 「Pools」で表示された画面の右上にある「Create」ボタンを押します。

Configuration: Basic

Name: http-pool-01 名前(任意)を指定

Description:

Health Monitors:

Active	Available
/Common/http	/Common/gateway_icmp
	http_head_f5
	https
	https_443

プールメンバーへのヘルスマニターを選択

Resources:

Load Balancing Method: Round Robin ロードバランシング方式を選択

Priority Group Activation: Disabled

New Members:

Node Name: (Optional)
Address: 10.99.100.217
Service Port: 80 HTTP

Web サーバの Address と Service Port を入力し Add ボタンを押しメンバーに追加

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.99.100.215	10.99.100.215	80		0
10.99.100.217	10.99.100.217	80		0

Buttons: Cancel Repeat **Finished**

(2) Pool が作成されると、以下の状態になります。

Local Traffic » Pools : Pool List

Pool List Statistics

Search Create...

Status	Name	Description	Application	Members	Partition / Path
ONLINE	http-pool-01			2	Common

Delete...

- (3) 作成した「http-pool-01」をクリックし、「Members」タブをクリックします。以下のように、Status がグリーンであればヘルスマonitorが成功しています。

The screenshot shows the F5 BIG-IP configuration page for the 'http-pool-01' pool. The 'Members' tab is selected, and the 'Current Members' table shows two active members with green status indicators.

Load Balancing

Load Balancing Method: Round Robin
Priority Group Activation: Disabled

Current Members

<input type="checkbox"/>	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
<input type="checkbox"/>	●	10.99.100.215:80	10.99.100.215	80		No	1	0 (Active)	0	Common
<input type="checkbox"/>	●	10.99.100.217:80	10.99.100.217	80		No	1	0 (Active)	0	Common

Buttons: Enable, Disable, Force Offline, Remove

5.1.2. HTTP(80)の Virtual Server の作成 次に Virtual Server (HTTP:Port80)を作成します。

- (1) 「Local Traffic」 → 「Virtual Servers」で表示された画面の右上にある「Create」ボタンを押して表示された画面で、以下のように設定します。

Hostname: big181.f5.jp.local | Date: Jun 27, 2019 | User: admin | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Main | Help | About | Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...

Statistics | iApps | DNS | Local Traffic | Network Map | **Virtual Servers** | Policies | Profiles | Ciphers | iRules | Pools | Nodes | Monitors | Traffic Class | Address Translation | Acceleration | Device Management | Shared Objects | Network | System

General Properties

Name: http-vs-001 名前(任意)を指定

Description: [Empty]

Type: Standard

Source Address: Host (selected) | Address List

Destination Address/Mask: Host (selected) | Address List: 10.99.1.81 (F5 ラボの場合)
仮想 IP アドレスとサービスポート:80 を指定

Service Port: Port (selected) | Port List: 80 | HTTP

Notify Status to Virtual Address: [checked]

State: Enabled

Configuration: Basic

Protocol: TCP

Protocol Profile (Client): tcp

Protocol Profile (Server): (Use Client Profile)

HTTP Profile (Client): http HTTP Profile を選択

HTTP Profile (Server): (Use Client Profile)

HTTP Proxy Connect Profile: None

FTP Profile: None

RTSP Profile: None

SSL Profile (Client): [Empty]

SSL Profile (Server): [Empty]

SMTSP Profile: None

POP3 Profile: None

Client LDAP Profile: None

Server LDAP Profile: None

Service Profile: None

SMTP Profile: None

VLAN and Tunnel Traffic: All VLANs and Tunnels

Source Address Translation: Auto Map Auto Map を選択

～中略～

Resources

iRules: [Empty]

Policies: [Empty]

Default Pool: http-pool-01 先ほど設定した Pool を選択

Default Persistence Profile: None

Fallback Persistence Profile: None

Cancel | Repeat | **Finished**

(2) Status がグリーンであれば、正常に動作していることを示します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 2:32 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Local Traffic » Virtual Servers : Virtual Server List

Virtual Server List Virtual Address List Statistics

Search Create...

Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input checked="" type="checkbox"/>	http-vs-001			10.99.1.81	80 (HTTP)	Standard	Edit...	Common

Enable Disable Delete...

5.1.3. クライアントからの HTTP アクセス

(1) テスト用クライアントから、作成した Virtual Server へ Web ブラウザでアクセスし、Web 画面が表示されることを確認します。

(2) 「Statistics」 → 「Module Statistics」 → 「Local Traffic」タブをクリックします。「Statistics Type」のプルダウンメニューから、「Pools」を選択します。それぞれの Web サーバの、Bits, Packets 等のカウントがアップしていることを確認し、ロードバランシングが正常に行われていることを確認します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 2:34 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Statistics » Module Statistics : Local Traffic » Pools

Traffic Summary DNS Local Traffic Subscriber Management Network Memory System

Dashboard
Module Statistics
Performance Reports

Statistics Type Pools
Data Format Normalized
Auto Refresh Disabled Refresh

Status	Pool	Pool Member	Partition / Path	Bits		Packets		Connections		Requests		Request Queue	
				In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age
<input checked="" type="checkbox"/>	http-pool-01		Common	10.2K	36.2K	10	10	0	2	2	2	0	0
<input type="checkbox"/>		10.99.100.215:80	Common	4.9K	18.4K	5	5	0	1	1	1	0	0
<input type="checkbox"/>		10.99.100.217:80	Common	5.3K	17.8K	5	5	0	1	1	1	0	0

Reset

カウンタをリセットしたい場合には、「Status」左横のチェックボックスにチェックを入れて、「Reset」ボタンを押します。

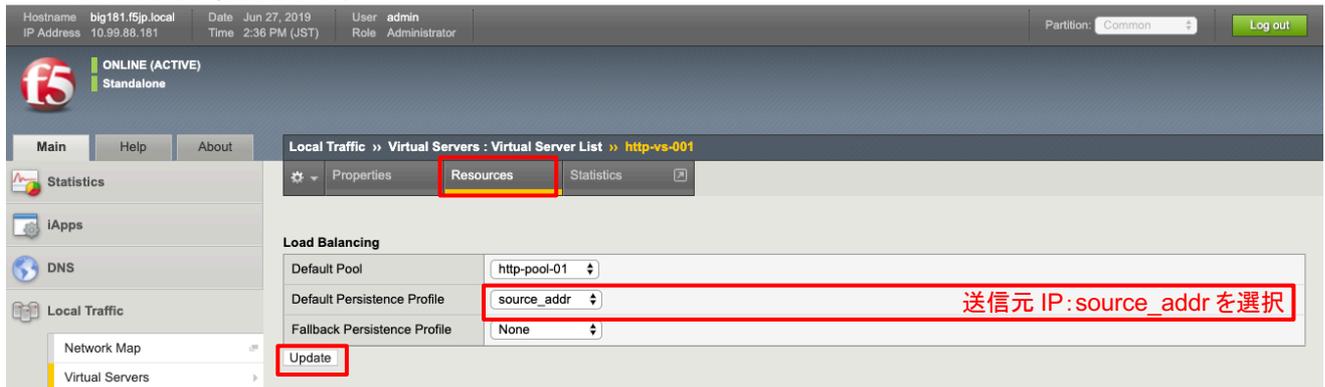
5.2. パーシステンス設定

ロードバランシングメソッドに従って1つのサーバに振り分けられた後、継続して同じサーバへアクセスしたい、という要望があります(例:お買いもの系サイト、インターネットバンキング)。このような要望を実現する機能をパーシステンスと呼びます。

本ガイドでは、送信元 IP アドレスパーシステンスと Cookie のパーシステンス設定を行います。

5.2.1. 送信元 IP アドレスによるパーシステンス

- (1) 「Local Traffic」→「Virtual Servers」で表示されたバーチャルサーバ: http-vs-001 を選択し、Resources タブをクリックすると、以下の画面が表示されます。
以下のように設定します。



5.2.2. クライアントからの HTTP アクセス

テスト用クライアントから、作成した Virtual Server へ Web ブラウザでアクセスし、Web 画面が表示されることを確認します。Statistics を見て、ロードバランシングされず同じサーバへのみ振り分けられていることを確認します。

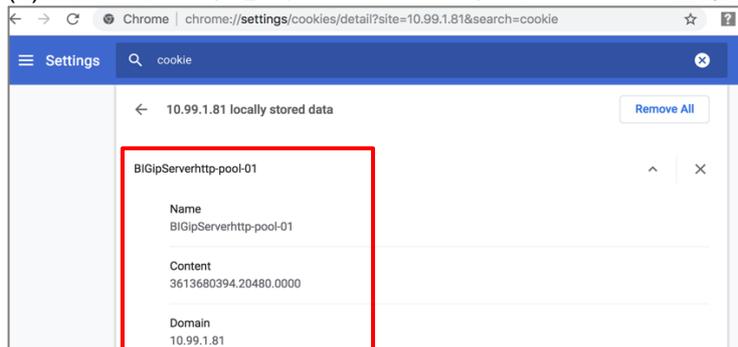
5.2.3. Cookie によるパーシステンス

- (1) 以下のように設定します。



5.2.4. クライアントからの HTTP アクセス

- (1) 5.2.2.と同内容を確認し、ブラウザの設定で cookie が登録されていることを確認します。



<ご参考> Chrome v75 の場合の確認手順
設定 > 詳細設定 > プライバシーとセキュリティ
> サイトの設定 > Cookie > すべての Cookie と
サイトデータを表示

確認ができれば、次項以降のテストのために、Persistence Profile を Virtual Server の設定からはずします。

5.3. HTTPS(Port:443)のロードバランシング設定:[パターン A]簡易的な設定方法

HTTPS 仮想サーバとして動作することだけを確認するのであれば、デフォルトで用意されている SSL Profile を使うことで、容易に実施できます。

5.3.1. HTTPS バーチャルサーバの設定

(1) 「Local Traffic」 → 「Virtual Servers」で表示された画面の右上にある「Create」ボタンを押し手表示された画面で以下のように設定します。

The screenshot shows the 'New Virtual Server' configuration page in the F5 GUI. The 'General Properties' section includes fields for Name (https-vs-001), Description, Type (Standard), Source Address (Host), Destination Address/Mask (10.99.1.81), Service Port (443, HTTPS), and State (Enabled). The 'Configuration' section includes Protocol (TCP), Protocol Profile (Client: tcp, Server: Use Client Profile), HTTP Profile (Client: http, Server: Use Client Profile), HTTP Proxy Connect Profile (None), FTP Profile (None), RTSP Profile (None), SSL Profile (Client: clientssl, Server: apm-default-serverssl), SMTP Profile (None), POP3 Profile (None), Client LDAP Profile (None), Server LDAP Profile (None), Service Profile (None), VLAN and Tunnel Traffic (All VLANs and Tunnels), and Source Address Translation (Auto Map).

～中略～

The screenshot shows the 'Resources' section of the configuration page. It includes fields for iRules, Policies, Default Pool (http-pool-01), Default Persistence Profile (None), and Fallback Persistence Profile (None). At the bottom, there are buttons for 'Cancel', 'Repeat', and 'Finished'.

5.3.2. クライアントからの HTTPS アクセス

- (1) テスト用クライアントから、作成した Virtual Server(HTTPS)へアクセスし、正常に SSL 処理が行われることを確認します。
- (2) 「Statistics」 → 「Module Statistics」 → 「Local Traffic」タブをクリックします。
「Statistics Type」のプルダウンメニューから、「Pools」を選択します。
それぞれの Web サーバの、Bits, Packets 等のカウントがアップしていることを確認し、ロードバランシングが正常に行われていることを確認します。

The screenshot shows the FortiGate web interface. The top navigation bar includes 'Main', 'Help', and 'About'. The 'Statistics' menu is expanded to 'Module Statistics : Local Traffic', with 'Local Traffic' selected. The 'Statistics Type' dropdown is set to 'Pools'. The table below shows the following data:

Status	Pool	Pool Member	Partition / Path	Bits		Packets		Connections			Requests		Request Queue	
				In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age	
<input type="checkbox"/>	http-pool-01		Common	99.5K	200.1K	100	90	0	5	17	17	0	0	
<input type="checkbox"/>		10.99.100.215:80	Common	52.1K	88.9K	52	46	0	3	9	9	0	0	
<input type="checkbox"/>		10.99.100.217:80	Common	47.4K	111.1K	48	44	0	2	8	8	0	0	

カウンタをリセットしたい場合には、「Status」左横のチェックボックスにチェックを入れて、「Reset」ボタンを押します。

5.4. HTTPS(Port:443)のロードバランシング設定:[パターン B]認証局発行の証明書の利用

認証局で署名されたサーバ証明書をインポートして利用する方法を記載します。

5.4.1. サーバ証明書の準備

一般的には、BIG-IP の GUI で CSR と秘密鍵を生成し、CSR を認証局(例:ペリサイン等)に送付します。その CSR に対して、認証局が署名を行うことでサーバ証明書が完成します。そのサーバ証明書を返送してもらい、インポートします。

本ガイドでは簡易的に、秘密鍵ファイルとサーバ証明書の両方がすでに存在しているものとし、両方をインポートする手順とします。

(F5 ラボの場合)リモートデスクトップ接続した PC のデスクトップ上にある、以下のフォルダを開いてください。



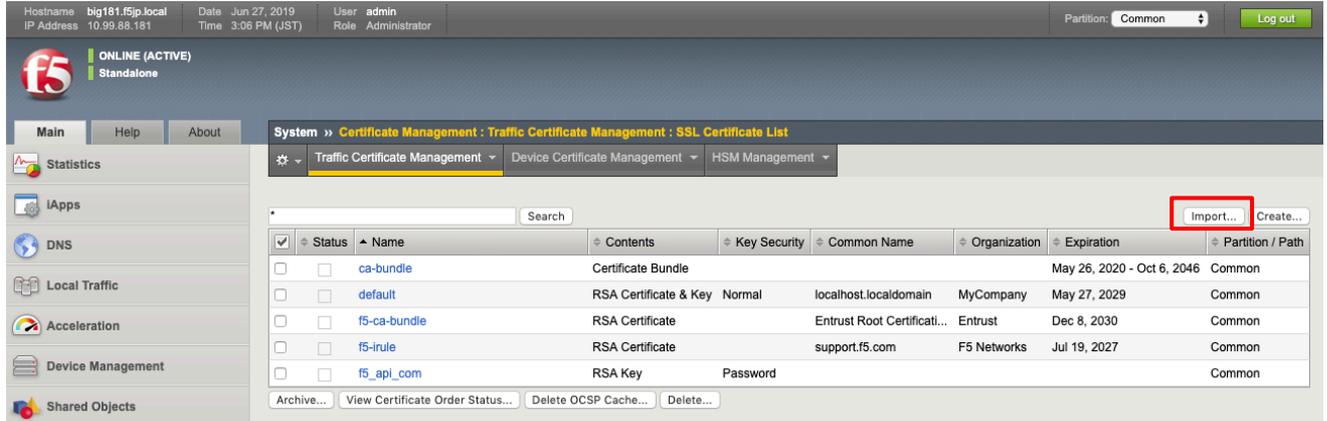
このフォルダ内の以下 2 つのファイルを使用します。

- ① 秘密鍵ファイル: **abcCompany-key.pem**
- ② サーバ証明書ファイル: **abcCompany-cert.pem**

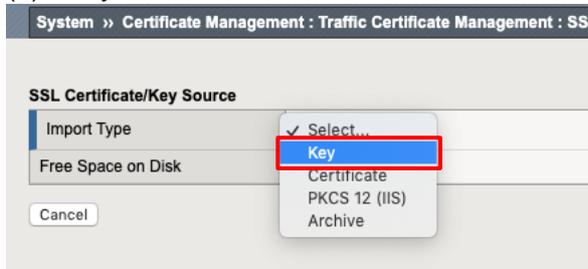
5.4.2. 秘密鍵とサーバ証明書のインポート

(1) まず、サーバの秘密鍵をインポートします。

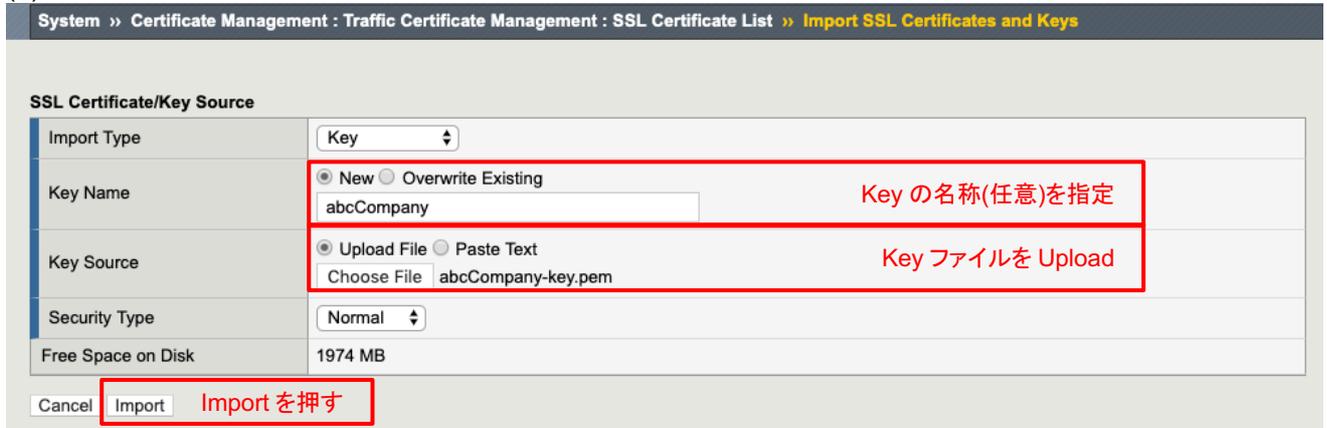
「System」 → 「Certificate Management」 → 「Traffic Certificate Management」 → 「SSL Certificate List」で表示された画面右上の「Import」ボタンを押します。



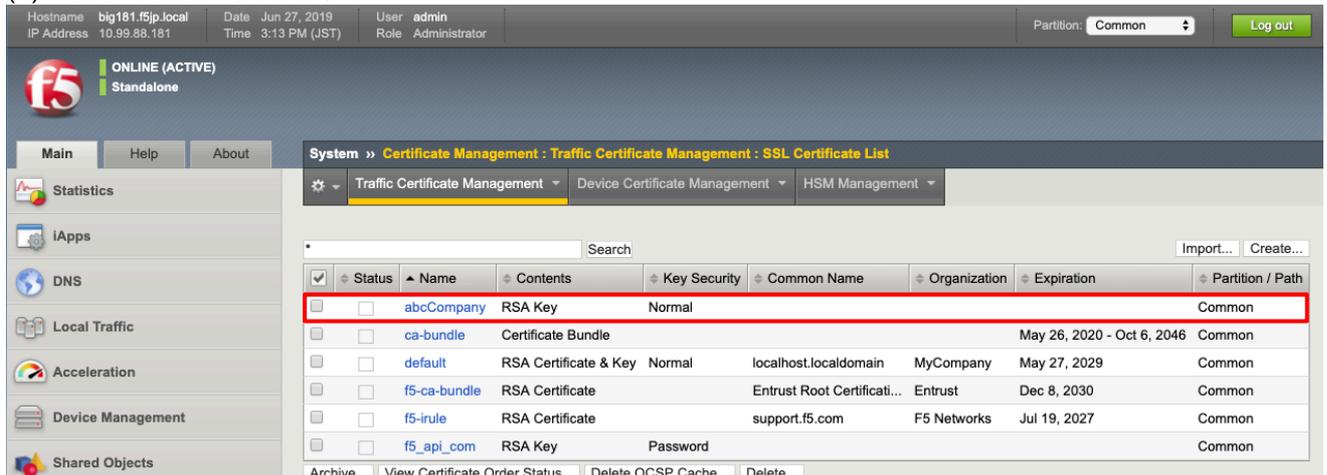
(2) Key を選択します。



(3) 以下のように設定します。



(4) 以下の状態になります。



(5) 次に、サーバ証明書をインポートします。

インポートした秘密鍵をクリックすると、以下の画面が現れます。「Import」ボタンを押します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 3:17 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System >> Certificate Management : Traffic Certificate Management : SSL Certificate List >> abcCompany

Statistics iApps DNS Local Traffic Acceleration

General Properties

Name	abcCompany
Partition / Path	Common
Certificate Subject(s)	No certificate

Import... Create... Import を押す

(6) 以下のように設定して、インポートします。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 3:20 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System >> Certificate Management : Traffic Certificate Management : SSL Certificate List >> /Common/abcCompany

Statistics iApps DNS Local Traffic Acceleration

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	/Common/abcCompany
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text Choose File abcCompany-cert.pem
Free Space on Disk	1974 MB

Cancel Import Import を押す

サーバ証明書を指定

(7) サーバ証明書がインポートされた状態です。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 3:24 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System >> Certificate Management : Traffic Certificate Management : SSL Certificate List

Statistics iApps DNS Local Traffic Acceleration Device Management Shared Objects

Traffic Certificate Management Device Certificate Management HSM Management

Search Import... Create...

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input checked="" type="checkbox"/>	abcCompany	RSA Certificate & Key	Normal	www.abc-company.com	ABC-Company	Jul 26, 2021	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle				May 26, 2020 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	May 27, 2029	Common
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 8, 2030	Common
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 19, 2027	Common
<input type="checkbox"/>	f5_api_com	RSA Key	Password				Common

Archive... View Certificate Order Status... Delete OCSP Cache... Delete...

(8) Client SSL Profile を作ります。

「Local Traffic」 → 「Profiles」 → 「SSL」 → 「Client」で表示された画面右上の「Create」ボタンを押すと、以下の画面が表示されますので、以下のように設定します。

Hostname big181.f5.jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 3:27 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

Statistics
iApps
DNS
Local Traffic

General Properties
Name abc-company-ssl-profile 名前(任意)を指定
Parent Profile clientssl

Configuration: Basic Custom
Certificate Key Chain /Common/abcCompany /Common/abcCompany
Add Edit Delete
右端のチェックボックスをチェックし、別 Window にて作成したサーバ証明書と Key を選択「Add」ボタンを押す

OCSP Stapling
Notify Certificate Status to Virtual Server
Proxy SSL
Proxy SSL Passthrough

Add SSL Certificate Key Chain

Certificate abcCompany
Key abcCompany
Chain None
Passphrase

Add Cancel

(9) 「Finished」ボタンを押すと、以下のようになります。

Hostname big181.f5.jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 3:29 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Local Traffic » Profiles : SSL : Client

Services Content Persistence Protocol SSL Authentication
Message Routing Other

Search Create...

Name	Application	Parent Profile	Partition / Path
<input checked="" type="checkbox"/> abc-company-ssl-profile		clientssl	Common
<input type="checkbox"/> clientssl		(none)	Common
<input type="checkbox"/> clientssl-insecure-compatible		clientssl	Common
<input type="checkbox"/> clientssl-secure		clientssl	Common
<input type="checkbox"/> crypto-server-default-clientssl		clientssl	Common
<input type="checkbox"/> splitsession-default-clientssl		clientssl	Common
<input type="checkbox"/> wom-default-clientssl		clientssl	Common

Delete...

(10) [パターンA]で作成済みの Virtual Server:Port443 を開き、「SSL Profile (Client)」部分の設定を以下のように変更し、Update ボタンを押します。

The screenshot displays the F5 configuration interface for a Virtual Server named 'https-vs-001'. The 'General Properties' section shows the server is available and listening on port 443 for HTTPS. The 'Configuration' section is set to 'Basic'. In the 'SSL Profile (Client)' section, the 'Selected' list contains 'abc-company-ssl-profile', which is highlighted by a red box and a red text annotation '作成した SSL Profile を選択'. The 'Available' list includes several default profiles. The 'Update' button at the bottom of the configuration area is also highlighted with a red box.

~省略~

5.4.3. クライアント PC の設定

5.4.3.1. 認証局の証明書のインポート

(1) サーバ証明書を BIG-IP にインポートしただけでは不十分です。このままでは、まだ、以下の画面を見ることがになります。(例:Chrome)



この画面が出る理由は、この Web サイト (= BIG-IP の Virtual Server) のサーバ証明書に署名した認証局 (F5J-CA) の証明書が Web ブラウザにインポートされていないことが原因です。認証局の証明書が Web ブラウザに入っていないと、サーバ証明書の発行元をチェックすることができないためです。

この問題を回避するために、認証局 (F5J-CA) の証明書を、クライアント PC の Web ブラウザへインポートする必要があります。

リモートデスクトップ接続した PC のデスクトップ上にある、以下のフォルダを開いてください。



このフォルダ内の以下のファイルを利用します。

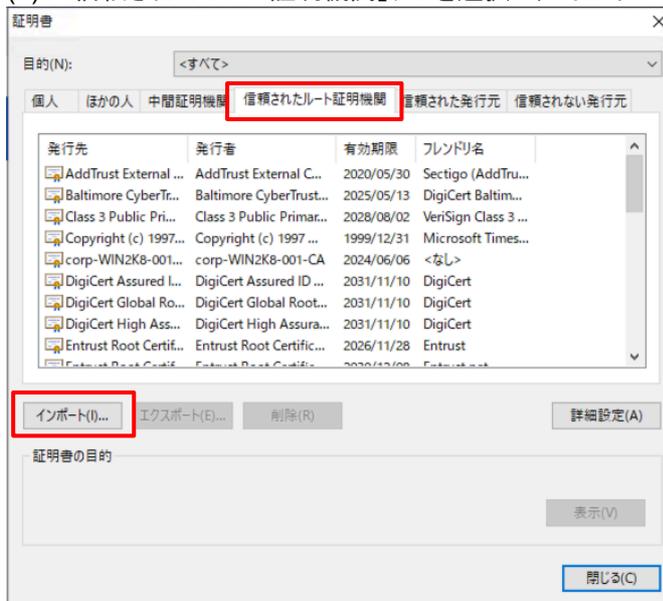
認証局ファイル: **cacert.pem**

以下の手順でクライアント PC の Web ブラウザ (例:Chrome) へインポートします。

(2) クライアント PC の Web ブラウザ（例: Chrome）へインポートします。Chrome の設定画面で、証明書の管理を選択します。



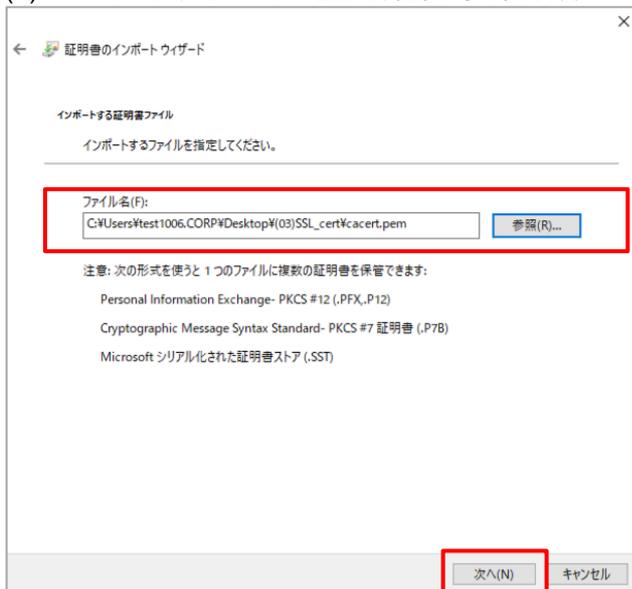
(3) 「信頼されたルート証明機関」タブを選択し、「インポート」ボタンを押して下さい。



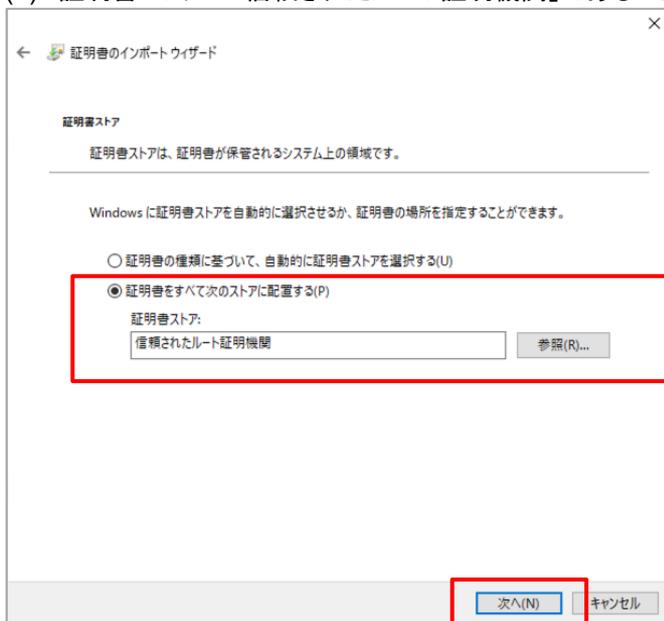
(4) 「次へ」を押して下さい。



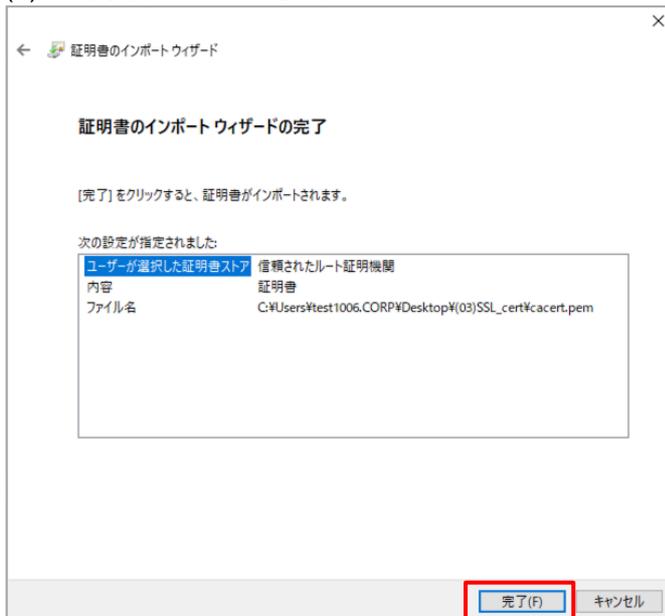
(5) インポートするファイルとして、認証局の証明書:cacert.pem を選び、「次へ」を押して下さい。



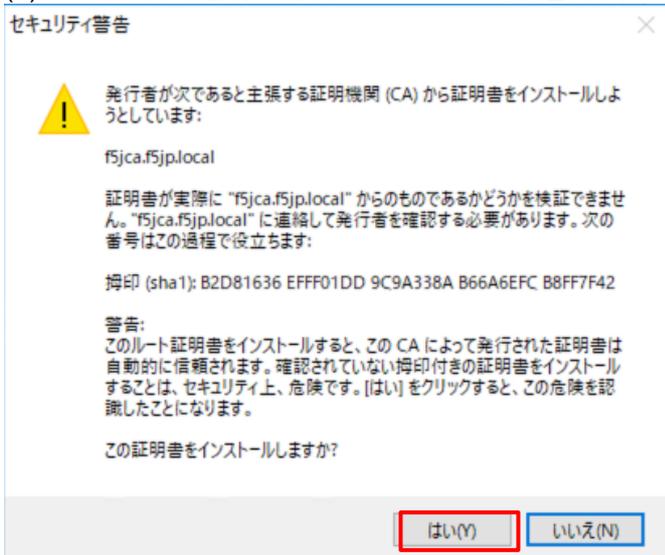
(6) 証明書ストアが「信頼されたルート証明機関」であることを確認し、「次へ」を押して下さい。



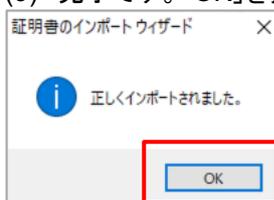
(7) 「完了」を押してください。



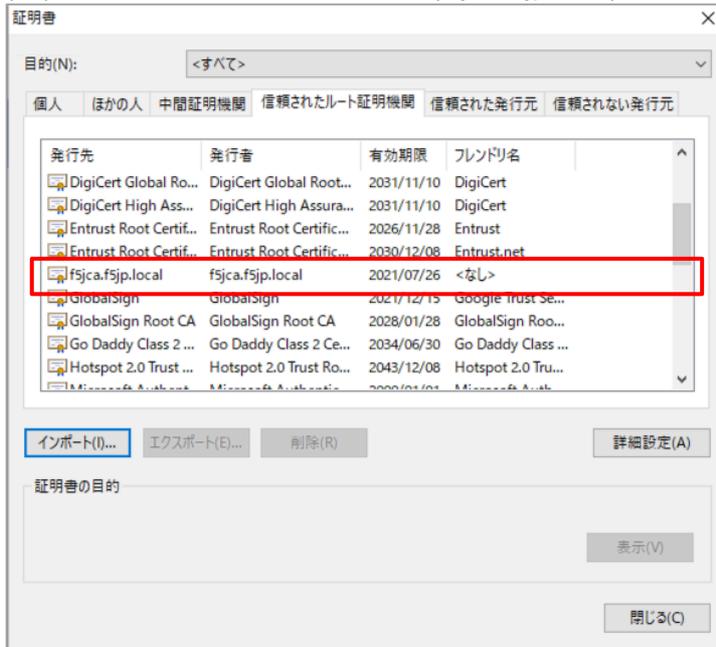
(8) セキュリティ警告に対し、ここでは「はい」を選択します。



(9) 完了です。「OK」を押してください。



(10) 「信頼されたルート証明機関」に、(f5jca.f5jp.local)のルート証明書がインポートされました。

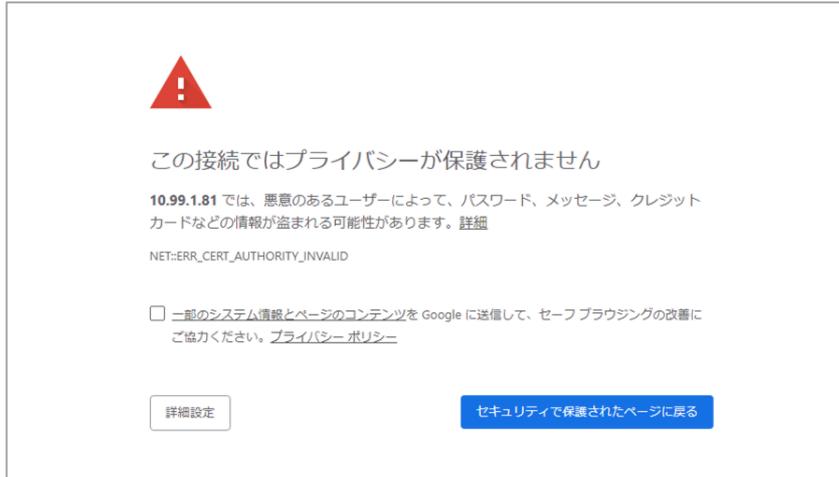


これで、「信頼されたルート証明機関」として、本ガイドの認証局 (F5J-CA) が登録されました。基本的にはこれで証明書のセキュリティ警告は表示されなくなります。

しかし、DNS による名前解決ができない環境においては、次のステップも必要です。

5.4.3.2. クライアント PC の hosts ファイルの編集

- (1) DNS による名前解決ができない環境の場合、URL として IP アドレスを入力することになります。この場合、クライアント PC へ認証局の証明書をインポートしても、まだ、以下の画面をみることになります。

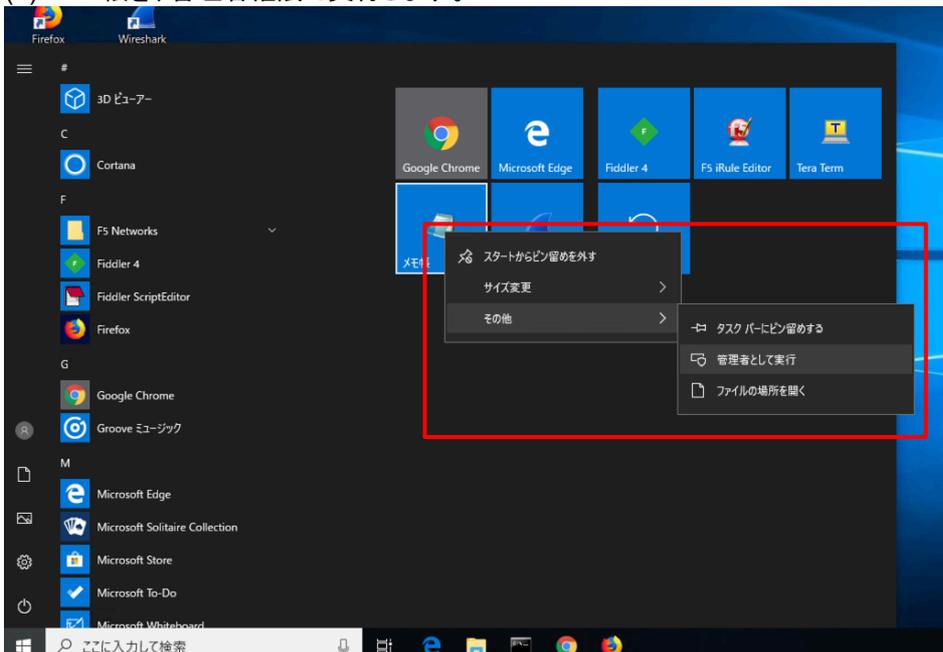


これは、Web サーバ(=Virtual Server)へアクセスして、Web サーバからサーバ証明書を受け取ったものの、サーバ証明書に記載された Common Name と、接続を要求した FQDN (≒URL) が一致しないことが原因です。

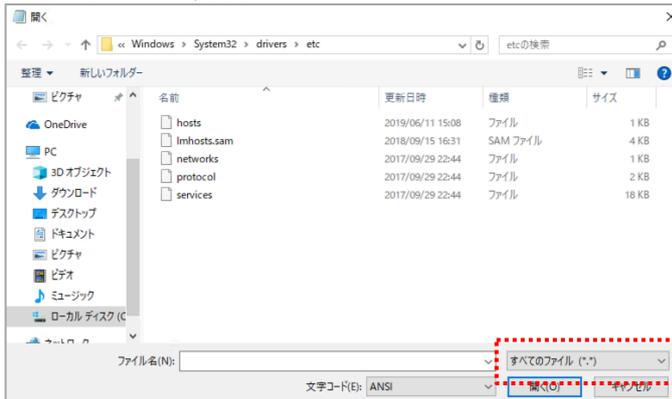
検証環境で比較的簡単に回避するためには、クライアント PC:Windows の hosts ファイルを編集することです。

本例では、サーバ証明書の Common Name は「www.abc-company.com」です。

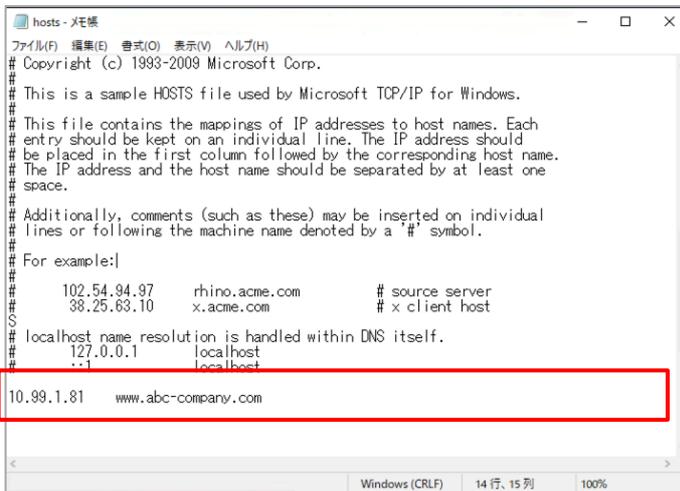
- (2) メモ帳を、管理者権限で実行します。



- (3) C:\Windows\System32\drivers\etc\hosts を編集します。
(「hosts」デフォルト状態では表示されないかもしれません。その場合は左下の「すべてのファイル (*.*)」を選択してください。)



※hosts に指定するアドレスは、ご自身で設定した Virtual Server の IP アドレスを指定してください。



Web ブラウザへ入力する URL は、IP アドレスではなく FQDN (<https://www.abc-company.com>) で入力します。

これで、SSL 証明書のセキュリティ警告を見ることなく、Web サーバ(Virtual Server) へ接続することができます。

5.4.4. クライアントからの HTTPS アクセス

- (1) テスト用クライアントから作成した Virtual Server (HTTPS)へアクセスし、正常に SSL 処理が行われることを確認します。
- (2) 「Statistics」 → 「Module Statistics」 → 「Local Traffic」タブをクリックします。
「Statistics Type」のプルダウンメニューから、「Pools」を選択します。
それぞれの Web サーバの、Bits, Packets 等のカウントがアップしていることを確認し、ロードバランシングが正常に行われていることを確認します。

The screenshot shows the F5 BIG-IP web interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains 'Statistics', 'iApps', 'DNS', 'Local Traffic', 'Acceleration', 'Device Management', and 'Shared Objects'. The main content area is titled 'Statistics >> Module Statistics : Local Traffic >> Pools'. Below this, there are tabs for 'Traffic Summary', 'DNS', 'Local Traffic', 'Subscriber Management', 'Network', 'Memory', and 'System'. The 'Local Traffic' tab is selected. Under 'Display Options', 'Statistics Type' is set to 'Pools'. Below that, there are options for 'Data Format' (Normalized) and 'Auto Refresh' (Disabled). A table displays traffic statistics for three pool members. The first row is highlighted with a red dashed box. The table has columns for Status, Pool, Pool Member, Partition / Path, Bits (In, Out), Packets (In, Out), Connections (Current, Maximum, Total), Requests (Total), and Request Queue (Depth, Maximum Age).

Status	Pool	Pool Member	Partition / Path	Bits In	Bits Out	Packets In	Packets Out	Connections Current	Connections Maximum	Connections Total	Requests Total	Request Queue Depth	Request Queue Maximum Age
<input checked="" type="checkbox"/>	http-pool-01		Common	44.6K	133.1K	39	39	0	4	7	7	0	0
<input type="checkbox"/>		10.99.100.215:80	Common	25.4K	76.0K	22	22	0	2	4	4	0	0
<input type="checkbox"/>		10.99.100.217:80	Common	19.2K	57.1K	17	17	0	2	3	3	0	0

カウンタをリセットしたい場合には、「Status」左横のチェックボックスにチェックを入れて、「Reset」ボタンを押します。

6. iRules の使い方

iRules はイベントベースのスクリプト言語で、アプリケーショントラフィック操作をカスタマイズ可能です。
(iRules の文法詳細に関しては、こちらのページをご参照下さい。<https://clouddocs.f5.com/api/irules/>)

iRules の作成は、BIG-IP のマネージメント管理画面(TMUI)、または iRules Editor、または F5 Editor Eclipse Plugin の何れかを利用します。

本ガイドでは TMUI の iRules 機能を使って、簡易的に、以下のような iRule を設定してみます。

「HTTP リクエストに含まれる User-Agent ヘッダによって、アクセスするサーバを変える」

具体的には、

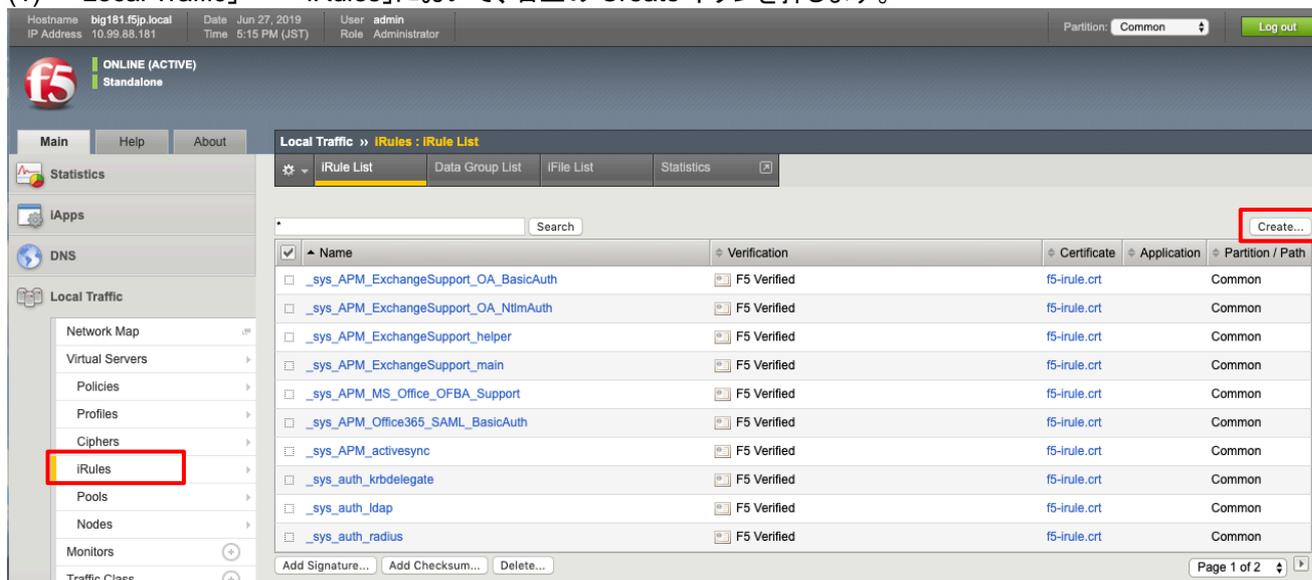
- ・ Firefox の場合は、 10.99.100.215:80 へ
 - ・ Internet Explorer の場合は 10.99.100.217:80 へ
- 接続する、というルールを作ってみます。

6.1. User-Agent を取得する

まず iRules を使って、User-Agent の値を取得してみます。

6.1.1. User-Agent ヘッダによる制御

(1) 「Local Traffic」 → 「iRules」において、右上の Create ボタンを押します。



The screenshot shows the F5 TMUI interface. At the top, there is a status bar with 'ONLINE (ACTIVE)' and 'Standalone'. The main navigation menu on the left includes 'Main', 'Help', 'About', 'Statistics', 'iApps', 'DNS', and 'Local Traffic'. Under 'Local Traffic', 'iRules' is highlighted with a red box. The main content area displays the 'iRule List' table. The table has columns for Name, Verification, Certificate, Application, and Partition / Path. A 'Create...' button is highlighted with a red box in the top right corner of the table area.

Name	Verification	Certificate	Application	Partition / Path
<input type="checkbox"/> _sys_APM_ExchangeSupport_OA_BasicAuth	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_OA_NtimAuth	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_helper	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_ExchangeSupport_main	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_MS_Office_OFBA_Support	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_Office365_SAML_BasicAuth	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_APM_activesync	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_auth_krbdelegate	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_auth_ldap	F5 Verified	f5-rule.crt		Common
<input type="checkbox"/> _sys_auth_radius	F5 Verified	f5-rule.crt		Common

- (2) User-Agent を、ログファイルへ出力する iRule を入力します。設定後、Finished ボタンを押します。

```
when HTTP_REQUEST {  
  log local0. "USER-AGENT is [string tolower [HTTP::header "User-Agent"]] "  
}
```

The screenshot shows the F5 configuration interface for creating a new iRule. The breadcrumb navigation is 'Local Traffic >> iRules : iRule List >> New iRule...'. The 'Name' field is 'User-Agent_check'. The 'Definition' field contains the following iRule code:

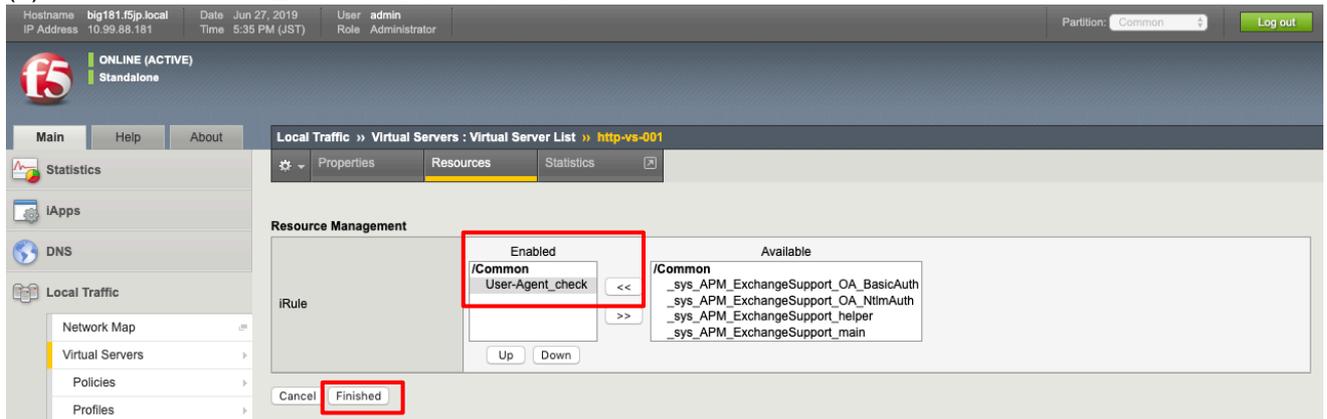
```
1 - when HTTP_REQUEST {  
2   log local0. "USER-AGENT is [string tolower [HTTP::header "User-Agent"]] "  
3 }
```

The 'Finished' button at the bottom is highlighted with a red box.

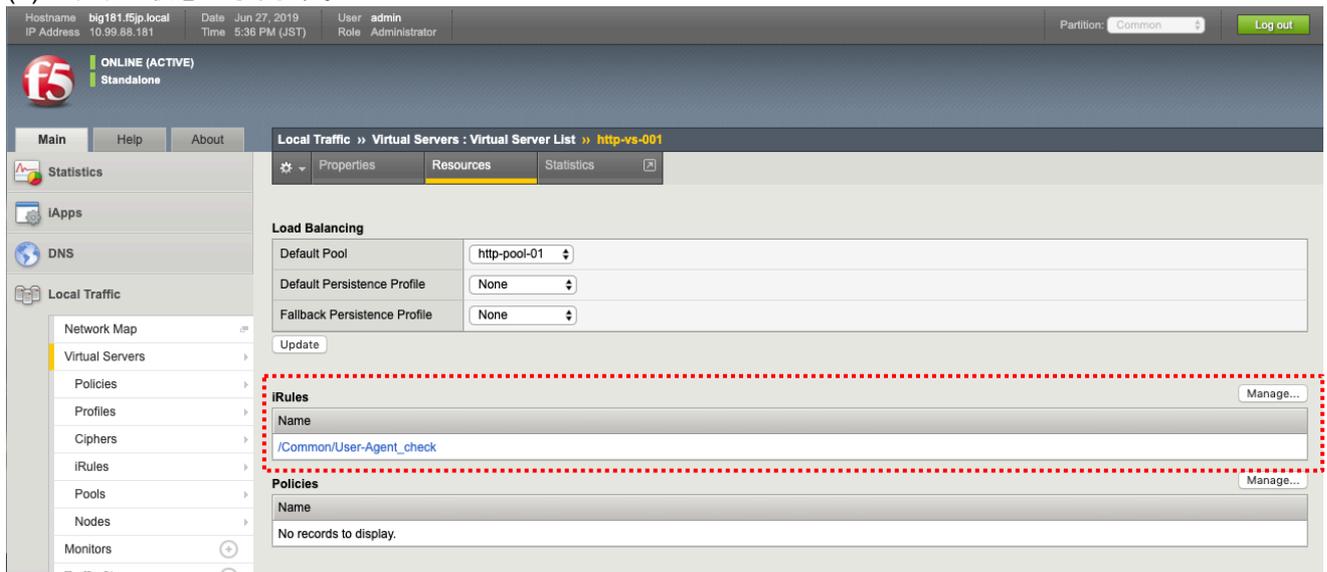
- (3) 次に、作成した iRule を Virtual Server へ適用します。「Local Traffic」→「Virtual Server」で表示された設定済みの Virtual Server を選択し、画面の上に表示された「Resources」タブをクリックします。iRules の部分の「Manage」ボタンを押します。

The screenshot shows the F5 configuration interface for a Virtual Server. The breadcrumb navigation is 'Local Traffic >> Virtual Servers : Virtual Server List >> http-vs-001'. The 'Resources' tab is selected and highlighted with a red box. The 'iRules' section has a 'Manage...' button highlighted with a red box.

(4) 作成した iRule を選択し、「<<」ボタンを押します。



(5) 以下の状態になります。



この iRule で出力されるログは、以下の手順で BIG-IP に SSH でアクセスし、コマンドラインで確認します

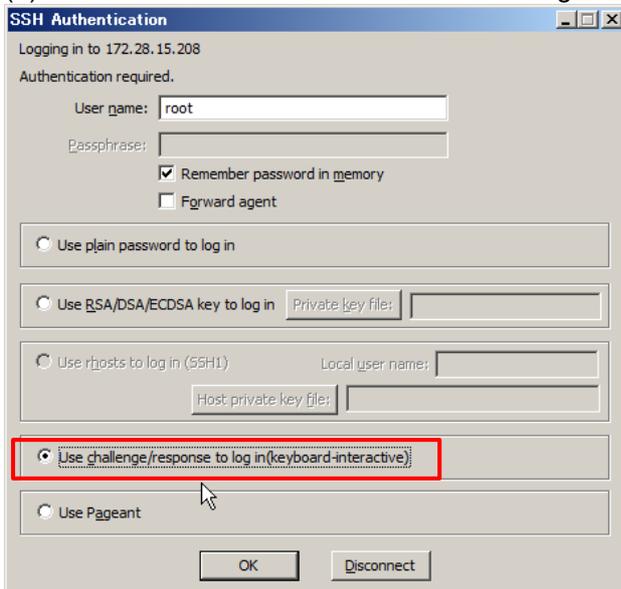
6.1.2. BIG-IP への SSH アクセス

SSH クライアント(例: TeraTerm)を使って、BIG-IP へ SSH でアクセスします。

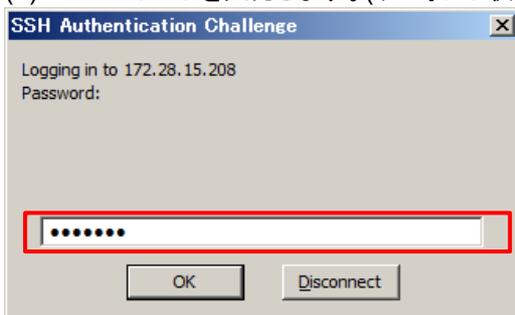
(1) SSH でログインします。



(2) User name に「root」を入力し、Use challenge/response to log in をチェックします。



(3) パスワードを入力します。(デフォルト状態のパスワードは「default」です)



(4) 以下のようなコマンドプロンプトが表示されます。

```
[root@bigXXX:Active:Standalone] config #
```

6.1.3. User-Agent をログ上で確認

(1) 以下のコマンドを実行します。

```
[root@bigXXX:Active:Standalone] config # tail -f /var/log/ltn
```

(2) クライアント PC で、iRule を設定した Virtual Server へ、以下 2 つのブラウザからアクセスします。

- Chrome
- Firefox

(3) /var/log/ltn に、以下のようなログ(例)が出力されます。

① Chrome

```
Jun 27 17:44:11 big181 info tmm1[9735]: Rule /Common/User-Agent_check <HTTP_REQUEST>: USER-AGENT is mozilla/5.0 (windows nt 10.0; win64; x64) applewebkit/537.36 (KHTML, like Gecko) chrome/75.0.3770.142 safari/537.36
```

② Firefox

```
Jun 27 17:43:53 big181 info tmm1[9735]: Rule /Common/User-Agent_check <HTTP_REQUEST>: USER-AGENT is mozilla/5.0 (windows nt 10.0; wow64; rv:65.0) Gecko/20100101 Firefox/68.0
```

6.2. User-Agent 毎にアクセス先 Pool Member を変える

上記の User-Agent 出力結果から、User-Agent に「firefox」の文字を含むものを 10.99.100.215:80 へ送り、それ以外は、10.99.100.217:80 へ送る、というルールを設定することにします。

(1) 先程作成した iRules を以下のように変更します。Update ボタンを押します。

```
when HTTP_REQUEST {  
    set UA [string tolower [HTTP::header "User-Agent"]]  
    if { $UA contains "firefox" } {  
        pool http-pool-01 member 10.99.100.215 80  
    }  
    else {  
        pool http-pool-01 member 10.99.100.217 80  
    }  
    log local0. "USER-AGENT is $UA"  
}
```

The screenshot shows the F5 iRule configuration interface. The 'User-Agent_check' iRule is selected, and its definition is displayed in the 'Definition' tab. The code is as follows:

```
1- when HTTP_REQUEST {  
2-  
3-     set UA [string tolower [HTTP::header "User-Agent"]]  
4-  
5-     if { $UA contains "firefox" } {  
6-         pool http-pool-01 member 10.99.100.215 80  
7-     }  
8-     else {  
9-         pool http-pool-01 member 10.99.100.217 80  
10-    }  
11-  
12-    log local0. "USER-AGENT is $UA"  
13- }
```

The 'Update' button is highlighted in a red box at the bottom of the interface.

(2) クライアント PC で、iRule を設定した Virtual Server へ、以下 2 つのブラウザからアクセスします。

- ① FireFox
- ② Chrome

それぞれが、iRule で指定した Pool Member へのみアクセスしていることを確認します。

(3) iRule 内の Pool Member の IP アドレスを入れ替えてみて、同様の確認を実施してみてください。
Firefox と Chrome で、アクセス先が入れ替わります。

iRule の使い方については以上です。

7. UCS の取得

UCS を取得することによって、現時点までの設定を保存しておくことができます。

- (1) 「System」 → 「Archives」 で表示された画面右上の「Create」ボタンを押します。
任意の名称(後に利用する際に分かりやすい名称)を入力し、「Finished」ボタンを押します。

Hostname big181.f5jp.local Date Jul 24, 2019 User admin
IP Address 10.99.88.181 Time 1:54 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System » Archives » New Archive...

Statistics
iApps
DNS
Local Traffic
Acceleration

General Properties

File Name	big-181-20190724
Encryption	Disabled ↓
Private Keys	Include ↓
Version	BIG-IP 14.1.0.6 Build 0.0.9

Cancel Finished

- (2) 「OK」ボタンを押します。

Hostname big181.f5jp.local Date Jul 24, 2019 User admin
IP Address 10.99.88.181 Time 1:57 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System » Archives

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management

Operation Status

Saving active configuration...
/var/local/ucs/big-181-20190724.ucs is saved.

OK

- (3) 以下の状態になります。

Hostname big181.f5jp.local Date Jul 24, 2019 User admin
IP Address 10.99.88.181 Time 2:12 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System » Archives

Archive List

Upload... Create...

File Name	Date	Size (Kbytes)
big-181-20190724.ucs	Wed Jul 24 13:56:47 JST 2019	19199

Delete...

- (4) UCS ファイル名をクリックすると、以下の画面になります。
本ガイドでは、この UCS ファイルを PC へダウンロードしておきます。Archive File を選択し、ダウンロードします。

Hostname big181.f5jp.local Date Jul 24, 2019 User admin
IP Address 10.99.88.181 Time 2:13 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System » Archives » big-181-20190724.ucs

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management

General Properties

File Name	big-181-20190724.ucs
Version	BIG-IP 14.1.0.6 Build 0.0.9
Encrypted	No
Date	Wed Jul 24 13:56:47 JST 2019
Size	19199 Kilobytes
Archive File	Download: big-181-20190724.ucs

Restore Delete

- (5) このまま UCS ファイルを BIG-IP 内に保存したままでもよいのですが、本ガイドでは、UCS を BIG-IP へアップロードして復元することを確認するために、ここでは一旦この UCS を削除します。

Hostname big181.f5jp.local Date Jun 27, 2019 User admin
IP Address 10.99.88.181 Time 7:03 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About System » Archives » big-181-20190627.ucs

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management

General Properties

File Name	big-181-20190627.ucs
Version	BIG-IP 14.1.0.5 Build 0.0.5
Encrypted	No
Date	Thu Jun 27 18:48:19 JST 2019
Size	107899 Kilobytes
Archive File	Download: big-181-20190627.ucs

Restore Delete

UCS ファイルによる復元動作を確認するために、次のステップで全コンフィグを消去します。

8. コンフィグの初期化(全消去)

コンフィグを全て消去する手順です。

8.1. BIG-IP への SSH アクセス

- (1) SSH クライアント(例:TeraTerm)を使って、BIG-IP へ SSH でアクセスします。
- (2) TMSH へ切り替えます。

```
[root@bigXXX:Active:Standalone] config # tmsch
```

以下のようなプロンプトに変わります。

```
root@(bigXXX)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

プロンプトが長いので、以降は「(tmos)#」の省略形を使います。

8.2. コンフィグの初期化

一旦、UCS を取得した BIG-IP (bigXXX.f5jp.local) の全設定を消去し、デフォルト状態に戻します。

(1) デフォルトコンフィグの流し込み

以下のコマンドを実行します。
(コンフィグをリセットしてよいか(y/n)をきかれるので、y と入力します。)
実行すると、コンフィグレーションが初期化されます。

```
(tmos)# load sys config default
```

(2) 保存

このデフォルトコンフィグを流し込んだ状態を保存します。

```
(tmos)# save sys config
```

9. UCS のリストア

初期化した BIG-IP(bigXXX.f5jp.local)を、UCS ファイルで復元します。

- (1) 一度でフォルドパスワード(admin/admin)でログオンし、パスワードを再設定します。
F5LAB では以下のように設定し、Save ボタンを押します。

Current Password: admin

New Password: ilovef5

Confirm: ilovef5

The screenshot shows the 'BIG-IP Configuration Utility' interface. On the left, there are input fields for 'Username' (admin), 'Current Password', 'New Password', and 'Confirm'. Below these fields are 'Cancel' and 'Save' buttons. The main content area displays the message: 'Your password has expired. Please change it using the fields on the left.' The footer contains copyright information: '(c) Copyright 1996-2018, F5 Networks, Inc., Seattle, Washington. All rights reserved. F5 Networks, Inc. Legal Notices'.

- (2) 設定したパスワードでログインします。

The screenshot shows the 'BIG-IP Configuration Utility' login screen. On the left, there are input fields for 'Username' and 'Password', and a 'Log in' button. The main content area displays the message: 'Welcome to the BIG-IP Configuration Utility. Log in with your username and password using the fields on the left.' A red message 'Password changed successfully.' is visible above the 'Username' field. The footer contains copyright information: '(c) Copyright 1996-2018, F5 Networks, Inc., Seattle, Washington. All rights reserved. F5 Networks, Inc. Legal Notices'.

- (3) ブラウザで BIG-IP へアクセスすると、最初に設定したウィザード画面が現れます。

The screenshot shows the 'Setup Utility' main screen. At the top, there is a status bar with 'ONLINE (ACTIVE)' and 'Standalone'. Below this is a navigation menu with 'Main', 'Help', and 'About' buttons. The main content area displays the 'Welcome' message: 'Setup Utility To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.' A 'Next...' button is visible at the bottom of the main content area. The footer contains copyright information: '(c) Copyright 1996-2018, F5 Networks, Inc., Seattle, Washington. All rights reserved. F5 Networks, Inc. Legal Notices'.

- (4) UCS ファイルで設定を戻すので、ウィザードで設定する必要はありません。
よって、このウィザードをコマンドラインで停止します。

```
[root@localhost:Active:Standalone] config # tmsm modify sys global-settings gui-setup disabled
```

- (5) もう一度 BIG-IP ヘブラウザでアクセスすると、以下の画面に変わります。
(ウィザードが開始されません。)

The screenshot shows the F5 configuration utility interface. At the top, it displays system information: Hostname: bigip1, IP Address: 10.99.88.181, Date: Jun 28, 2019, Time: 1:25 AM (PDT), User: admin, Role: Administrator. The interface is titled 'ONLINE (ACTIVE) Standalone'. The main navigation menu includes Main, Help, and About. The 'Statistics' menu is expanded, showing options for Dashboard, Module Statistics, and Performance Reports. The 'Setup' section is active, displaying 'User Documentation', 'Preferences', and 'Additional Setup Options'. The 'Support' section is also visible, featuring 'Ask F5', 'Deployment Guides', and 'DevCentral'.

- (6) コマンドラインで、ログを tail し、ucs リストア状況を確認する設定をします。

```
[root@localhost:Active:Standalone] config # tail -f /var/log/ltn|grep ucs
```

- (7) 「System」 → 「Archives」 で表示された画面右上の「Upload」ボタンを押します。
保存しておいた UCS ファイルを指定して、Upload します。

The screenshot shows the 'System >> Archives >> Upload...' page. The 'Upload Configuration Archives' section is active. The 'File Name' field contains 'big-181-20190724.ucs' and is highlighted with a red box. The 'Options' section has an unchecked checkbox for 'Overwrite existing archive file'. The 'Upload' button is highlighted with a red box. A red annotation 'UCS ファイルを指定' points to the file name field.

- (8) アップロードした UCS ファイルをクリックします。

The screenshot shows the 'System >> Archives' page with the 'Archive List' table. The table has columns for File Name, Date, and Size (Kbytes). The file 'big-181-20190724.ucs' is listed with a date of 'Tue Jul 23 22:21:41 PDT 2019' and a size of '19199'. The file name and its corresponding date/size are highlighted with a red box.

File Name	Date	Size (Kbytes)
big-181-20190724.ucs	Tue Jul 23 22:21:41 PDT 2019	19199

(9) 「Restore」ボタンを押します。

The screenshot shows the F5 BIG-IP configuration interface. At the top, it displays system information: Hostname: bigip1, IP Address: 10.99.88.181, Date: Jul 23, 2019, Time: 10:22 PM (PDT), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main content area is titled 'System » Archives » big-181-20190724.ucs'. On the left, there is a navigation menu with options like Statistics, iApps, DNS, Local Traffic, Acceleration, and Device Management. The main panel shows 'General Properties' for the archive file, including File Name, Version, Encrypted status, Date, Size, and Archive File. At the bottom of this panel, the 'Restore' button is highlighted with a red rectangle, next to a 'Delete' button.

(10) 以下の状態のときは、「OK」ボタンを押さず、しばらく待ちます。

The screenshot shows the F5 BIG-IP configuration interface during a restoration process. The top bar is the same as in the previous screenshot. The main content area is titled 'System » Archives'. The 'Operation Status' section displays the message: 'Restoring System Archive. The status will be updated shortly...'. Below this message, there is an 'OK' button.

「OK」を押しても問題はないのですが、次の画面に遷移すると、リストアが完了することを示すログを確認することができないので、いつ完了したのかがわかりにくいいため、ここでは「OK」を押さずにしばらく待ちます。

つい、「OK」を押してしまった場合にも、しばらく待てば、リストアは完了します。

(11) 一時的に以下のようなメッセージが表示されるかもしれませんが、そのまま待ちます。

The screenshot shows the F5 BIG-IP configuration interface with an error message. The top bar shows Hostname: bigip1, IP Address: 10.99.88.181, Date: Jul 24, 2019, Time: 2:24 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. A yellow banner at the top of the main content area displays the message: 'The configuration has not yet loaded. If this message persists, it may indicate a configuration problem.' The main content area is titled 'System » Archives'. The 'Operation Status' section displays the message: 'Restoring System Archive. The status will be updated shortly...'. Below this message, there is an 'OK' button.

(12) コマンドラインのログを確認し、以下のように UCS リストアが成功するまで待ちます。

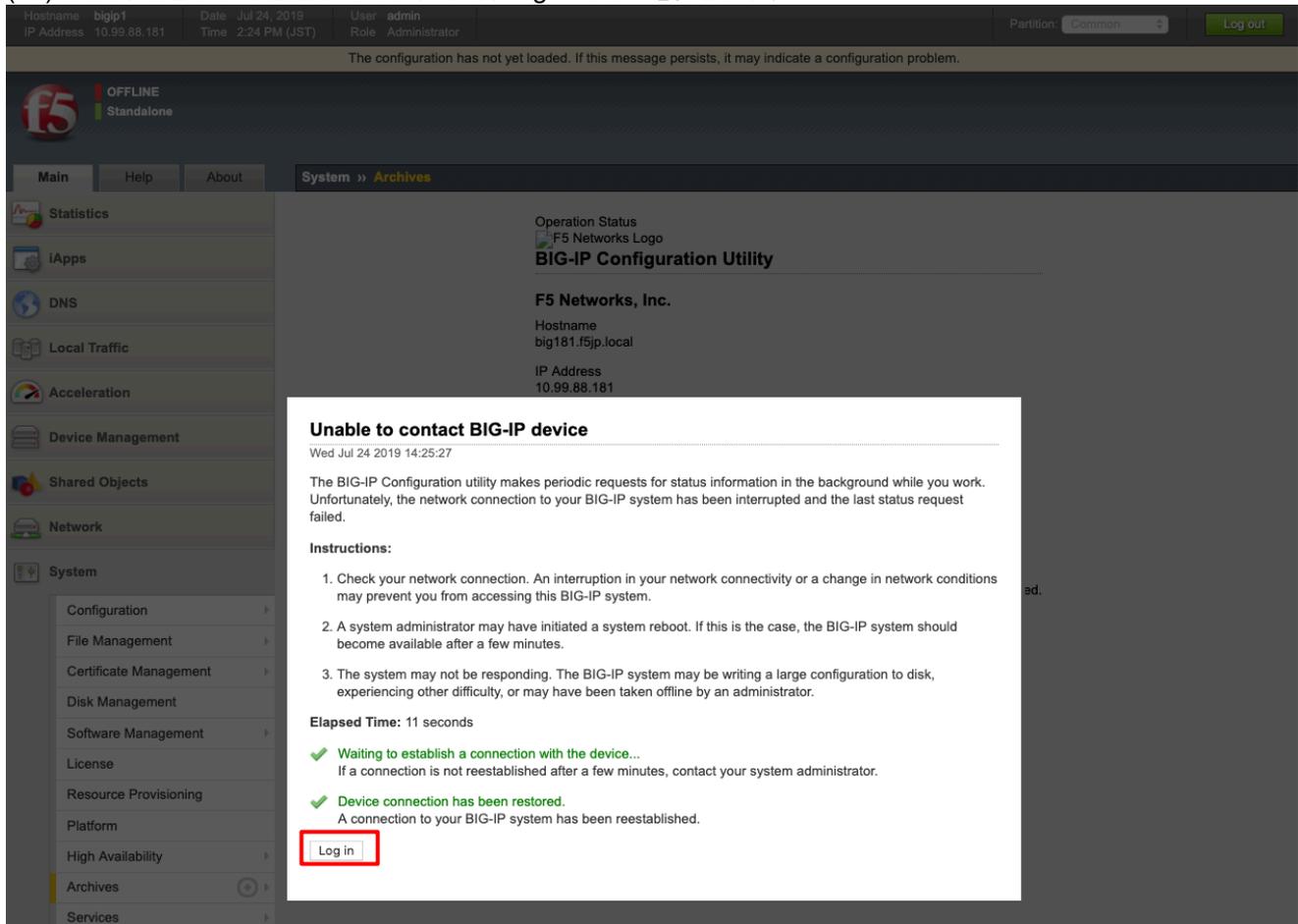
```
[root@localhost:Active:Standalone] config # tail -f /var/log/lm|grep ucs
Jul 23 22:42:50 localhost.localdomain info tmsh[29942]: Begin config install operation: /var/local/ucs/big-181-20190724.ucs
Jul 23 22:42:55 localhost.localdomain notice logger[1271]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart stop named
Jul 23 22:42:57 localhost.localdomain notice logger[1306]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart stop zrd
Jul 23 22:42:57 localhost.localdomain info install_ucs.pm[1175]: Install the license file from UCS onto the system.
Jul 24 14:43:00 localhost.localdomain notice logger[2049]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart stop restjavad restnoded
Jul 24 14:43:00 localhost.localdomain notice logger[2140]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart start named
Jul 24 14:43:00 localhost.localdomain notice logger[2147]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart start zrd
Jul 24 14:43:01 localhost.localdomain notice logger[2294]: /usr/bin/perl /usr/local/bin/im -exclfrom -q -force /var/local/ucs/big-181-20190724.ucs ==> /bin/bigstart start restjavad restnoded
Jul 24 14:43:02 localhost.localdomain notice logger[2414]: /bin/sh /usr/lib/csyncd/reloadnamed.sh /run/ucs.restore.pid ==> /bin/bigstart start zrd

Broadcast message from systemd-journald@localhost.localdomain (Wed 2019-07-24 14:43:04 JST):

logger[2645]: Re-starting bigd

2019 Jul 24 14:43:04 localhost.localdomain logger[2645]: Re-starting bigd
Jul 24 14:44:11 big181.f5jp.local info install_ucs.pm[1175]: UCS installation success.
```

(13) 成功すると以下の画面になりますので、Log in ボタンを押します。

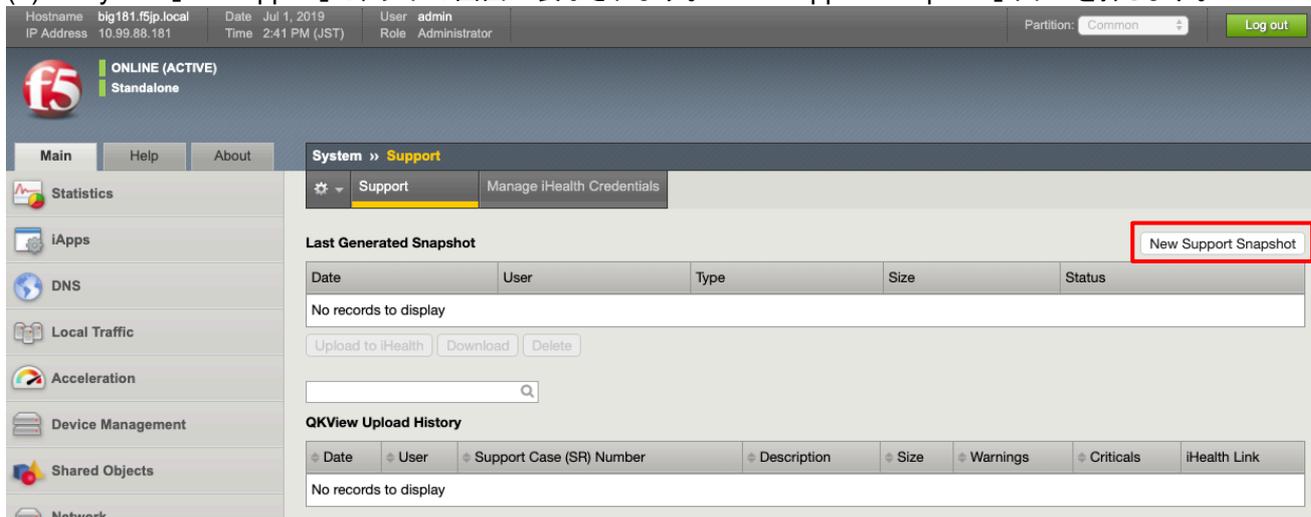


(14) 設定済みの ID とパスワードでログインし、リストアされていることを確認します。

10. QKview の取得

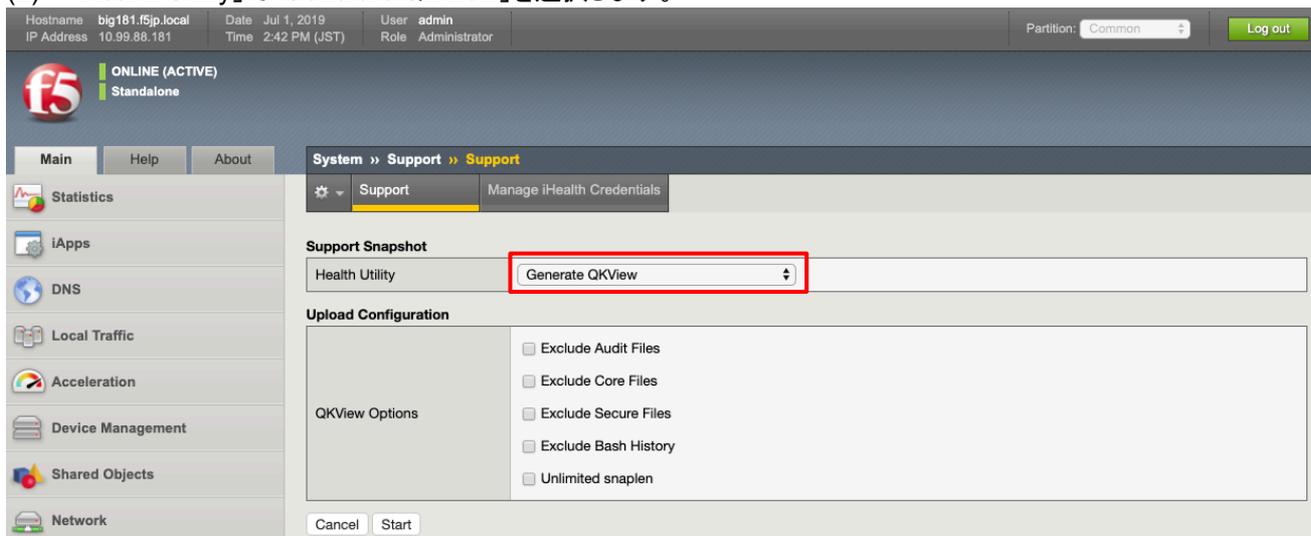
何らかの不具合発生時には、F5 サポートへ QKview の送付が必要となります。
以下に QKview の取得方法を記載します。

(1) 「System」→「Support」で、以下の画面が表示されます。「New Support Snapshot」ボタンを押します。



The screenshot shows the F5 management console interface. At the top, there is a status bar with Hostname: big181.f5.jp.local, IP Address: 10.99.88.181, Date: Jul 1, 2019, Time: 2:41 PM (JST), User: admin, Role: Administrator, and Partition: Common. The main navigation menu includes Main, Help, and About. The left sidebar contains various system monitoring tools like Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, and Network. The main content area is titled 'System >> Support' and contains a 'Support' tab and a 'Manage iHealth Credentials' tab. Under the 'Support' tab, there is a section for 'Last Generated Snapshot' with a table showing no records and a 'New Support Snapshot' button highlighted with a red box. Below this is a search bar and buttons for 'Upload to iHealth', 'Download', and 'Delete'. There is also a section for 'QKView Upload History' with a table showing no records and columns for Date, User, Support Case (SR) Number, Description, Size, Warnings, Criticals, and iHealth Link.

(2) 「Health Utility」で「Generate QKView」を選択します。



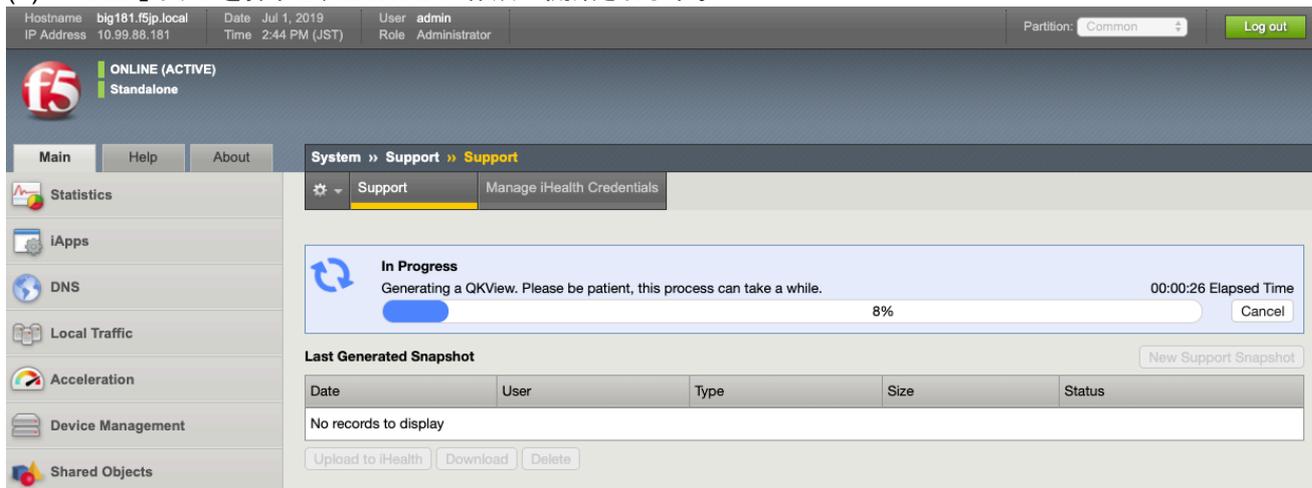
The screenshot shows the F5 management console interface. At the top, there is a status bar with Hostname: big181.f5.jp.local, IP Address: 10.99.88.181, Date: Jul 1, 2019, Time: 2:42 PM (JST), User: admin, Role: Administrator, and Partition: Common. The main navigation menu includes Main, Help, and About. The left sidebar contains various system monitoring tools like Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, and Network. The main content area is titled 'System >> Support >> Support' and contains a 'Support' tab and a 'Manage iHealth Credentials' tab. Under the 'Support' tab, there is a section for 'Support Snapshot' with a dropdown menu showing 'Health Utility' and 'Generate QKView' (highlighted with a red box). Below this is a section for 'Upload Configuration' with a list of checkboxes for 'Exclude Audit Files', 'Exclude Core Files', 'Exclude Secure Files', 'Exclude Bash History', and 'Unlimited snaplen'. At the bottom, there are 'Cancel' and 'Start' buttons.

上記で、「Generate and Upload QKView to iHealth」を選択すると、iHealth サイトに QKView を直接アップロード可能となります。

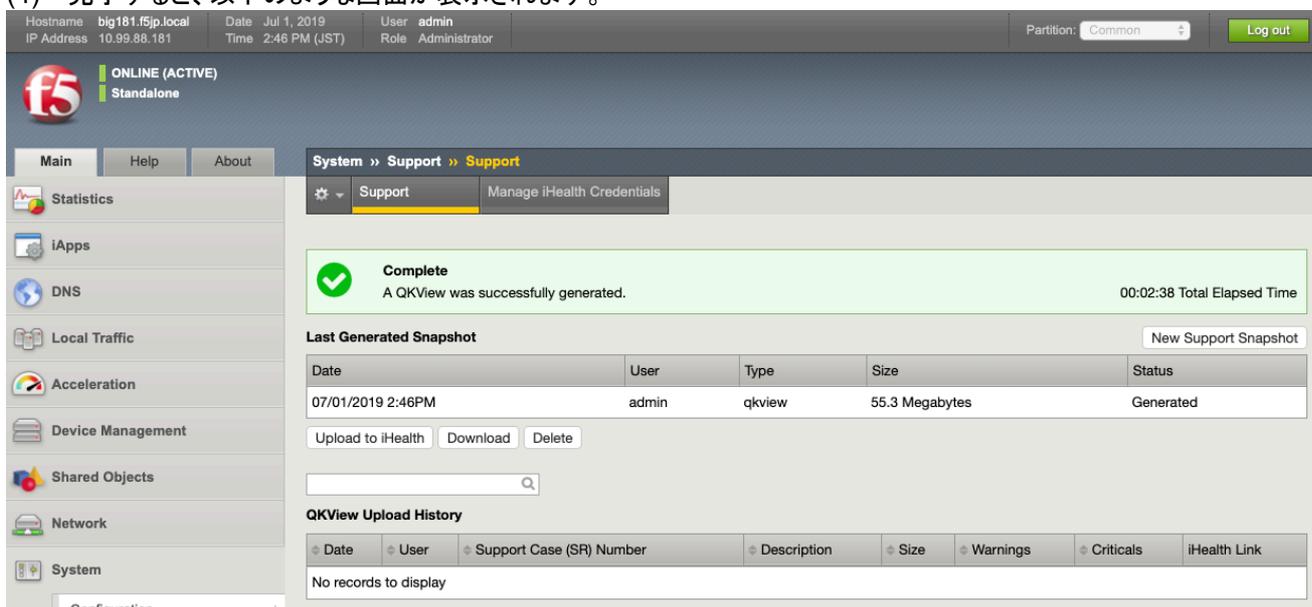
iHealth は BIG-IP の設定データや過去1ヶ月分のログデータを閲覧できる大変便利なツールです(予め簡単なユーザ登録が必要です)。iHealth の詳細に関しては、以下の Article に情報が掲載されております。

K12878: Generating diagnostic data using the qkview utility
<https://support.f5.com/csp/article/K12878>

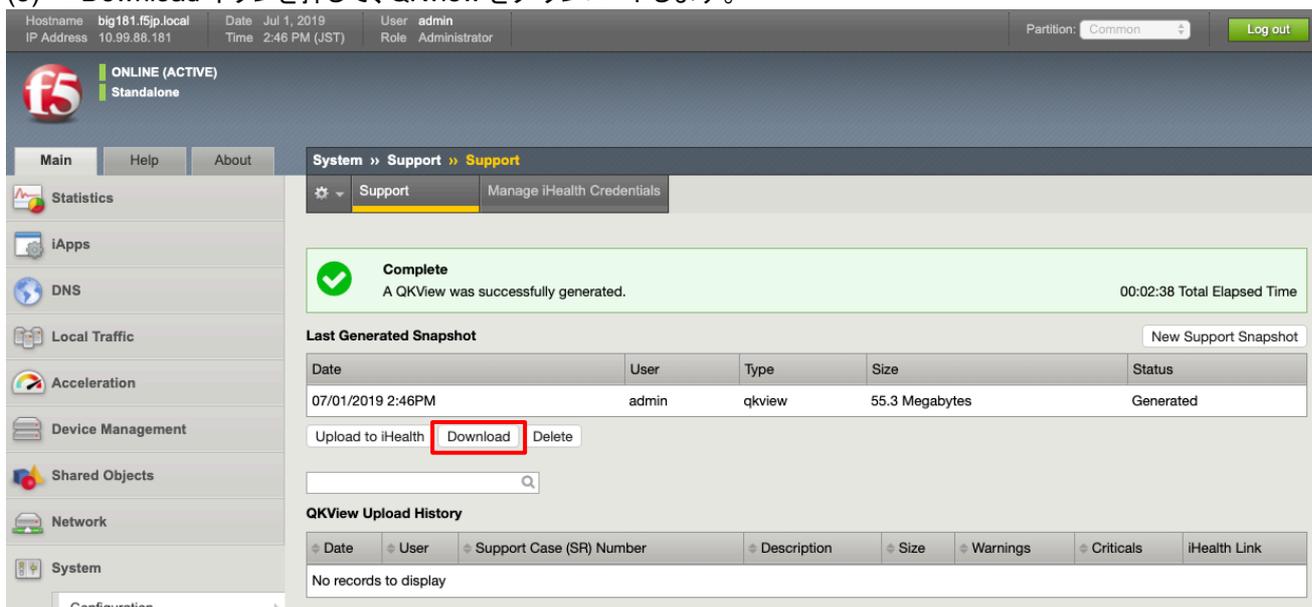
(3) 「Start」ボタンを押すと、QKView の作成が開始されます。



(4) 完了すると、以下のような画面が表示されます。



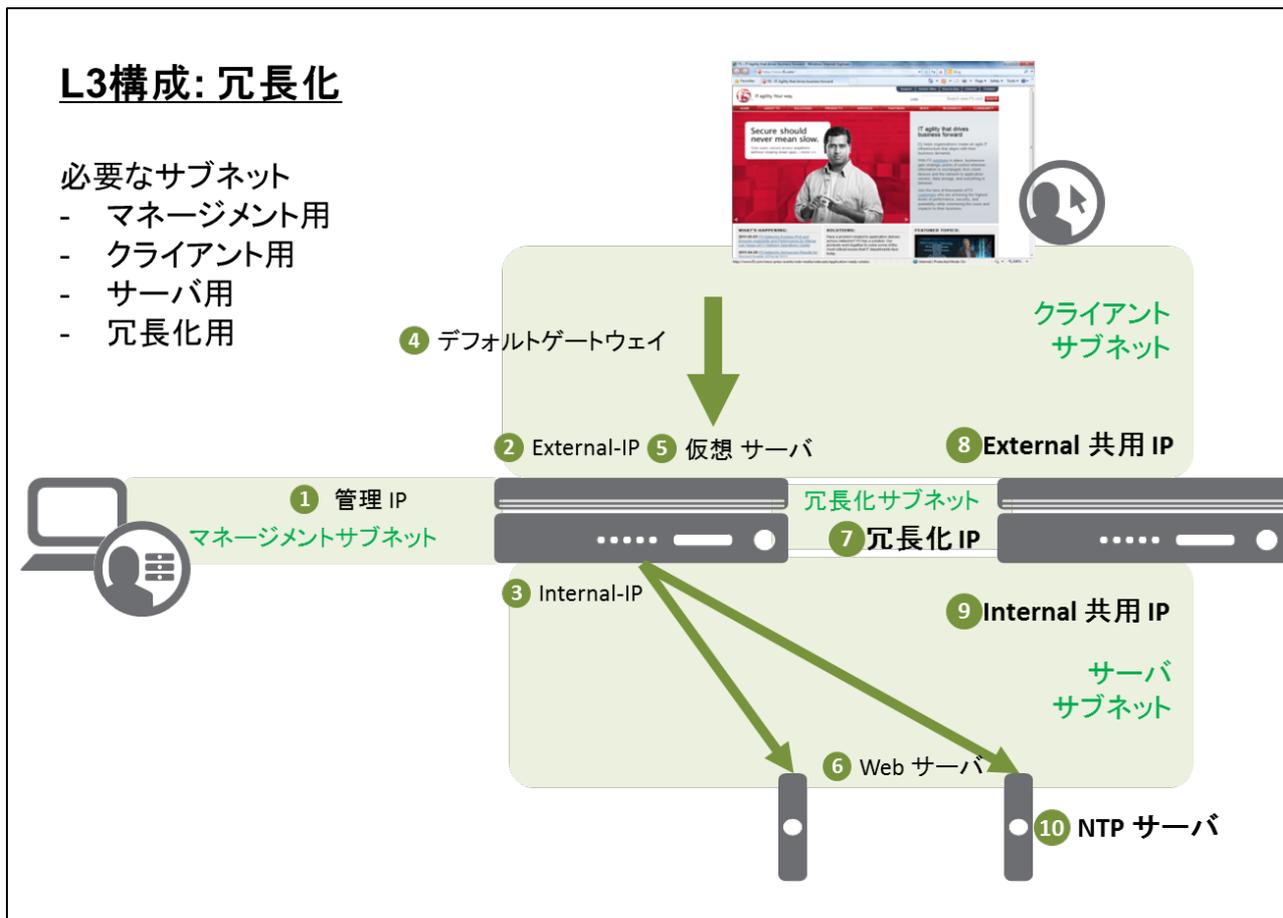
(5) 「Download」ボタンを押して、QKView をダウンロードします。



以上で QKview の取得は終了です。

11. L3 構成:冗長化

11.1. L3 構成:冗長化イメージ

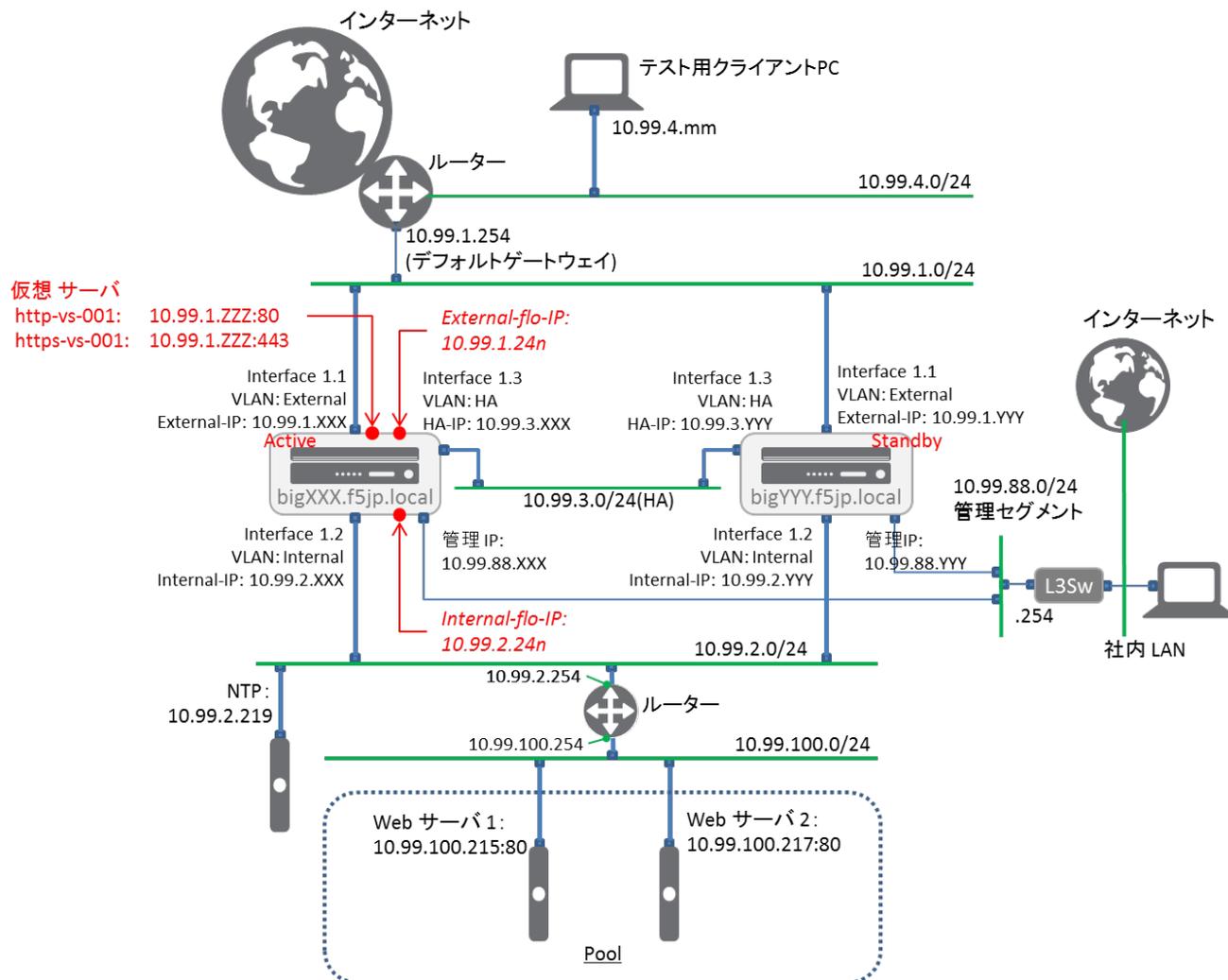


スタンドアロン構成に加え、冗長化用サブネットが必要になります。また、2 台で共有し、どちらかが Active に動作する共有 IP アドレスを設定し、サーバのデフォルト GW として指定します。

項目	名前(サンプル)		名前(サンプル)	
	1号機	値(サンプル)	2号機	値(サンプル)
ホスト名		bigXXX.f5jp.local		bigYYY.f5jp.local
① 管理インタフェース	---	10.99.88.XXX/24	---	10.99.88.YYY/24
② External インタフェース	external	10.99.1.XXX/24	external	10.99.1.YYY/24
③ Internal インタフェース	internal	10.99.2.XXX/24	internal	10.99.2.YYY/24
④ デフォルトゲートウェイ		10.99.1.254	⇒	設定同期によりコピー
⑤ 仮想サーバアドレス	http-vs-001 https-vs-001	10.99.1.ZZZ:80 10.99.1.ZZZ:443	⇒	設定同期によりコピー
⑥ Webサーバ1の アドレス:ポート	---	10.99.100.215:80	⇒	設定同期によりコピー
Webサーバ2の アドレス:ポート	---	10.99.100.217:80	⇒	設定同期によりコピー
⑦ 冗長化用インタフェース	HA	10.99.3.XXX/24	HA	10.99.3.YYY/24
⑧ External 共用	external-flo-ip	10.99.1.24n	⇒	設定同期によりコピー
⑨ Internal 共用	internal-flo-ip	10.99.2.24n	⇒	設定同期によりコピー
⑩ NTPサーバ		10.99.100.219		

11.2. L3 構成: 冗長化のネットワークサンプル

もう一台 BIG-IP を追加して、L3 構成の冗長化設定を行います。



このサンプルでは、NTP サーバを 10.99.2.219 とし、BIG-IP はこのサーバとの時刻同期を行うことします。(冗長化を行う BIG-IP 同士は、時刻を合わせておく必要があります。)

BIG-IP 間の HA (High Availability) VLAN は、冗長化の制御パケットをやり取りする専用の VLAN です。External や Internal VLAN を利用することも可能ですが、HA 専用の VLAN を追加することを推奨しています。よって、本構成においては、HA VLAN を追加しています。

11.3. Active 機(bigXXX.f5jp.local)の設定

11.3.1. HA VLAN の設定

(1) 「Network」→「VLANs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN を設定します。

Hostname big181.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 2:49 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » VLANs : VLAN List » New VLAN...

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
Network

Interfaces
Routes
Self IPs
Packet Filters
Quick Configuration
Trunks
Tunnels
Route Domains
VLANs
Service Policies

General Properties

Name HA 名前(任意)を指定
Description
Tag

Resources

Interface: 1.1
Tagging: Untagged
Add
1.3 (untagged) ポート&Untaggedを選択
Edit Delete

Configuration: Basic

Source Check
MTU 1500

sFlow

Polling Interval Default
Sampling Rate Default

Cancel Repeat Finished

11.3.2. HA VLAN の IP 設定

(1) 「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN の IP を設定します。

Hostname big181.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 2:51 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network » Self IPs » New Self IP...

Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
Network

Configuration

Name HA-ip 名前(任意)
IP Address 10.99.3.181 10.99.3.XXX(F5 ラボの場合) IP アドレス
Netmask 255.255.255.0 サブネットマスク
VLAN / Tunnel HA VLANを設定
Port Lockdown Allow Default (※注)必ず Allow None 以外を選ぶ
Traffic Group Inherit traffic group from current partition / path
traffic-group-local-only (non-floating)
Service Policy None

Cancel Repeat Finished

(※注) Allow None を選ぶと HA の通信も止めてしまい、HA が組めません。(ここでは Allow Default を選びます)

11.3.3. Device の設定

(1) 次に、「Device Management」→「Devices」で、自分自身:bigXXX.f5jp.local(Self)を選択します。

Hostname big181.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 2:54 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Device Management » Devices

Device List

Search

Status	Name	Address	Hostname	Version	Time Delta (sec)
	big181.f5jp.local (Self)	10.99.88.181	big181.f5jp.local	BIG-IP v14.1.0.5 (Build 0.0.5)	0

Overview
Devices
Device Groups

(2) 「ConfigSync」タブを選択し、HA VLAN に指定した IP アドレスを選択し「Update」を押します。

Hostname big181.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 2:55 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Device Management » Devices » big181.f5jp.local

Properties **ConfigSync** Failover Network Mirroring

ConfigSync Configuration

Local Address 10.99.3.181 (HA) HA VLAN に設定した SelfIP を選択

Update

(3) 「Failover Network」タブを選択し、「Add」ボタンを押します。

Hostname big181.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 3:04 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Device Management » Devices » big181.f5jp.local

Properties ConfigSync **Failover Network** Mirroring

Failover Unicast Configuration

Local Address Port VLAN

No records to display.

Delete

Failover Multicast Configuration

Use Failover Multicast Address Enabled

Update

Add...

(4) HA VLAN に設定した IP アドレスを選択します。

The screenshot shows the 'New Failover Unicast Address' configuration page. The 'Address' dropdown menu is set to '10.99.3.181 (HA)', which is highlighted with a red box and a red annotation: 'HA VLAN に設定した SelfIP を選択'. The 'Port' is set to '1026'. At the bottom, the 'Finished' button is highlighted with a red box.

(5) 以下のような状態になります。

The screenshot shows the 'Failover Unicast Configuration' page. A table lists the configured addresses:

<input checked="" type="checkbox"/>	Local Address	Port	VLAN
<input type="checkbox"/>	10.99.3.181	1026	HA

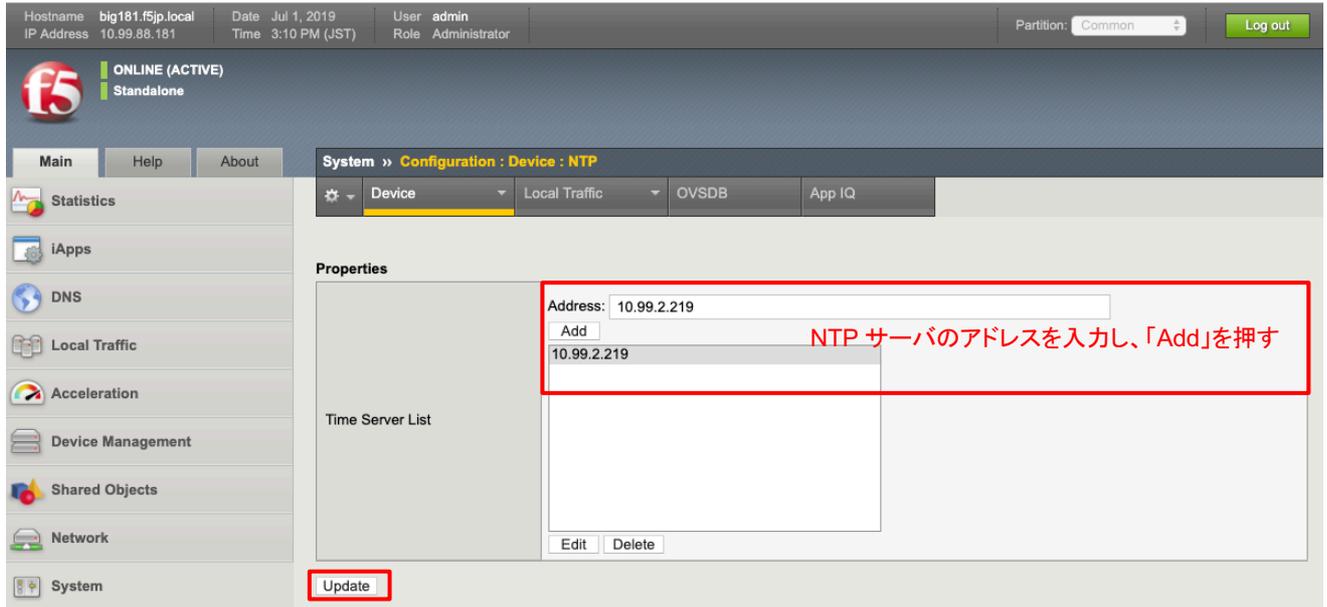
The row containing '10.99.3.181' is highlighted with a red box. Below the table, the 'Failover Multicast Configuration' section shows 'Use Failover Multicast Address' set to 'Enabled'.

(6) 「Mirroring」タブを選択し、HA VLAN に指定した IP アドレスをプライマリに指定します。任意ですが、ここでは Secondary として、Internal VLAN に指定した IP アドレスを選択しています。選択後、「Update」を押します。

The screenshot shows the 'Mirroring Configuration' page. The 'Primary Local Mirror Address' is set to '10.99.3.181 (HA)' and the 'Secondary Local Mirror Address' is set to '10.99.2.181 (internal)'. Both dropdown menus are highlighted with a red box and a red annotation: 'Primary には HA VLAN に設定した SelfIP を選択 Secondary は任意(ここでは Internal VLAN を選択)'. The 'Update' button at the bottom is also highlighted with a red box.

11.3.4. 時刻同期(NTP)設定

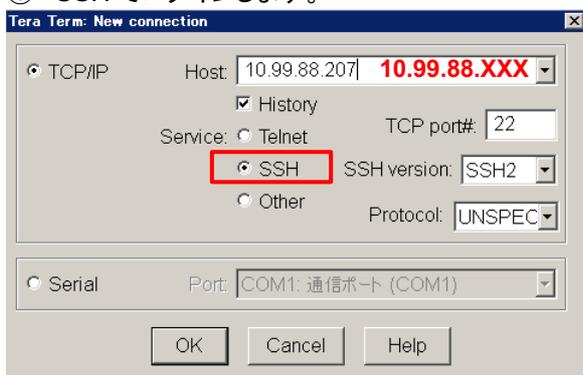
- (1) 「System」 → 「Configuration」 → 「Device」 → 「NTP」を選択します。
Address 欄に、NTP サーバの IP アドレスを入力し、「Add」ボタンを押します。



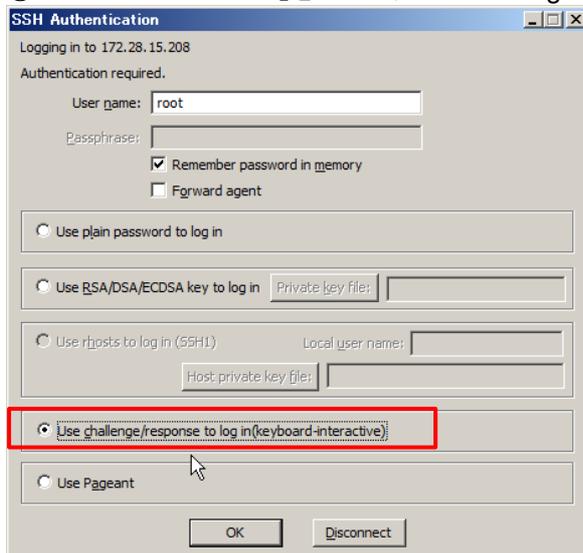
[ご参考] NTP 同期状態の確認

NTP 同期状態の確認は、コマンドラインから実施します。以下に、Tera Term を利用した場合の確認方法を示します。

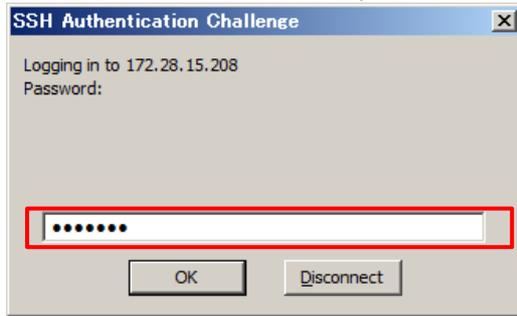
- ① SSH でログインします。



- ② User name に「root」を入力し、Use challenge/response to log in をチェックします。



- ③ パスワードを入力します。(デフォルト状態のパスワードは「default」です)



- ④ SSH アクセスが完了したら、「ntpq -np」を実行します。先頭に「*」がついていれば、同期が完了しています。(同期完了状態になるまで、時間がかかる場合があります。)

```
[root@bigXXX:Active:Standalone] config # ntpq -np
remote          refid          st t when poll reach  delay  offset jitter
=====
*10.99.2.219    133.243.238.164 2 u  115 128   377  1.927  -2.995  1.491
```

11.4. Standby 機(bigYYY.f5jp.local)の設定

Standby 機(bigYYY.f5jp.local)に対して、Host Name, password 等を設定し、bigXXX.f5jp.local での VLAN, Self IP, Devices の設定と同様の設定を行います。

11.4.1. VLAN 設定

(1) Standby 機(bigYYY.f5jp.local)に設定された VLAN は以下のようになります。

<input type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	HA	4092	1.3			Common
<input type="checkbox"/>	external	4094	1.1			Common
<input type="checkbox"/>	internal	4093	1.2			Common

11.4.2. Self-IP 設定

(1) Standby 機(bigYYY.f5jp.local)に設定された Self IP アドレスは以下のようになります。

<input type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	HA-ip		10.99.3.180	255.255.255.0	HA	traffic-group-local-only	Common
<input type="checkbox"/>	external-ip		10.99.1.180	255.255.255.0	external	traffic-group-local-only	Common
<input type="checkbox"/>	internal-ip		10.99.2.180	255.255.255.0	internal	traffic-group-local-only	Common

11.4.3. Device 設定

「Device Management」→「Devices」で、自分自身:bigYYY.f5jp.local(self)を選択し、Active 機同様に、Device Connectivity の設定を行います。

(1) ConfigSync 設定

Hostname big180.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.180 Time 3:38 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Device Management » Devices » big180.f5jp.local

ConfigSync Configuration

Local Address: 10.99.3.180 (HA) HA VLAN の SelfIP を選択

Update

(2) Failover Network 設定

Hostname big180.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.180 Time 3:39 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Device Management » Devices » big180.f5jp.local

New Failover Unicast Address

Address: 10.99.3.180 (HA) HA VLAN の SelfIP を選択

Port: 1026

Cancel Repeat Finished

(3) Mirroring 設定

Hostname big180.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.180 Time 3:42 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Device Management » Devices » big180.f5jp.local

Mirroring Configuration

Primary Local Mirror Address: 10.99.3.180 (HA) Primary には HA VLAN に設定した SelfIP を選択

Secondary Local Mirror Address: 10.99.2.180 (internal) Secondary は任意(ここでは Internal VLAN を選択)

Update

11.4.4. NTP 設定

(1) NTP の設定も Active 機同様に行います。

Hostname big180.f5jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.180 Time 3:45 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

System » Configuration : Device : NTP

Properties

Address: 10.99.2.219
Add
10.99.2.219 NTP サーバのアドレスを入力し、「Add」を押す

Time Server List

Edit Delete

Update

11.5. デバイストラスト設定 (Active 機(bigXXX.f5jp.local)側から実施)

デバイストラスト設定にて、冗長化する機器間で信頼関係を結びます。
以降は、Active 機(bigXXX.f5jp.local)からのみ、設定します。

(1) 「Device Management」→「Device Trust」→「Device Trust Members」を選択し、「Add」ボタンを押します。

The screenshot shows the F5 Device Management web interface. At the top, the status is 'ONLINE (ACTIVE) Standalone'. The breadcrumb navigation is 'Device Management >> Device Trust : Device Trust Members'. In the left sidebar, the 'Device Trust' menu item is highlighted with a red box. In the main content area, the 'Add...' button is highlighted with a red box. Below the 'Add...' button is a table with columns for Name, Device Type, Hostname, Serial Number, and MAC Address. The table currently shows 'No records to display'.

(2) "Peer"を選択し、Standby 機(bigYYY.f5jp.local)の IP アドレスと管理者 ID(Admin)とパスワードを指定します。
「Retrieve Device Information」ボタンを押します。

The screenshot shows the 'Retrieve Device Credentials (Step 1 of 3)' form in the F5 Device Management interface. The 'Device Type' dropdown is set to 'Peer'. The 'Device IP Address' field contains '10.99.3.180 10.99.3.YYY (F5LAB の場合)'. The 'Administrator Username' is 'admin' and the 'Administrator Password' is masked with '.....'. The 'Retrieve Device Information' button is highlighted with a red box. Red annotations on the right side of the form provide instructions: 'Peer'を選択 (Peer is selected), Standby 機の IP アドレスを入力 (Enter Standby device IP address), 管理者ユーザ名を入力 (Enter administrator username), and 管理者のパスワードを入力 (Enter administrator password).

- (3) Standby 機(bigYYY.f5jp.local)の証明書情報が表示されます。「Device Certificate Matches」ボタンを押します。

Hostname: big181.f5jp.local | Date: Jul 1, 2019 | User: admin | Partition: Common | Log out

IP Address: 10.99.88.181 | Time: 3:31 PM (JST) | Role: Administrator

ONLINE (ACTIVE) Standalone

Device Management > Device Trust

Retrieve Device Credentials (Step 1 of 3)

Device Type	Peer
Device IP Address	10.99.3.180
Administrator Username	admin
Administrator Password	*****

Verify Device Certificate (Step 2 of 3)

Subject	/C=- -/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	10.99.3.180
Expiration	Sun May 27 10:28:25 JST 2029
Serial Number	f5a08e00892d57f0
Signed	Yes
SHA-1	9111022b67ff8c55471be7897499988cc7fa80d5
MD5	4660541f0f5ed7b75b3d8931f5b2eb66

Cancel **Device Certificate Matches**

- (4) Standby 機の Hostname を確認し、「Add Device」を押します。

Hostname: big181.f5jp.local | Date: Jul 1, 2019 | User: admin | Partition: Common | Log out

IP Address: 10.99.88.181 | Time: 3:32 PM (JST) | Role: Administrator

ONLINE (ACTIVE) Standalone

Device Management > Device Trust

Retrieve Device Credentials (Step 1 of 3)

Device Type	Peer
Device IP Address	10.99.3.180
Administrator Username	admin
Administrator Password	*****

Verify Device Certificate (Step 2 of 3)

Subject	/C=- -/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	10.99.3.180
Expiration	Sun May 27 10:28:25 JST 2029
Serial Number	f5a08e00892d57f0
Signed	Yes
SHA-1	9111022b67ff8c55471be7897499988cc7fa80d5
MD5	4660541f0f5ed7b75b3d8931f5b2eb66

Add Device (Step 3 of 3)

Name	big180.f5jp.local
------	-------------------

Cancel **Add Device**

(5) 承認されたデバイスとして登録された状態です。

Hostname: big191.f5jp.local | Date: Jul 26, 2019 | User: admin | Partition: Common | Log out

ONLINE (ACTIVE) | Awaiting Initial Sync

Device Management » Device Trust : Device Trust Members

Peer and Subordinate Devices

<input checked="" type="checkbox"/>	Name	Device Type	Hostname	Serial Number	MAC Address
<input type="checkbox"/>	big190.f5jp.local	Peer	big190.f5jp.local	42170a79-3a7e-0ceb-b6b25c8c6b9d	00:50:56:97:1d:4c

(6) 「Device Management」→「Devices」で見ると、(self)に加え、Standby 機(bigYYY.f5jp.local)も表示されます。(ここは確認のみです。)

Hostname: big191.f5jp.local | Date: Jul 26, 2019 | User: admin | Partition: Common | Log out

ONLINE (ACTIVE) | Awaiting Initial Sync

Device Management » Devices

Device List

Status	Name	Address	Hostname	Version	Time Delta (sec)
	big190.f5jp.local	10.99.88.190	big190.f5jp.local	BIG-IP v14.1.0.6 (Build 0.0.9)	0
	big191.f5jp.local (Self)	10.99.88.191	big191.f5jp.local	BIG-IP v14.1.0.6 (Build 0.0.9)	0

11.6. デバイスグループの設定

デバイスグループは、デバイストラストで信頼関係を結んだ機器の間で、どの機器間で冗長化を行うかの指定です。デバイストラストは BIG-IP × 3 台以上で構成することも可能で、例えば、(1)と(2)で冗長化を行い、(2)と(3)はコンフィグ同期のみ行う、という組合せが可能となっています。この組み合わせをデバイスグループで指定します。

2 台で冗長化を行う場合はデバイスグループの組み方をあまり意識する必要はありませんが、設定は必要です。

(1) 「Device Management」→「Device Groups」において、Create ボタンを押し、以下のように入力します。

The screenshot shows the 'New Device Group' configuration page in the F5 Device Management interface. The following settings are highlighted with red boxes and annotations:

- Name:** Device-Group-001 (Annotation: 名前(任意)を設定)
- Group Type:** Sync-Failover (Annotation: 「Sync-Failover」を選択)
- Members:** big180.f5jp.local and big181.f5jp.local are selected in the 'Includes' list. (Annotation: 冗長化を行うデバイス(自分自身を含む)を選択)
- Network Failover:** Enabled (Annotation: ネットワークフェイルオーバーを行うので、チェック)

At the bottom of the configuration form, the 'Finished' button is highlighted with a red box.

(2) デバイスグループが作られた状態です。

The screenshot shows the 'Device Group List' page in the F5 Device Management interface. The table below shows the details of the newly created device group:

Group Name	Type	ConfigSync	ConfigSync Status	Members
Device-Group-001 (Includes Self)	Sync-Failover	Manual	Changes Pending	2

管理(マネージメント)IP アドレスの 4 オクテット目の数字が大きい方が、デフォルトで"Active"となります。

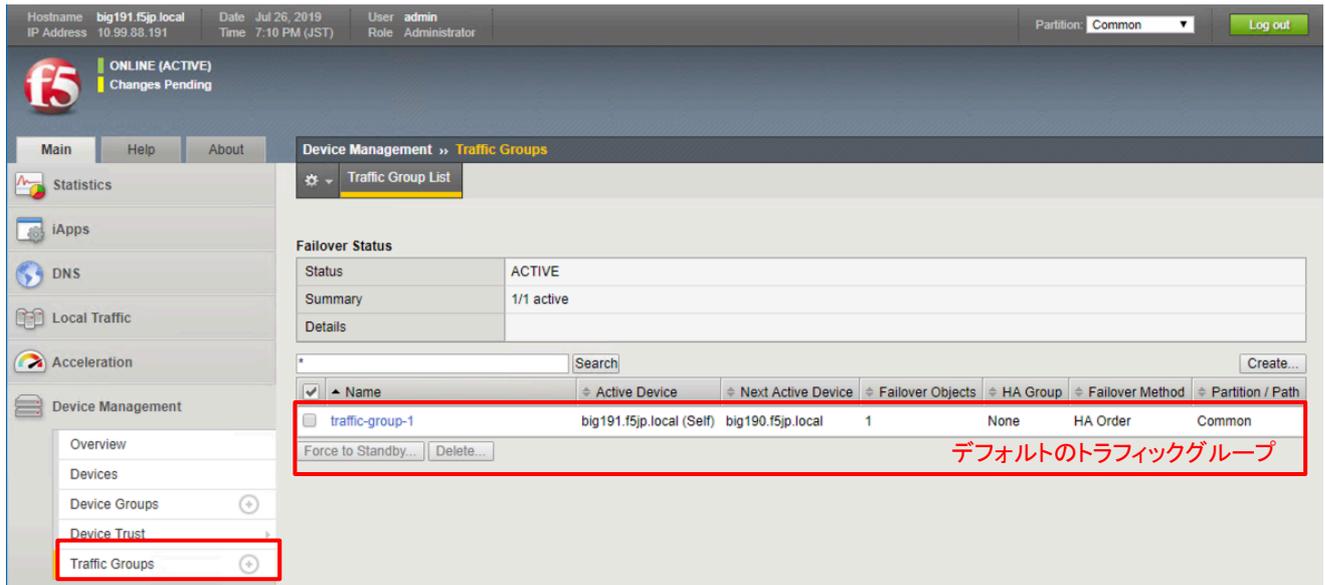
11.7. トラフィックグループの設定

トラフィックグループは、デバイスグループ内で移動するオブジェクトの集合です。
主に、Virtual Server と共有 IP(Floating IP)がトラフィックグループのオブジェクトです。

「Device Management」→「Traffic Groups」を確認します。

11.7.1. トラフィックグループの確認

デフォルトで、「Traffic-group-1」という名前のトラフィックグループが存在しています。
以降、この Traffic-group-1 に対して、Floating IP および Virtual Server を割当てていきます。
(ここでは確認のみです。)



The screenshot shows the F5 BIG-IP web interface. The top navigation bar includes the F5 logo, status indicators (ONLINE (ACTIVE), Changes Pending), and user information (User: admin, Role: Administrator). The main content area is titled "Device Management >> Traffic Groups" and contains a "Traffic Group List" section. Below this, there is a "Failover Status" section showing "Status: ACTIVE" and "Summary: 1/1 active". A table lists the traffic groups, with the first entry, "traffic-group-1", highlighted by a red box. The table columns are: Name, Active Device, Next Active Device, Failover Objects, HA Group, Failover Method, and Partition / Path. The values for "traffic-group-1" are: Name: traffic-group-1, Active Device: big191.f5jp.local (Self), Next Active Device: big190.f5jp.local, Failover Objects: 1, HA Group: None, Failover Method: HA Order, and Partition / Path: Common. A red annotation "デフォルトのトラフィックグループ" (Default Traffic Group) is placed to the right of the table row. The left sidebar shows the "Device Management" menu with "Traffic Groups" selected and highlighted by a red box.

Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
traffic-group-1	big191.f5jp.local (Self)	big190.f5jp.local	1	None	HA Order	Common

11.7.2. Floating IP の設定

Floating IP は、Active 機ダウン時に Standby 機が引き継ぐ、自身に設定された IP アドレス(Self IP)を指します。実サーバは、この IP アドレスをデフォルトゲートウェイに指定することで、Active/Standby の切り替わり発生時にも、即座に通信を再開できます。

(1) Internal VLAN 側の共用 IP(Floating IP)を追加設定します。

「Network」→「Self IPs」で表示された画面右上の「Create」ボタンを押し、表示された画面で以下のように設定します。

ここで、Traffic-group-1 を選択することで、そのトラフィックグループに属させます。

Field	Value	Annotation
Name	internal-flo-ip	名前(任意)を設定
IP Address	10.99.2.241 10.99.2.(24n)	フローティング IP アドレスを設定
Netmask	255.255.255.0	サブネットマスクを指定
VLAN / Tunnel	internal	VLAN を選択
Port Lockdown	Allow Default	この IP アドレス上のサービス(SSH/GUI 等)を許可
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)	「traffic-group-1」を選択
Service Policy	None	

Buttons: Cancel, Repeat, **Finished**

(2) External VLAN 側の共用 IP(Floating IP)も追加設定します。

Field	Value	Annotation
Name	external-flo-ip	名前(任意)を設定
IP Address	10.99.1.241 10.99.1.(24n)	フローティング IP アドレスを設定
Netmask	255.255.255.0	サブネットマスクを指定
VLAN / Tunnel	external	VLAN を選択
Port Lockdown	Allow None	この IP アドレス上のサービス(SSH/GUI 等)を停止
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)	「traffic-group-1」を選択
Service Policy	None	

Buttons: Cancel, Repeat, **Finished**

11.7.3. Virtual Server と Traffic-Group の紐付け(確認)

- (1) 「Local Traffic」→「Virtual Servers」→「Virtual Address List」を選択します。
この Properties の Traffic Group で、「traffic-group-1」が選択されていることを確認します。

Hostname big181.f5.jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 4:46 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Changes Pending

Main Help About Local Traffic » Virtual Servers : Virtual Address List » 10.99.1.81

Statistics iApps DNS Local Traffic Acceleration

General Properties

Name	10.99.1.81
Partition / Path	Common
Address	10.99.1.81
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating) 「traffic-group-1」が選択されていることを確認
Availability	<input checked="" type="radio"/>
State	Enabled
Auto Delete	<input checked="" type="checkbox"/>

Configuration

Availability Calculation	When any virtual server is available
Connection Limit	0
ARP	<input checked="" type="checkbox"/> Enabled
ICMP Echo	Always
Spanning	<input type="checkbox"/>
Route Advertisement	Disabled

Update Delete

11.7.4. Traffic Group に紐付けられたオブジェクトの確認

- (1) 「Device Management」→「Traffic Groups」の Traffic-group-1 をクリックし、「Failover Objects」タブをクリックして、中身を確認すると、フェイルオーバーオブジェクトは以下のようになっています。

Hostname big181.f5.jp.local Date Jul 1, 2019 User admin
IP Address 10.99.88.181 Time 4:48 PM (JST) Role Administrator Partition: Common Log out

ONLINE (ACTIVE)
Changes Pending

Main Help About Device Management » Traffic Groups » traffic-group-1

Statistics iApps DNS Local Traffic Acceleration Device Management

Failover Objects

Name	Address	Type	Partition / Path
10.99.1.81	10.99.1.81	Virtual Address	Common
external-flo-ip	10.99.1.241	Self IP	Common
internal-flo-ip	10.99.2.241	Self IP	Common

11.8. ConfigSync

Active 機(bigXXX.f5jp.local)のみに行った設定を、Standby 機(bigYYY.f5jp.local)に同期するために、ConfigSyncを行います。

「Device Management」→「Overview」を選択すると、2つの Device Group が作成されています。

I	device_trust_group	trust group に peer を設定すると、システムによって自動的に作成されます。peer の基本情報を Sync します。
II	Device-Group-001 (任意の名前)	前項で作成したユーザ設定領域のデータを Sync します。

I は自動で Sync されますが、II はデフォルトでマニュアル Sync の設定となっています。II は初回設定時、または UCS ファイルからデータをリストアした後に Sync を実施する必要があります。

(1) 「Device Management」→「Overview」を選択します。

Active 機(bigXXX.f5jp.local)を選択し、「Sync」ボタンを押すことで、コンフィグ同期が行われます。

The screenshot shows the F5 ConfigSync interface. At the top, it displays system information: Hostname big181.f5jp.local, Date Jul 1, 2019, Time 5:05 PM (JST), User admin, Role Administrator, Partition: Common, and a Log out button. The main content area is titled 'Device Management >> Overview'. Under 'Device Groups', 'Device-Group-001' is shown with a yellow 'Changes Pending' indicator, 2 Devices, Sync-Failover Group, Manual Sync, and 'No successful group sync'. A message box says 'Changes Pending' with a recommended action: 'Synchronize big181.f5jp.local to group Device-Group-001'. Below this, 'Recent Changes' lists 'big181.f5jp.local (Self)' with a yellow status and 'Awaiting initial Sync with Changes Pending', and 'big180.f5jp.local' with a blue status and 'Awaiting Initial Sync'. Under 'New Device Group Members', 'big180.f5jp.local' is listed with a blue status and 'Awaiting Initial Sync'. 'Sync Options' includes 'Push the selected device configuration to the group' (selected) and 'Pull the most recent configuration to the selected device'. A red box highlights the 'Sync' button. At the bottom, 'In Sync' shows 'device_trust_group' as 'In Sync' with 2 Devices, Sync-Only Group, Auto Sync, and 'In sync on 7/1/2019 at 16:29:44'.

(2) しばらく待って、コンフィグ同期が完了し、各ステータスがグリーンになり、状態が“In Sync”となります。

The screenshot shows the F5 ConfigSync interface after synchronization. The top system information is updated: Time 5:07 PM (JST). The 'Device Management >> Overview' page now shows 'Device-Group-001' with a green 'In Sync' indicator, 2 Devices, Sync-Failover Group, Manual Sync, and 'In sync on 7/1/2019 at 16:43:31'. A message box says 'In Sync' with the text 'All devices are in sync. There are no changes pending.' Below this, 'Recent Changes' lists 'big180.f5jp.local' and 'big181.f5jp.local (Self)', both with green status and 'In Sync'. 'Sync Options' now says 'No sync options are available.' At the bottom, 'In Sync' shows 'device_trust_group' as 'In Sync' with 2 Devices, Sync-Only Group, Auto Sync, and 'In sync on 7/1/2019 at 16:29:44'. The 'big180.f5jp.local' and 'big181.f5jp.local (Self)' devices in the 'Recent Changes' list are highlighted with red boxes.

11.9. Traffic-group-1 の Active/Standby の切替え

11.9.1. Traffic-group-1 の Active/Standby の切替え

デフォルトでは、管理 IP アドレス設定の大きい値を持つものが Traffic-group-1 の Active 機になりますが、マニュアルで強制的に Active と Standby を切替えます。

- (1) アクティブ機の「Device Management」→「Traffic Groups」から Traffic-group-1 を選択し、「Force to Standby」ボタンを押します。

The screenshot shows the F5 configuration interface. At the top, the status is 'ONLINE (ACTIVE) In Sync'. The left sidebar shows 'Device Management' > 'Traffic Groups'. The main content area is titled 'Device Management >> Traffic Groups' and shows the configuration for 'traffic-group-1'. The 'General Properties' section includes fields for Name, Partition / Path, Description, MAC Masquerade Address, Current Device (big181.f5jp.local), and Next Active Device (big180.f5jp.local). The 'Health Monitor' section shows 'HA Group' set to 'none'. The 'Failover Configuration' section includes 'Failover Method' (Failover using Preferred Device Order and then Load Aware), 'Failover Order' (Preferred Order and Load Aware), and 'HA Load Factor' (1). At the bottom, the 'Force to Standby' button is highlighted with a red box.

- (2) 確認のポップアップがでるので、「Force to Standby」ボタンを押します。

The screenshot shows a confirmation dialog box titled 'Force Traffic Group to Standby'. It contains a question mark icon and the text 'Are you sure you want to force this Traffic Group to standby?'. At the bottom, there are two buttons: 'Force to Standby' (highlighted with a red box) and 'Cancel'.

- (3) その結果、Active から Standby に変わります。

The screenshot shows the F5 configuration interface after the change. The status at the top is now 'ONLINE (STANDBY) In Sync'. The left sidebar shows 'Device Management' > 'Traffic Groups'. The main content area is titled 'Device Management >> Traffic Groups' and shows the 'Failover Status' for 'traffic-group-1'. The 'Status' field is highlighted with a red box and shows 'STANDBY'. Below this, there is a table listing the traffic groups and their configurations.

Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
traffic-group-1	big180.f5jp.local	big181.f5jp.local (Self)	3	None	HA Order	Common

(4) Standby だった BIG-IP は Active になります。

Hostname: big180.f5jp.local | Date: Jul 1, 2019 | User: admin | IP Address: 10.99.88.180 | Time: 5:13 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)
In Sync

Device Management » Traffic Groups

Traffic Group List

Failover Status

Status	ACTIVE
Summary	1/1 active
Details	

Search

Name	Active Device	Next Active Device	Failover Objects	HA Group	Failover Method	Partition / Path
traffic-group-1	big180.f5jp.local (Self)	big181.f5jp.local	3	None	HA Order	Common

Force to Standby... Delete...

11.9.2. クライアントからの接続確認

- (1) テスト用クライアントから、作成した Virtual Server へ Web ブラウザでアクセスし、Web 画面が表示されることを確認します。
- (2) 「Statistics」 → 「Module Statistics」 → 「Local Traffic」タブをクリックします。
「Statistics Type」のプルダウンメニューから、「Pools」を選択します。
それぞれの Web サーバの、Bits, Packets 等のカウントがアップしていることを確認し、ロードバランシングが正常に行われていることを確認します。

Hostname: big180.f5jp.local | Date: Jul 1, 2019 | User: admin | IP Address: 10.99.88.180 | Time: 5:16 PM (JST) | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)
In Sync

Statistics » Module Statistics : Local Traffic » Pools

Local Traffic

Display Options

Statistics Type: Pools

Data Format: Normalized

Auto Refresh: Disabled | Refresh

Status	Pool	Pool Member	Partition / Path	Bits		Packets		Connections			Requests		Request Queue	
				In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age	
<input checked="" type="checkbox"/>	http-pool-01	10.99.100.215:80	Common	10.6K	35.4K	11	11	0	2	2	2	0	0	
<input checked="" type="checkbox"/>		10.99.100.217:80	Common	5.1K	17.5K	5	5	0	1	1	1	0	0	
<input checked="" type="checkbox"/>		10.99.100.217:80	Common	5.6K	17.9K	6	6	0	1	1	1	0	0	

Reset

カウンタをリセットしたい場合には、「Status」左横のチェックボックスにチェックを入れて、「Reset」ボタンを押します。

- (3) 再度 traffic-group-1 の切替え、クライアントからの通信が復旧するかを確認してください。

12. コマンドラインによる設定

このセクションは、初期化状態の BIG-IP からロードバランシングができるまでと冗長化の状態までをコマンドラインで実施する手順です。

12.1. コンフィグの初期化(全消去)

- (1) 既述のセクション:「8. コンフィグの初期化(全消去)」を参照して、2つの BIG-IP のコンフィグを消去してください。

12.2. 初期設定

(1) GUI で実行されるウィザードの停止

```
(tmos)# modify sys global-settings gui-setup disabled
```

(2) ホスト名の指定

```
(tmos)# modify sys global-settings hostname bigXXX.f5jp.local
```

(3) 設定の確認

```
(tmos)# list sys global-settings
sys global-settings {
  gui-setup disabled
  hostname bigXXX.f5jp.local
  mgmt-dhcp disabled
}
```

(4) タイムゾーンの指定と確認

```
(tmos)# modify sys ntp timezone Japan
(tmos)# list sys ntp
sys ntp {
  timezone Japan
}
```

(5) admin のパスワード変更

```
(tmos)# modify auth password admin
changing password for admin
new password:
confirm password:
```

12.3. ネットワークの設定

(1) VLAN 設定と確認

```
(tmos)# create net vlan external interfaces replace-all-with { 1.1 }
(tmos)# create net vlan internal interfaces replace-all-with { 1.2 }
(tmos)# list net vlan
net vlan external {
  fwd-mode 13
  if-index 400
  interfaces {
    1.1 {}
  }
  tag 4094
}
net vlan internal {
  fwd-mode 13
  if-index 416
  interfaces {
    1.2 {}
  }
  tag 4093
}
```

(2) Self-IP の設定と確認

```
(tmos)# create net self external-ip address 10.99.1.XXX/24 vlan external
(tmos)# create net self internal-ip address 10.99.2.XXX/24 vlan internal allow-service default

(tmos)# list net self
net self internal-ip {
  address 10.99.2.XXX/24
  allow-service {
    default
  }
  traffic-group traffic-group-local-only
  vlan internal
}
net self external-ip {
  address 10.99.1.XXX/24
  traffic-group traffic-group-local-only
  vlan external
}
```

(3) ルーティングの設定と確認

```
(tmos)# create net route default-GW gw 10.99.1.254 network default
(tmos)# create net route Office-Servers gw 10.99.2.254 network 10.99.100.0/24

(tmos)# list net route
net route Office-Servers {
  gw 10.99.2.254
  network 10.99.100.0/24
}
net route default-GW {
  gw 10.99.1.254
  network default
}
```

12.4. Pool と Virtual Server の設定

12.4.1. HTTP(80)用 Pool と VS

(1) Pool 設定と確認

```
(tmos)# create ltm pool http-pool-01 { members add { 10.99.100.215:http { } 10.99.100.217:http { } } monitor http }
(tmos)# list ltm pool
ltm pool http-pool-01 {
  members {
    10.99.100.215:http {
      address 10.99.100.215
      session monitor-enabled
      state up
    }
    10.99.100.217:http {
      address 10.99.100.217
      session monitor-enabled
      state up
    }
  }
  monitor http
}
```

(2) VS 設定

```
(tmos)# create ltm virtual http-vs-001 { destination 10.99.1.ZZZ:http pool http-pool-01 profiles add { http }
source-address-translation { type automap } }
(tmos)# list ltm virtual
ltm virtual http-vs-001 {
  creation-time 2019-07-01:18:07:15
  destination 10.99.1.81:http
  ip-protocol tcp
  last-modified-time 2019-07-01:18:07:15
  mask 255.255.255.255
  pool http-pool-01
  profiles {
    http { }
    tcp { }
  }
  source 0.0.0.0/0
  source-address-translation {
    type automap
  }
  translate-address enabled
  translate-port enabled
  vs-index 23
}
```

(3) パーシステンス設定

```
(tmos)# modify ltm virtual http-vs-001 { persist replace-all-with { source_addr }}
(tmos)# list ltm virtual
ltm virtual http-vs-001 {
  creation-time 2019-07-01:18:07:15
  destination 10.99.1.81:http
  ip-protocol tcp
  last-modified-time 2019-07-01:18:07:15
  mask 255.255.255.255
  persist {
    source_addr {
      default yes
    }
  }
  pool http-pool-01
  profiles {
    http { }
    tcp { }
  }
  source 0.0.0.0/0
  source-address-translation {
    type automap
  }
  translate-address enabled
  translate-port enabled
  vs-index 23
}
```

12.4.2. SSH 用 VS

後の show コマンドで、コネクションテーブルの確認が行いやすいので、SSH 用 VS も作っておきます。

(1) Pool 設定

```
(tmos)# create ltm pool ssh-pool-001 { members add { 10.99.100.215:ssh { } 10.99.100.217:ssh { } }
monitor tcp }
(tmos)# list ltm pool ssh-pool-001
ltm pool ssh-pool-001 {
  members {
    10.99.100.215:ssh {
      address 10.99.100.215
      session monitor-enabled
      state up
    }
    10.99.100.217:ssh {
      address 10.99.100.217
      session monitor-enabled
      state up
    }
  }
  monitor tcp
}
```

(2) VS 設定

```
(tmos)# create ltm virtual ssh-vs-001 { destination 10.99.1.ZZZ:ssh pool ssh-pool-001 profiles replace-all-
with { tcp } source-address-translation { type automap } }
(tmos)# list ltm virtual ssh-vs-001
ltm virtual ssh-vs-001 {
  creation-time 2019-07-01:18:18:09
  destination 10.99.1.81:ssh
  ip-protocol tcp
  last-modified-time 2019-07-01:18:18:09
  mask 255.255.255.255
  pool ssh-pool-001
  profiles {
    tcp { }
  }
  source 0.0.0.0/0
  source-address-translation {
    type automap
  }
  translate-address enabled
  translate-port enabled
  vs-index 24
}
```

12.5. コンフィグの保存

```
(tmos)# save sys config
```

12.6. 冗長化設定

12.6.1. 1号機(XXX)での設定

(1) HA用VLANとSelf-IPの設定

```
(tmos)# create net vlan HA interfaces replace-all-with { 1.3 }  
(tmos)# create net self HA-ip address 10.99.3.XXX/24 vlan HA allow-service default
```

(2) Centralized management (cm)⇔Device Management 設定の変更

BIG-IP 間の冗長化では、各デバイスが持つ証明書によって信頼関係を結びます。
その証明書を、初期値のホスト名から、新しく設定したホスト名に変更します。
(GUI では自動的に実施してくれますが、CLI では必要なステップです。)

```
(tmos)# mv cm device bigip1 bigXXX.f5jp.local
```

(3) Device Management で、各 Device の Configsync、Mirror アドレス、Failover アドレスを設定した部分に該当します。

```
(tmos)# modify cm device bigXXX.f5jp.local { configsync-ip 10.99.3.XXX mirror-ip 10.99.3.XXX mirror-  
secondary-ip 10.99.2.XXX unicast-address {{ ip 10.99.3.XXX }} }
```

(4) 一旦 cm 設定を消去します。このことで、冗長化に必要な設定(証明書など)が新しいホスト名で再生成されます。

```
(tmos)# delete cm trust-domain all
```

(5) NTP 同期の設定をします。

```
(tmos)# modify sys ntp servers add { 10.99.2.219 }
```

一旦 TMSH から抜けて、BASH に戻り、NTP 同期状態を確認します。

```
(tmos)# quit  
config # ntpq -p  
remote refid st t when poll reach delay offset jitter  
=====
```

remote	refid	st	t	when	poll	reach	delay	offset	jitter
*10.99.2.219	133.243.238.243	2	u	6	64	1	1.854	0.561	0.357

```
=====
```

再び、TMSH へ戻ります。

```
config # tmsH  
(tmos)#
```

(6) コンフィグ保存

```
(tmos)# save sys config
```

12.6.2. 2号機(YYY)の設定

2号機で、冗長化に必要な設定を実施します。

(1) 初期設定

```
(tmos)# modify sys global-settings gui-setup disabled
(tmos)# modify sys global-settings hostname bigYYY.f5jp.local
(tmos)# modify sys ntp timezone Japan
```

(2) VLAN 設定

```
(tmos)# create net vlan external interfaces replace-all-with { 1.1 }
(tmos)# create net vlan internal interfaces replace-all-with { 1.2 }
(tmos)# create net vlan HA interfaces replace-all-with { 1.3 }
```

(3) Self-IP 設定

```
(tmos)# create net self external-ip address 10.99.1.YYY/24 vlan external
(tmos)# create net self internal-ip address 10.99.2.YYY/24 vlan internal allow-service default
(tmos)# create net self HA-ip address 10.99.3.YYY/24 vlan HA allow-service default
```

(4) 冗長化用の設定

```
(tmos)# mv cm device bigip1 bigYYY.f5jp.local
(tmos)# modify cm device bigYYY.f5jp.local { configsync-ip 10.99.3.YYY mirror-ip 10.99.3.YYY mirror-
secondary-ip 10.99.2.YYY unicast-address { { ip 10.99.3.YYY } } }
(tmos)# delete cm trust-domain all
```

(5) NTP 設定

```
(tmos)# modify sys ntp servers add { 10.99.2.219 }
```

(6) admin のパスワード変更

```
(tmos)# modify auth password admin
changing password for admin
new password:
confirm password:
```

(7) コンフィグ保存

```
(tmos)# save sys config
```

12.6.3. 再び 1号機(XXX)からの実行

(1) Device-Trust の実施

```
(tmos)# modify cm trust-domain Root add-device { device-ip 10.99.3.YYY device-name bigYYY.f5jp.local
username admin password peold4649 ca-device true }
```

(2) Device-Group の設定

```
(tmos)# create cm device-group Device-Group-001 { type sync-failover devices add { bigXXX.f5jp.local
bigYYY.f5jp.local } }
```

(3) Floating-IP の設定

```
(tmos)# create net self external-flo-ip address 10.99.1.24n/24 traffic-group traffic-group-1
vlan external
(tmos)# create net self internal-flo-ip address 10.99.2.24n/24 traffic-group traffic-group-1
vlan internal allow-service default
```

(4) コンフィグ保存

```
(tmos)# save sys config
```

(5) Config-Sync の実行

```
(tmos)# run cm config-sync to-group Device-Group-001
```

12.6.4 1号機(XXX)からの実行

冗長化を構成した最初だけ、アドレスの大きいほう Active になります。
よって、本ガイドでは、1号機(XXX)が Active となるので、Traffic-Group を 2号機(YYY)へ切り替えてみます。

```
(tmos)# run sys failover standby traffic-group traffic-group-1
```

冗長化はこれで終了です。

12.7. [参考]root のパスワード変更

root のパスワード変更を行いたい場合は、以下のコマンドを実行してください。

```
(tmos)# modify auth password root  
changing password for root  
new password:  
confirm password:  
  
(tmos)# save sys config
```

12.8. show コマンドのサンプル

いくつかの show コマンド(設定の確認コマンド)を記載します。

12.8.1. コネクションテーブルの確認

クライアント PC から、設定した SSH(22) Virtual Server へアクセスし、コネクションテーブルの状態を確認します。

(1) 現存する全コネクションの確認

```
(tmos)# show sys connection
Sys::Connections
10.99.3.YYY:60141 10.99.3.XXX:1026 10.99.3.YYY:60141 10.99.3.XXX:1026 udp 0 (tmm: 1) none
10.99.4.WW:52266 10.99.1.XXX:22 10.99.2.XXX:52266 10.99.100.215:22 tcp 10 (tmm: 0) none
10.99.3.XXX:59049 10.99.3.YYY:1026 10.99.3.XXX:59049 10.99.3.YYY:1026 udp 0 (tmm: 1) none
Total records returned: 3
```

(2) 確認したいコネクションの絞り込み

```
(tmos)# show sys connection cs-client-addr 10.99.4.WW
Sys::Connections
10.99.4.WW:52266 10.99.1.XXX:22 10.99.2.XXX:52266 10.99.100.215:22 tcp 7 (tmm: 0) none
Total records returned: 1
```

(3) 絞り込んだコネクションの詳細

```
(tmos)# show sys connection cs-client-addr 10.99.4.WW all-properties
Sys::Connections
10.99.4.WW:52266 - 10.99.1.XXX:22 - 10.99.2.XXX:52266 - 10.99.100.215:22
-----
TMM          0
Type         any
Acceleration none
Protocol     tcp
Idle Time    40
Idle Timeout 300
Unit ID      1
Lasthop      /Common/external 00:50:56:bd:65:b5
Virtual Path 10.99.1.XXX:22

ClientSide   ServerSide
Client Addr  10.99.4.WW:52266 10.99.2.XXX:52266
Server Addr  10.99.1.XXX:22     10.99.100.215:22
Bits In      31.4K              35.9K
Bits Out     37.5K              34.0K
Packets In   24                 26
Packets Out  31                 32
Total records returned: 1
```

12.8.2. ハードウェアに関わる情報(CPUの詳細やシリアル番号等)の確認

```
(tmos)# show sys hardware
```

12.8.3. 各パーティションの OS の確認

```
(tmos)# show sys software
```

12.8.4. 現在利用中の OS バージョンの確認

```
(tmos)# show sys version
```

12.8.5. Virtual Server の状態確認

```
(tmos)# show ltm virtual ssh-vs-001 raw
```

13. おわりに

基本的なセットアップに関しては以上で終了となります。

LTM には、送信元 IP やクッキーを用いたセッション維持、外部 Syslog サーバへの詳細な通信ログ送信、iRule と呼ばれるスクリプティング機能を利用したトラフィック処理のカスタマイズなど、本セットアップガイドにてカバーしきれない豊富な機能が実装されています。使い方次第で単純な負荷分散から高度なトラフィックコントロールまで、さまざまにご利用頂けます。

また LTM 以外の BIG-IP シリーズ製品ラインナップにおいては、ソフトウェアモジュールライセンスを追加することで広域負荷分散やファイアウォール機能、SSL-VPN 機能など、アプリケーションアクセスを最適化する為の多彩な機能が使用できるようになりますので、詳細は各種 WEB サイトにてご確認いただくか、F5 公式販売代理店にお問い合わせください。

<F5 ネットワークス WEB サイトの紹介>

F5 ネットワークスジャパン総合サイト

<https://f5.com/jp>

F5 のセキュリティ ソリューション

<https://f5.com/jp/products/security>

AskF5: ナレッジベース総合サイト(英語)

<https://support.f5.com/kb/en-us.html>

DevCentral: F5 ユーザコミュニティサイト(英語: アカウント登録が必要です)

<https://devcentral.f5.com/>

F5 公式販売代理店リスト

https://www.f5.com/ja_jp/partners/jp-find-a-partner

以上

更新日: 2019-10-15

本資料は設計・構築を補助するための情報提供を目的としています。内容についてできる限り正確を期すよう努めてはおりますが、いかなる明示または暗黙の保証も責任も負いかねます。本資料の情報は、使用先の責任において使用されるべきものであることをあらかじめご了承ください。この文書に記載された製品の仕様、ならびに動作に関しては各社ともにこれらを予告なく変更する場合があります。F5 製品の各機能やコマンドに関する正式な情報に関しては AskF5(<https://support.f5.com/>)の対応するハードウェアプラットフォーム、ソフトウェアバージョンに即してご確認下さい。

本資料の著作権は、F5 ネットワークスジャパン合同会社にあります。本文中にある製品名は、各社の商標または登録商標です。
