F5 Networks Japan Technical Information Documentation

F5 Networks, Inc.

2023 年 09 月 26 日

F5 2023 Read The Docs Guide

目次:

第 1 章　LTM の基礎 5
1.1 LTM 動作概要 5

第 2 章　L3 構成: スタンドアローン 7
2.1 L3 構成: スタンドアローンイメージ 7
2.2 L3 構成: スタンドアローンのネットワーク・サンプル 8

第 3 章　初期設定 9
3.1 管理ポートの IP アドレス設定 9
3.2 管理ポートへの SSH アクセス 10
3.3 管理ポートへの GUI アクセス 10

第 4 章　ネットワーク設定 15
4.1 VLAN の作成 15
4.2 Self IP の設定 16
4.3 ルーティングの設定 16

第 5 章　ロードバランシング設定 19
5.1 HTTP (Port 80) のロードバランシング設定 19
5.2 パーシステンス設定 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
5.4 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 23

第 6 章　iRules の使い方 33
6.1 User-Agent を取得する 33
6.2 User-Agent 毎にアクセス先 Pool Member を変える 35

第 7 章　UCS の取得 37

第 8 章　コンフィグの初期化 (全消去) 39
8.1 BIG-IP への SSH アクセス . . . 39
8.2 コンフィグの初期化 . . . 39

第 9 章　UCS のリストア 41

第 10 章　QKview の取得 47

第 11 章　L3 構成: 冗長化 49
11.1 L3 構成: 冗長化イメージ . . . 49
11.2 L3 構成: 冗長化のネットワークサンプル . . . 49
11.3 Active 機 (big50.f5jp.local) の設定 . . . 51
11.4 Standby 機 (big40.f5jp.local) の設定 . . . 53
11.5 デバイストラスト設定 ※ Active 機 (big50.f5jp.local) 側から実施 . . . 55
11.6 デバイスグループの設定 . . . 56
11.7 トラフィックグループの設定 . . . 56
11.8 ConfigSync . . . 58
11.9 Traffic-group-1 の Active/Standby の切替え . . . 59

第 12 章　コマンドラインによる設定 61
12.1 コンフィグの初期化 (全消去) . . . 61
12.2 初期設定 . . . 61
12.3 ネットワークの設定 . . . 62
12.4 Pool と Virtual Server の設定 . . . 63
12.5 コンフィグの保存 . . . 66
12.6 冗長化設定 . . . 66
12.7 root のパスワード変更 . . . 69
12.8 show コマンドのサンプル . . . 69

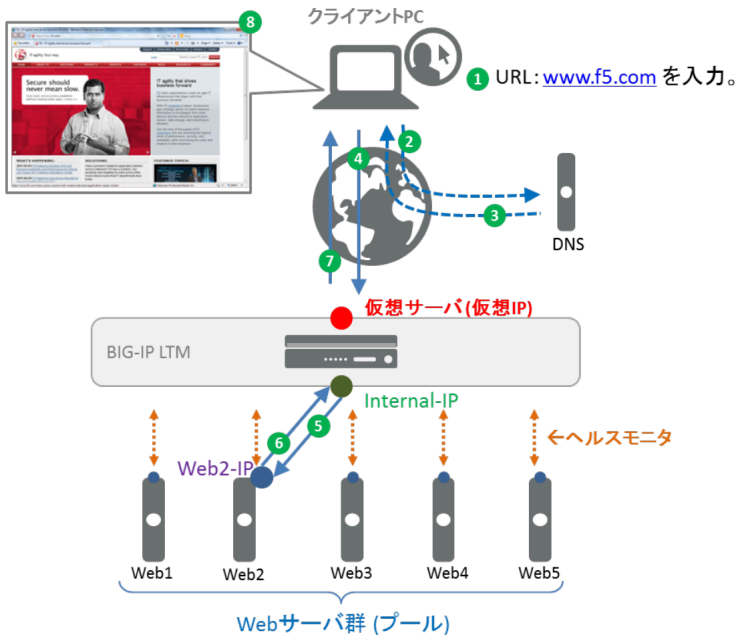
第 13 章　おわりに 73

1 LTM の基礎

本章では、基本的な LTM の設定内容についてご紹介致します。

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、定期的なヘルスモニタリングにて稼動監視を行っています。

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。

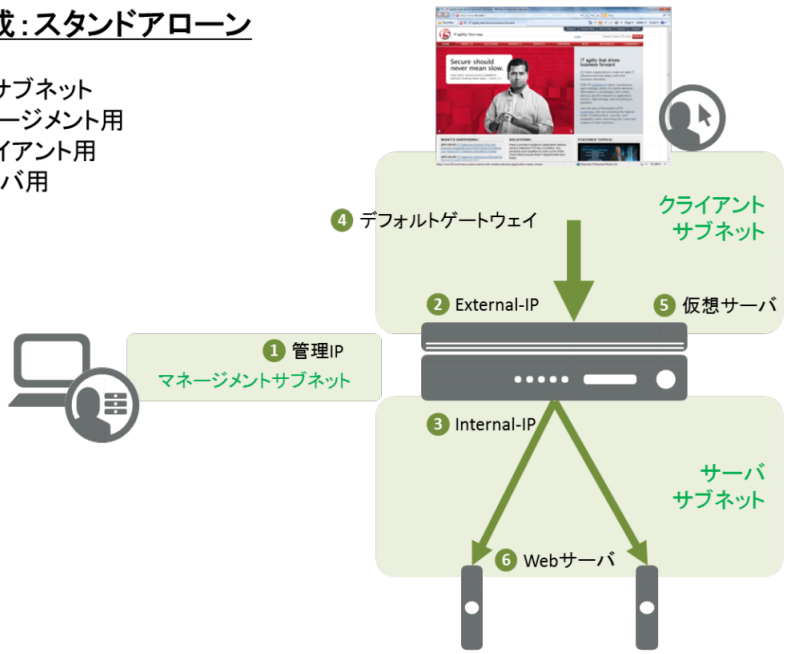
4. Web ブラウザは、その IP アドレス (仮想サーバ) 宛に HTTP リクエストを送信。
5. BIG-IP LTM は、Web サーバ群の中から 1 台 (この例では Web2) を選び、宛先アドレスを変換して HTTP リクエストを転送。
6. Web サーバ (Web2) は、その HTTP リクエストに対する HTTP レスポンスを送信。
7. HTTP レスポンスを受けとった BIG-IP LTM は、送信元アドレス変換を行い、その HTTP レスポンスをクライアント PC へ転送。
8. www.f5.com の Web ページが表示される。

2 L3 構成: スタンドアローン

本章では、スタンドアローンの L3 構成についてご紹介致します。

2.1 L3 構成: スタンドアローンイメージ

構成イメージは、以下の通りです。



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 1,7,8 は、以下が設定されています。

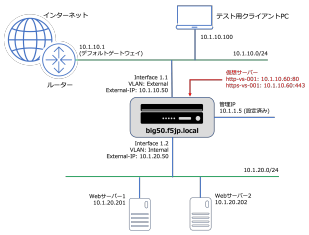
1 (管理 IP): 192.168.1.245/24

7 (CLI パスワード): **default**

8 (GUI パスワード): **admin**

2.2 L3 構成: スタンドアローンのネットワーク・サンプル

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"10.1.10.60:80"と"10.1.10.60:443"の 2 つを設定します。

プールメンバーは、以下の 2 つです。

10.1.20.201:80

10.1.20.202:80

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"10.1.10.1"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 PC」) から行います。

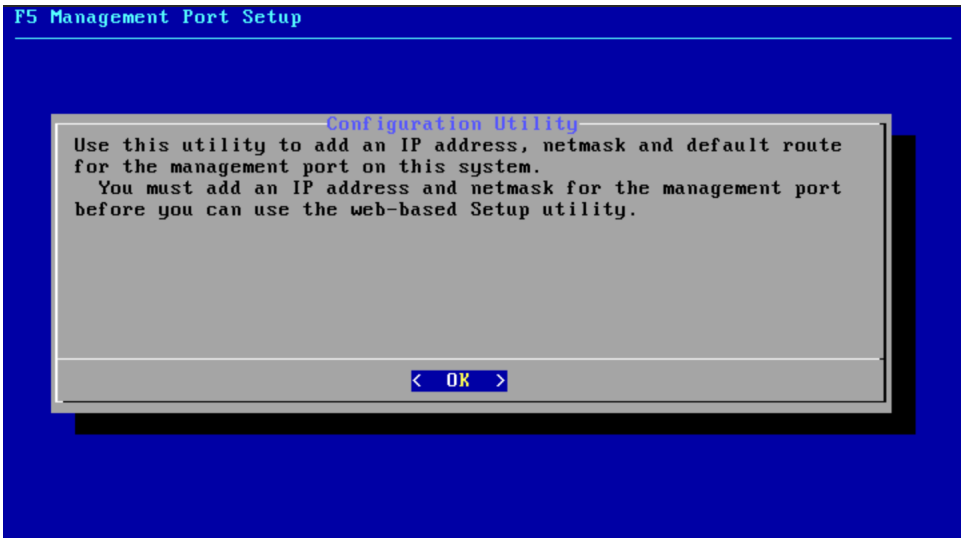
3 初期設定

3.1 管理ポートの IP アドレス設定

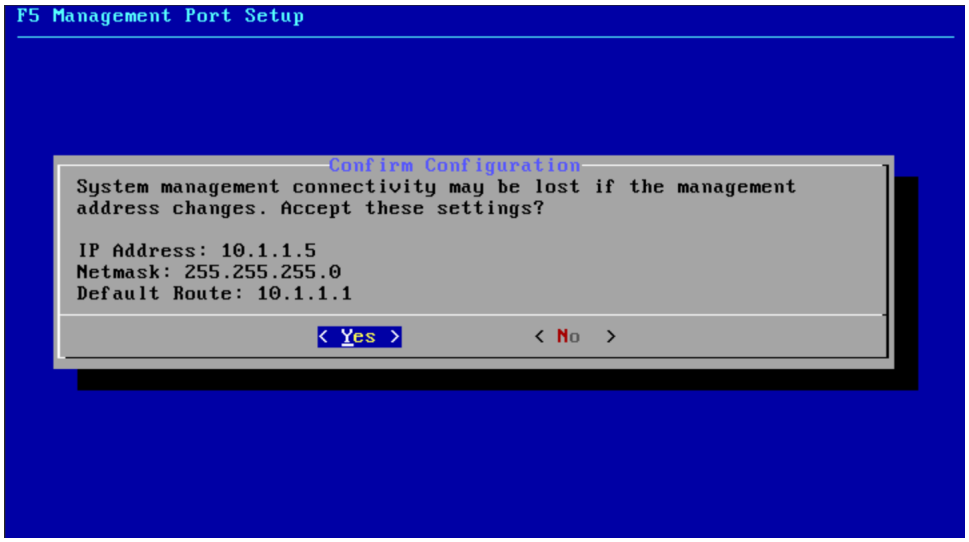
注釈: F5 UDF Lab では設定済みなので、実施不要です。UDF Lab をご利用の方は、本ページ下部の"Next"をクリックして、次のページへ進んでください。

最初に、BIG-IP の管理ポートに IP アドレスを設定します。

- コンソールポートに root ユーザーでログインして、「config」と入力し、管理ポートの設定ユーティリティを起動します。

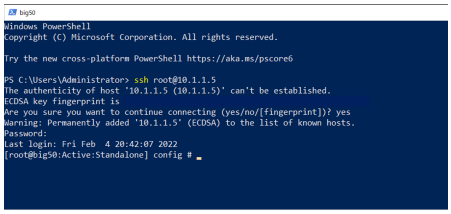


- 管理ポートの IP アドレス (IPv4/IPv6)、サブネットマスク、デフォルトルートを設定します。DHCP で動的に取得する設定も可能です。設定を確認後、「Yes」を選択して終了します。



3.2 管理ポートへの SSH アクセス

- BIG-IP に対して、ターミナルソフトを使って SSH アクセスが可能です。F5 UDF Lab では、テスト用クライアント PC の PowerShell やコマンドプロンプトから、SSH コマンドでアクセスできます。



- ログインすると、以下のようなコマンドプロンプトが表示されます。

```
[root@big50:Active:Standalone] config #
```

- SSH Key を設定して UDF Lab 上の BIG-IP にアクセスする方法については、以下の情報をご参照ください。

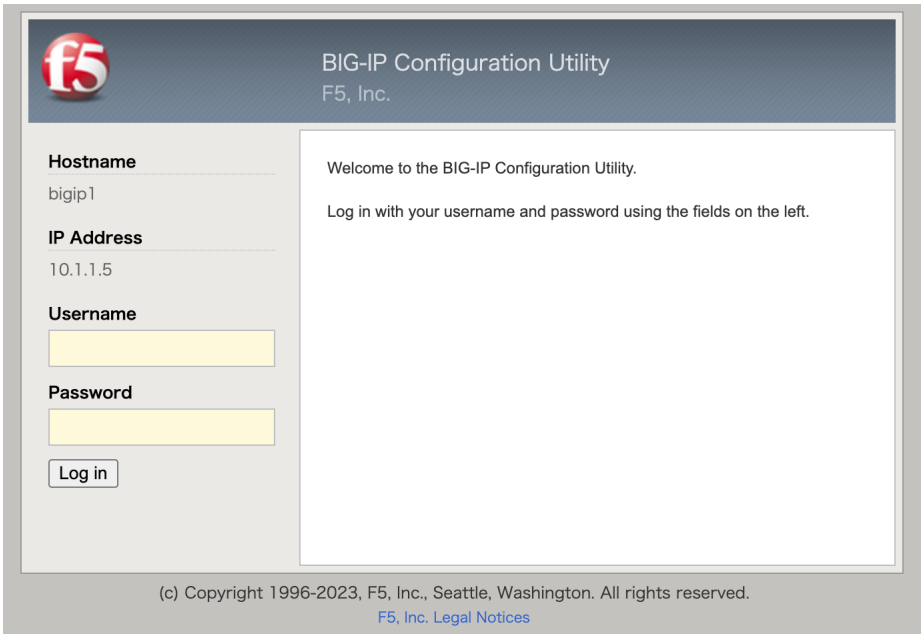
https://help.udf.f5.com/en/articles/3832165-how-to-join-an-f5-training-course

3.3 管理ポートへの GUI アクセス

- 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。
- 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。

Username: **admin**

Password: **admin**



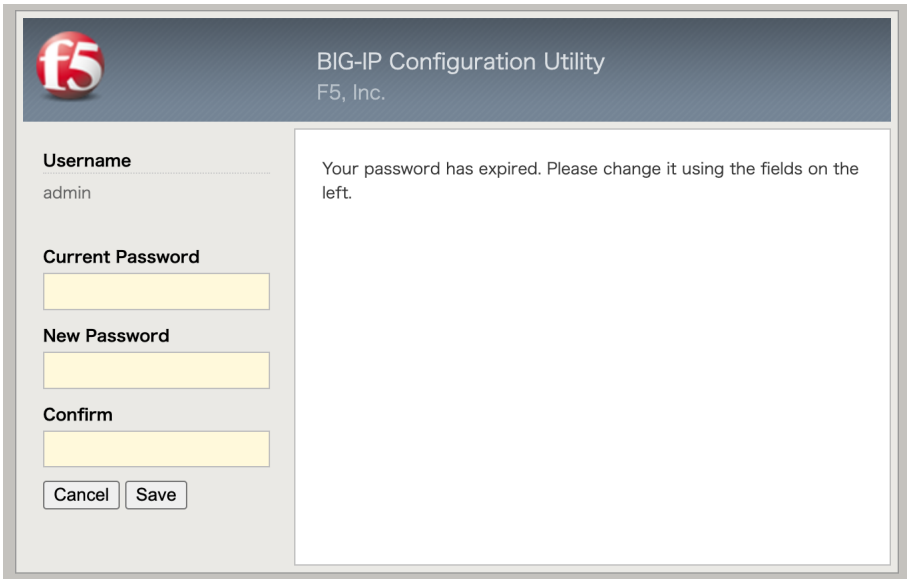
注釈: バージョン 14.0 より、デフォルトで BIG-IP のセキュアパスワードポリシーが有効となっています。パスワードポリシーを変更しない限り、v13.0 以前のデフォルトパスワードは利用できません。

本ガイドでは以下のように設定し、「Save」ボタンを押します。

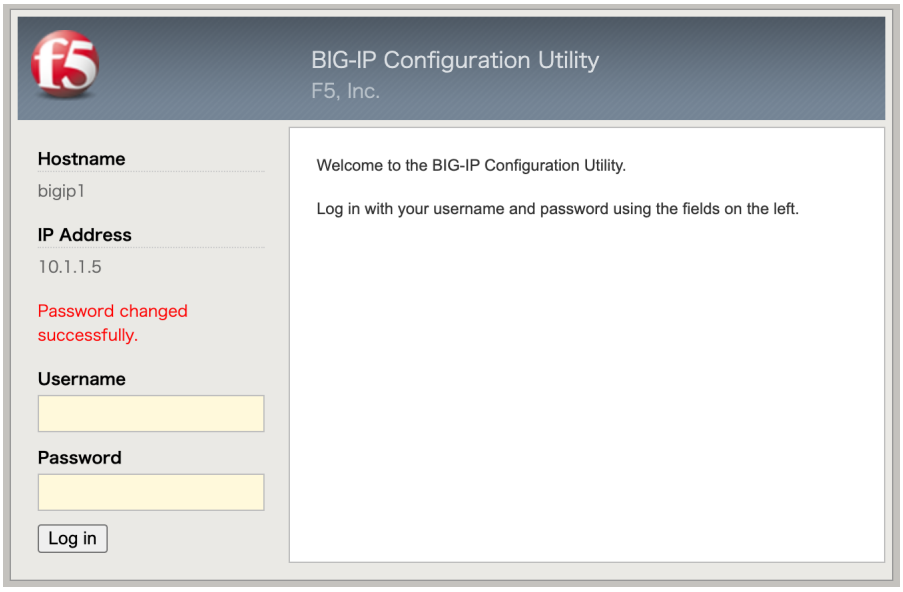
Current Password: **admin**

New Password: **ilovef5**

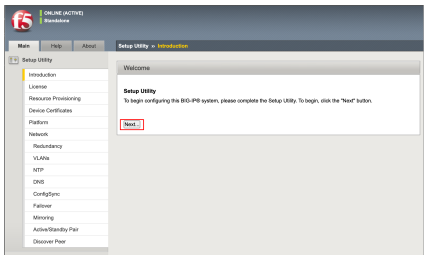
Confirm: **ilovef5**

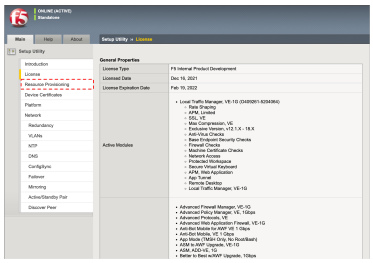


- 設定したパスワードでログインし直します。



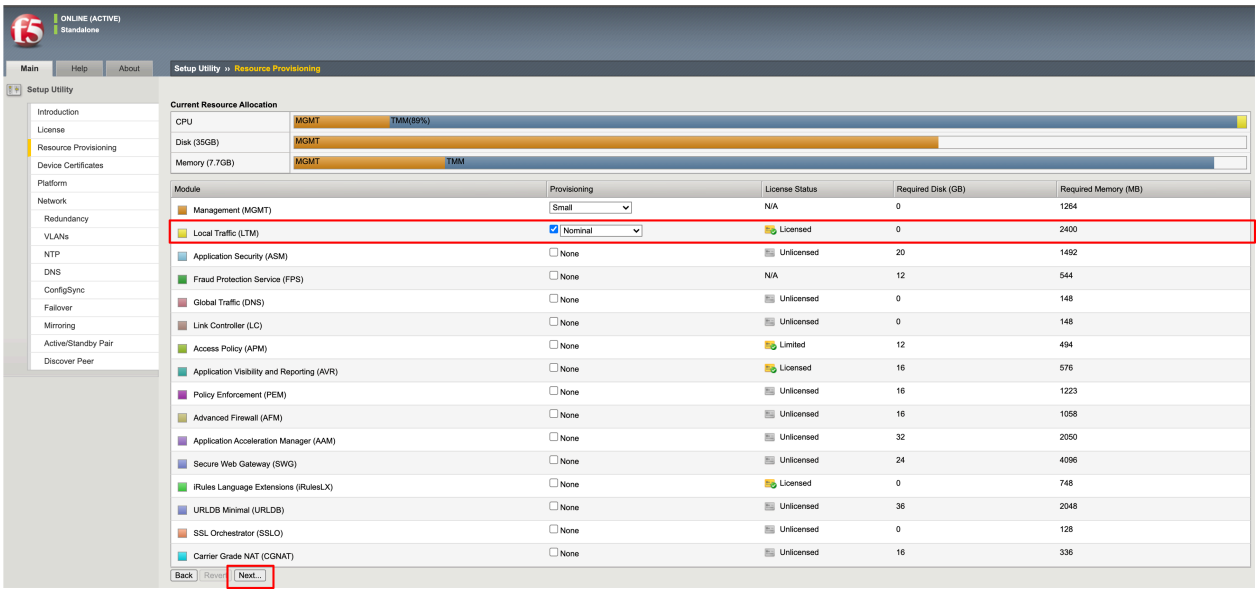
- 「Next」ボタンを押します。
- ライセンス画面が出ます。「Next」ボタンを押します。





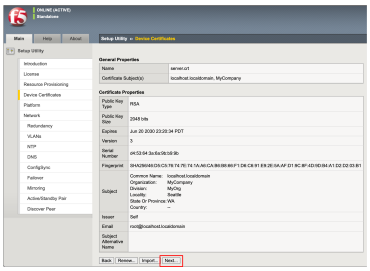
(中略)

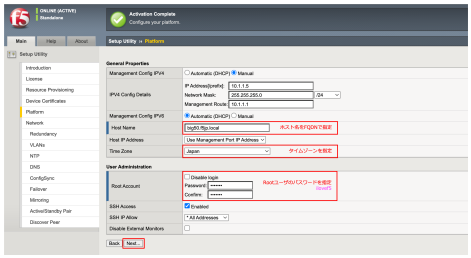
- プロビジョニング画面がでますが、デフォルトで LTM が選択されているので、そのまま「Next」ボタンを押します。



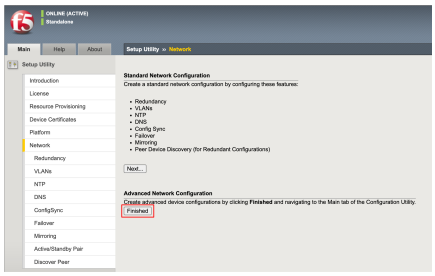
- SSL 証明書の確認がなされますが、デフォルトのまま、「Next」ボタンを押します。
- ホスト名、タイムゾーン、Root のパスワードを設定します。「Next」ボタンを押します。

注釈: IPv4 アドレスについては、F5 UDF Lab では設定済みなので、変更不要です。





- 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。



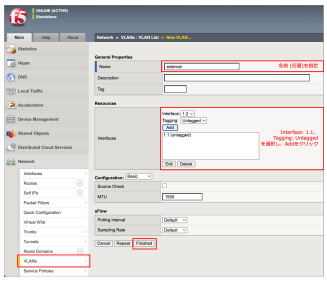
4 ネットワーク設定

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。

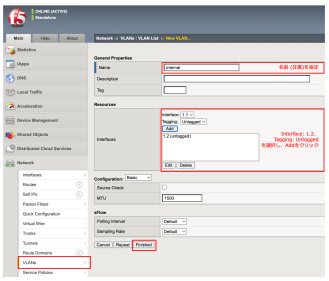
4.1 VLAN の作成

「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。

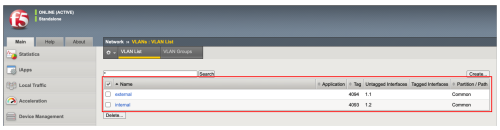
- External VLAN を設定します。



- Internal VLAN を設定します。



- 設定後は、以下の状態になります。

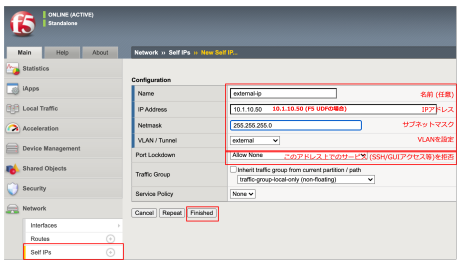


4.2 Self IP の設定

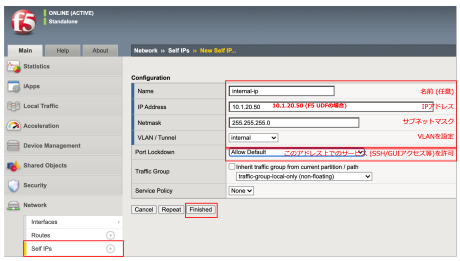
BIG-IP に設定した VLAN それぞれに対して、IP アドレスを設定します。この IP アドレスのことを “ Self IP “ と呼びます。

「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。

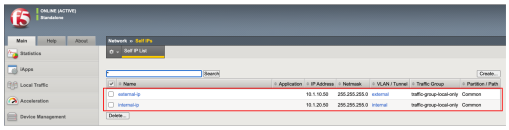
- External VLAN の Self IP を設定します。



- Internal VLAN の Self IP を設定します。



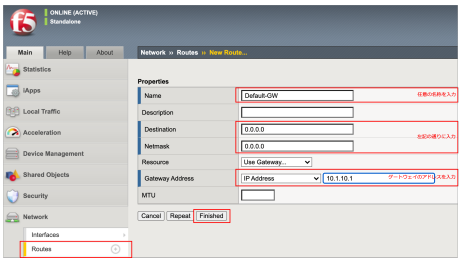
- 一覧では、以下のような状態になります。



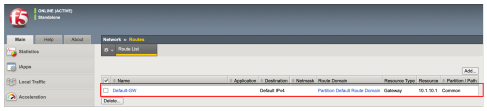
4.3 ルーティングの設定

4.3.1 デフォルトゲートウェイの設定

- 「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。



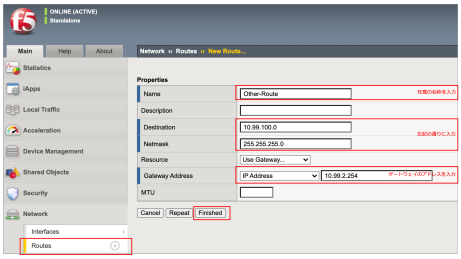
- 設定後は、以下の状態になります。



4.3.2 その他ルーティング設定 (参考)

- 例として 10.99.100.0/24 へ到達するためのルーティングを、同様に設定します

注釈: F5 UDF Lab では設定不要です。



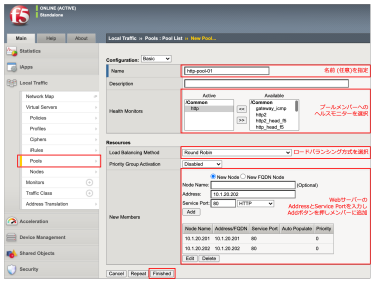
5 ロードバランシング設定

5.1 HTTP (Port 80) のロードバランシング設定

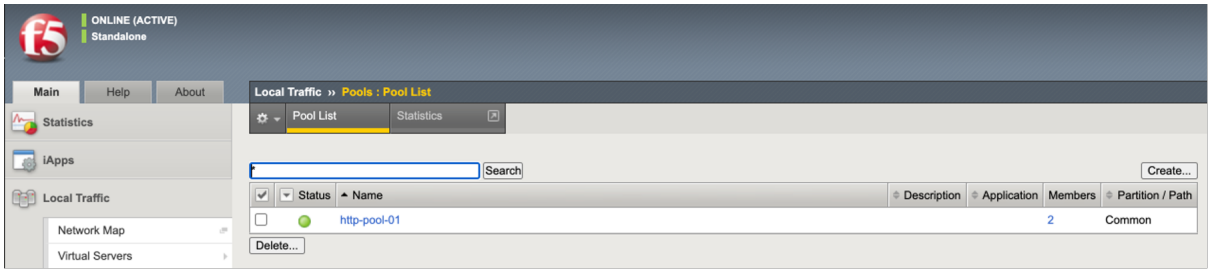
5.1.1 Pool の作成

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。

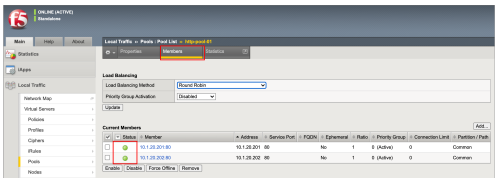
- 「Local Traffic」 → 「Pools」で表示された画面の右上にある「Create」ボタンを押します。



- Pool が作成されると、以下の状態になります。



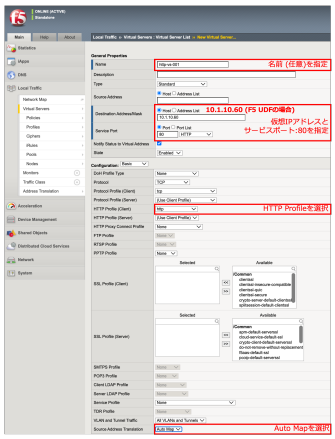
- 作成した「http-pool-01」をクリックし、「Members」タブをクリックします。以下のように、Status がグリーンであればヘルスモニターが成功しています。



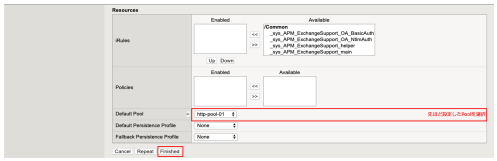
5.1.2 HTTP (80) の Virtual Server の作成

次に HTTP Virtual Server (Port 80) を作成します。

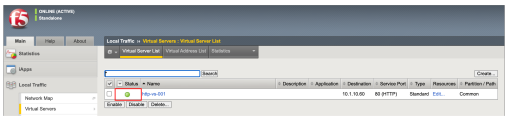
- 「Local Traffic」 → 「Virtual Servers」で表示された画面の右上にある「Create」ボタンを押して表示された画面で、以下のように設定します。



(中略)



- 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。

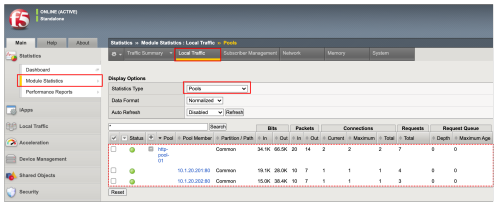


5.1.3 クライアントからの HTTP アクセス

- 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」 → 「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。



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: 買い物系サイト，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タンス

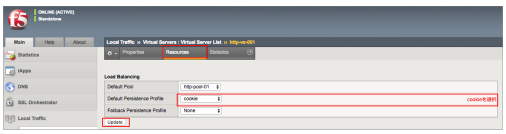
- 「Local Traffic」→「Virtual Servers」で表示されたバーチャルサーバ : http-vs-001 を選択し、Resources タブをクリックすると、以下の画面が表示されます。
- 以下のように設定します。

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。Statictics を見て、負荷分散されずに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 によるパーシスタンス

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

クライアントからの *HTTP* アクセス 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。

＜参考＞ Google Chrome の場合の確認手順

- 画面右上の「?」をクリックし、「その他のツール」 → 「デベロッパー ツール」を選択します。
- 「Application (アプリケーション)」タブを選択し、「Storage (ストレージ)」 → 「Cookies (Cookie)」を選択して、Cookie の内容を確認します。

注釈: 確認ができたら、次項以降のテストのために、Persistance Profile を Virtual Server の設定からはずします。

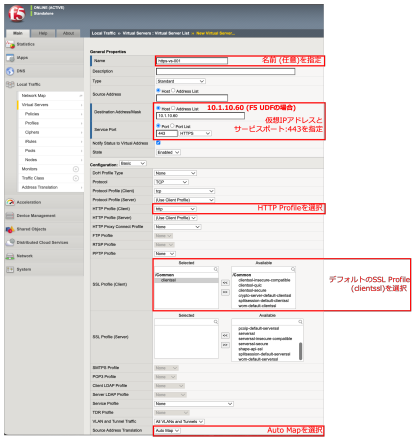
5.3 HTTPS (Port 443) のロードバランシング設定: ［パターン A］簡易的な設定方法

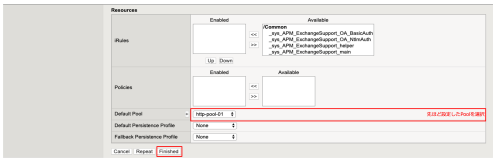
HTTPS 仮想サーバとして動作することだけを確認するのであれば、デフォルトで用意されている SSL Profile を使うことで、容易に実施できます。

5.3.1 HTTPS バーチャルサーバの設定

- 「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。

(中略)





5.3.2 クライアントからの HTTPS アクセス

> **クライアントからの *HTTP* アクセス** 参照。

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。

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:ベリサイン等) 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。

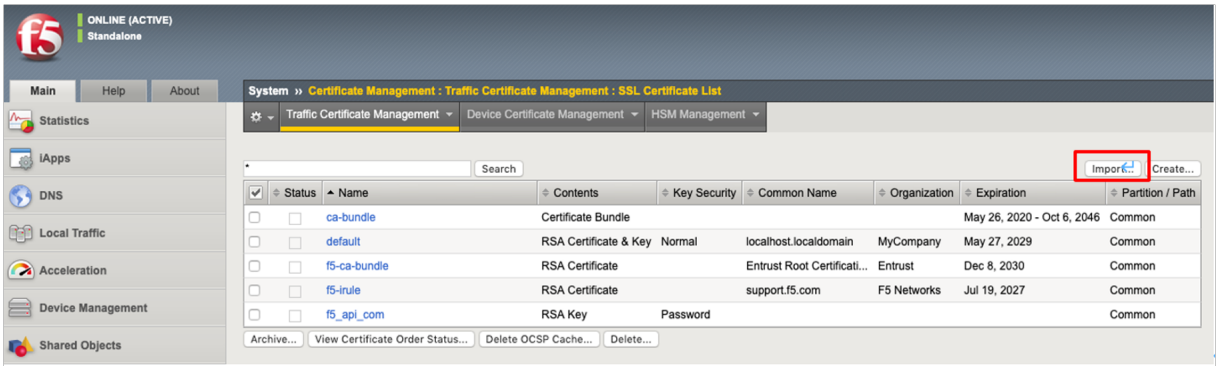
(F5 UDF Lab の場合) リモートデスクトップ接続した PC のデスクトップ上にある、以下のフォルダを開いてください。

このフォルダ内の以下 2 つのファイルを使用します。

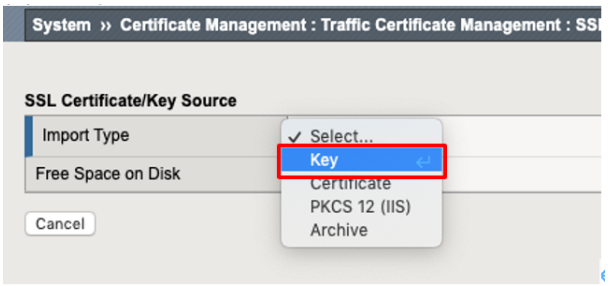
1. 秘密鍵ファイル: **abcCompany-key.pem**
2. サーバ証明書ファイル: **abcCompany-cert.pem**

5.4.2 秘密鍵とサーバ証明書のインポート

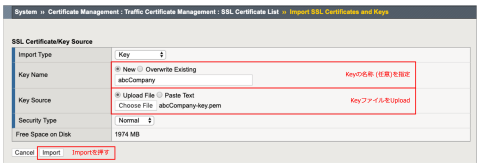
- まず、サーバの秘密鍵をインポートします。
- 「System」→「Certificate Management」→「Traffic Certificate Management」→「SSL Certificate List」で表示された画面右上の「Import」ボタンを押します。

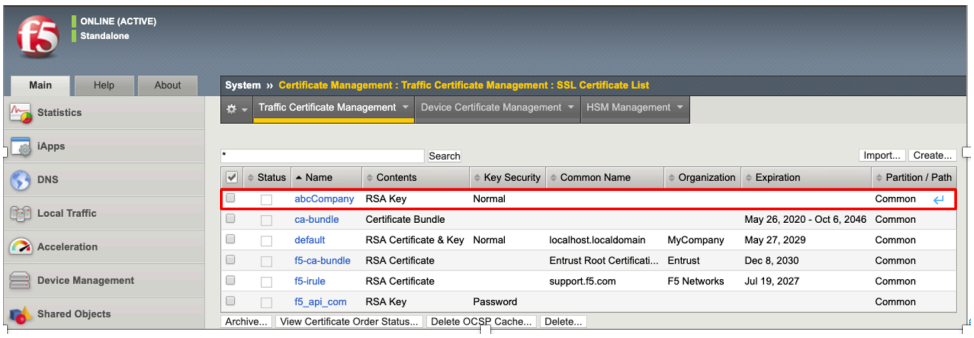


- Key を選択します。



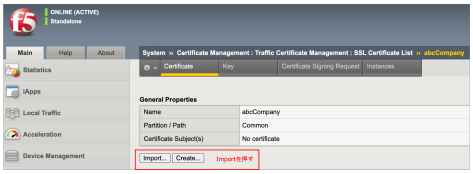
- 以下のように設定します。



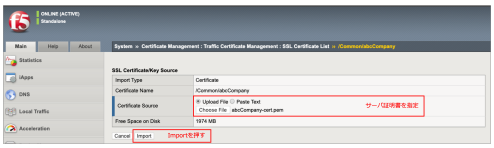


- 以下の状態になります。

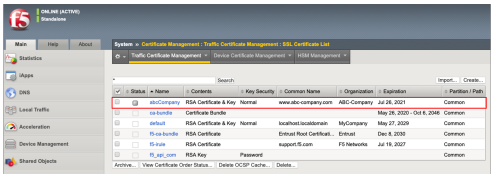
- 次に、サーバ証明書をインポートします。インポートした秘密鍵をクリックすると、以下の画面が現れます。「Import」ボタンを押します。



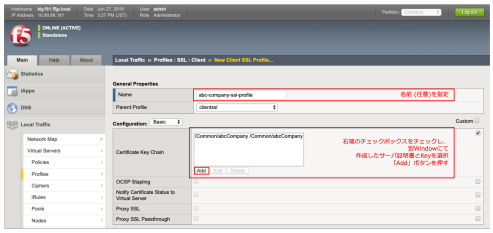
- 以下のように設定して、インポートします。



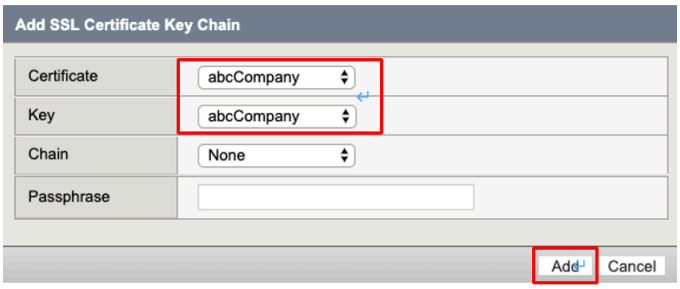
- サーバ証明書がインポートされた状態です。

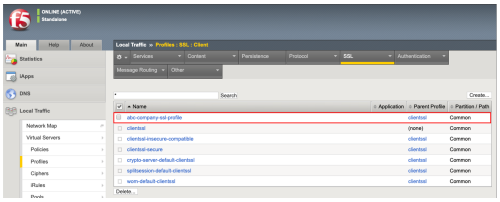


- Client SSL Profile を作ります。「Local Traffic」 → 「Profiles」 → 「SSL」 → 「Client」で表示された画面右上の「Create」ボタンを押すと、以下の画面が表示されますので、以下のように設定します。

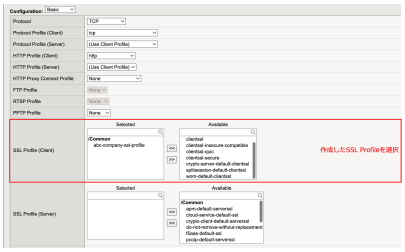


- 「Finished」ボタンを押すと、以下のようになります。





- ［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。



(省略)

5.4.3 クライアント PC の設定

注釈: F5 UDF Lab 環境では、CA 証明書はクライアントに設定済みです。hosts ファイルも編集済みです。

認証局の証明書のインポート

- 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。

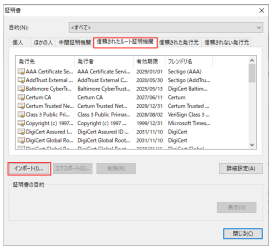
リモートデスクトップ接続した PC のデスクトップ上にある、以下のフォルダを開いてください。

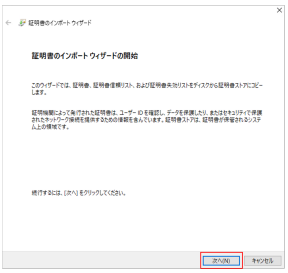
このフォルダ内の以下のファイルを利用します。

認証局ファイル: **cacert.pem**

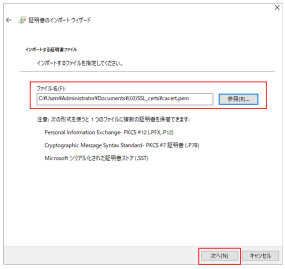
以下の手順でクライアント PC の Web ブラウザ (例: Chrome) へインポートします。

- 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、「プライバシーとセキュリティ」 → 「セキュリティ」 → 「デバイス証明書の管理」を選択します。
- 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。
- 「次へ」を押して下さい。

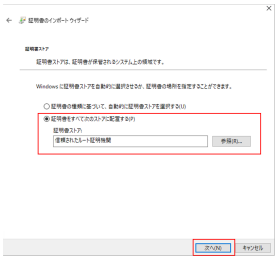




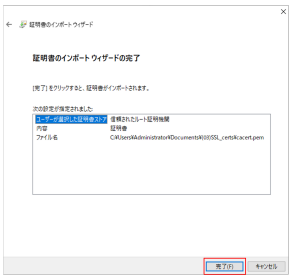
- インポートするファイルとして、認証局の証明書 (cacert.pem) を選び、「次へ」を押してください。



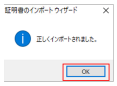
- 証明書ストアが「信頼されたルート証明機関」であることを確認し、「次へ」を押してください。



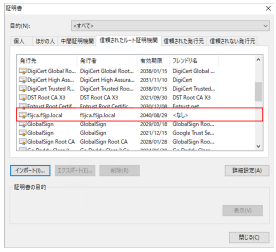
- 「完了」を押してください。
- 以下のようなセキュリティ警告が表示された場合、ここでは「はい」を選択します。



- 完了です。「OK」を押してください。



- 「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。

クライアント PC の hosts ファイルの編集

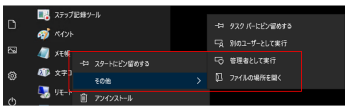
- DNS による名前解決ができない環境の場合、URL として IP アドレスを入力することになります。この場合、クライアント PC へ認証局の証明書をインポートしても、引き続き、以下の画面が表示されます。

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。

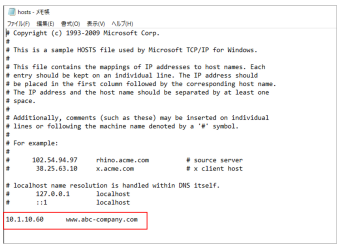
検証環境で比較的簡単に回避するためには、クライアント PC: Windows の hosts ファイルを編集することです。

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

- Windows の「メモ帳」アプリを、管理者権限で実行します。



- C:WindowsSystem32driversetchosts 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、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、BIG-IP の Virtual Server 経由で Web サーバ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

クライアントからの *HTTP* アクセス 参照。

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。

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) から実行可能です。
また、F5 DevCentral が推奨する Visual Studio Code (VS Code) 向けの拡張機能として、「F5 Networks iRules (https://marketplace.visualstudio.com/items?itemName=bitwisecook.irule)」があります。

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、10.1.20.201:80 へ
- Chrome (Firefox 以外のブラウザ) の場合は、10.1.20.202:80 へ

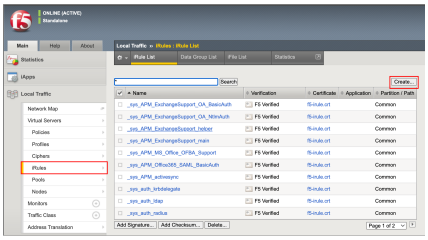
接続する、というルールを作成します。

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。

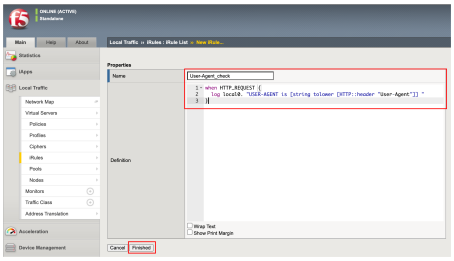
6.1.1 User-Agent ヘッダによる制御

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

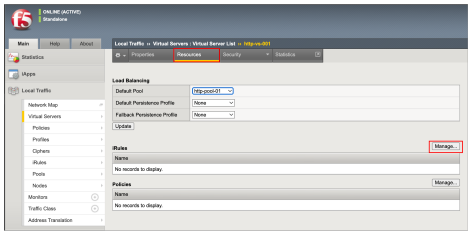


- User-Agent を、ログファイルへ出力する iRule を入力します。設定後、Finished ボタンを押します。

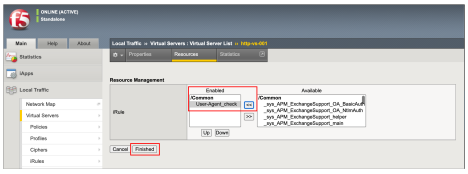
```
when HTTP_REQUEST {
  log local0. "USER-AGENT is [string tolower [HTTP::header "User-Agent"]] "
}
```



- 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。

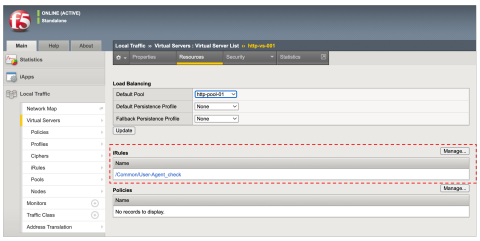


- 作成した iRule を選択し、「<<」ボタンを押します。



- 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

管理ポートへの *SSH* アクセス を参照。

6.1.3 User-Agent をログ上で確認

- 以下のコマンドを実行します。

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。

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

- クライアント PC で、iRule を設定した Virutal Server へ、Chrome および Firefox から以下 2 つのブラウザからアクセスします。
- /var/log/ltm に、以下のようなログ (例) が出力されます。

Chrome の場合

```
Jun 27 17:44:11 big50 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
```

Firefox の場合

```
Jun 27 17:43:53 big50 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 10.1.20.201:80 へ送り、それ以外は、10.1.20.202:80 へ送る、というルールを設定することにします。

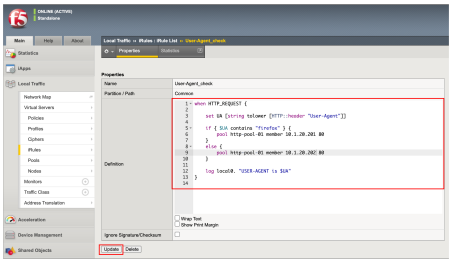
- 先程作成した iRules を以下のように変更します。Update ボタンを押します。

```
when HTTP_REQUEST {

    set UA [string tolower [HTTP::header "User-Agent"]]

    if { $UA contains "firefox" } {
        pool http-pool-01 member 10.1.20.201 80
    }
    else {
        pool http-pool-01 member 10.1.20.202 80
    }

    log local0. "USER-AGENT is $UA"
}
```

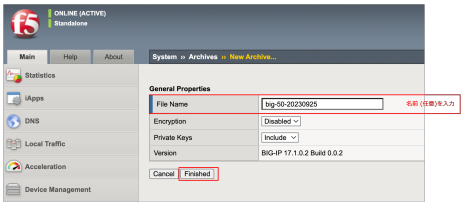


- クライアント PC で、iRule を設定した Virtual Server へ、Firefox および Chrome からアクセスします。
- それぞれが、iRule で指定した Pool Member へのみアクセスしていることを確認します。
- iRule 内の Pool Member の IP アドレスを入れ替えてみて、同様の確認を実施してみてください。Firefox と Chrome で、アクセス先が入れ替わります。

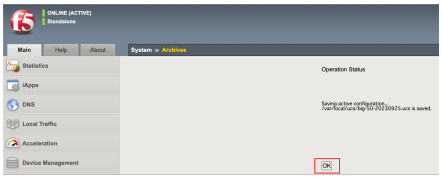
7 UCS の取得

UCS (User Configuration Set) アーカイブを取得することで、現時点までの設定を保存しておくことができます。

- 「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。



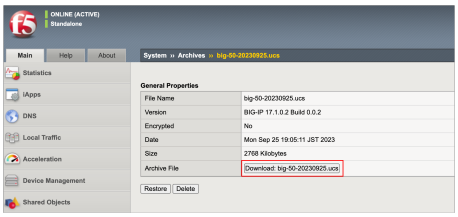
- 「OK」ボタンを押します。

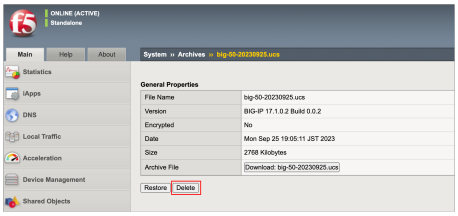


- 以下の状態になります。

- 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。
- 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。

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。


ONLINE (ACTIVE)
Standalone
Main
Help
About
Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
System » Archives » big-50-20230925.ucs
General Properties
File Name
big-50-20230925.ucs
Version
BIG-IP 17.1.0.2 Build 0.0.2
Encrypted
No
Date
Mon Sep 25 19:05:11 JST 2023
Size
2768 Kilobytes
Archive File
Download: big-50-20230925.ucs
Restore
Delete


ONLINE (ACTIVE)
Standalone
Main
Help
About
Statistics
iApps
DNS
Local Traffic
Acceleration
Device Management
Shared Objects
System » Archives » big-50-20230925.ucs
General Properties
File Name
big-50-20230925.ucs
Version
BIG-IP 17.1.0.2 Build 0.0.2
Encrypted
No
Date
Mon Sep 25 19:05:11 JST 2023
Size
2768 Kilobytes
Archive File
Download: big-50-20230925.ucs
Restore
Delete

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

管理ポートへの *SSH* アクセス を参照。

注釈: 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 (big50.f5jp.local) の全設定を消去し、デフォルト状態に戻します。

- TMSH への移行

SSH 等で BIG-IP の Linux OS Shell にアクセスした状態で以下のコマンドを実行します。

```
[root@big40:Active:Standalone] config # tmsh
root@(big40)(cfg-sync Standalone)(Active)(/Common)(tmos)#
```

- 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 とインプットします。)
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
```

- 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 (big50.f5jp.local) を、UCS ファイルで復元します。

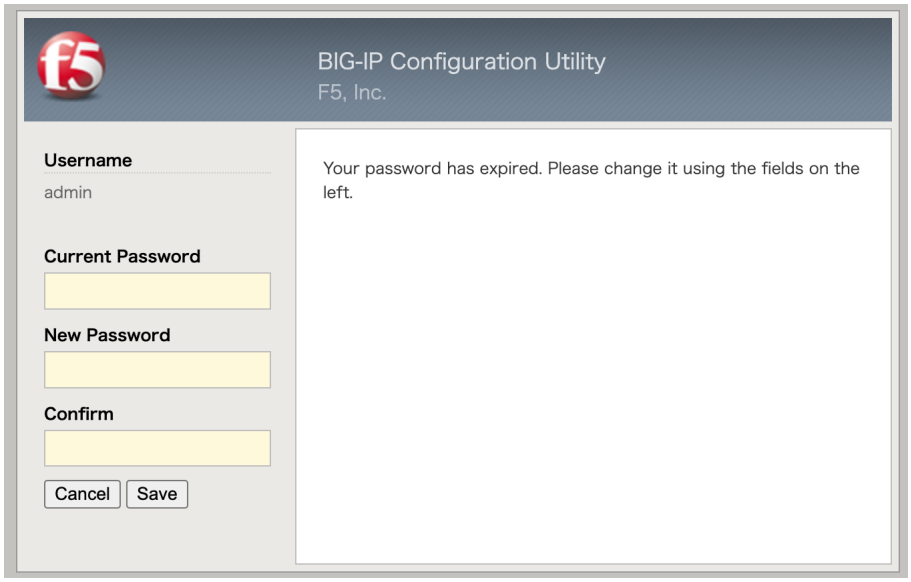
- 一度デフォルドパスワード (admin/admin) でログオンし、パスワードを再設定します。

F5 LAB では以下のように設定し、Save ボタンを押します。

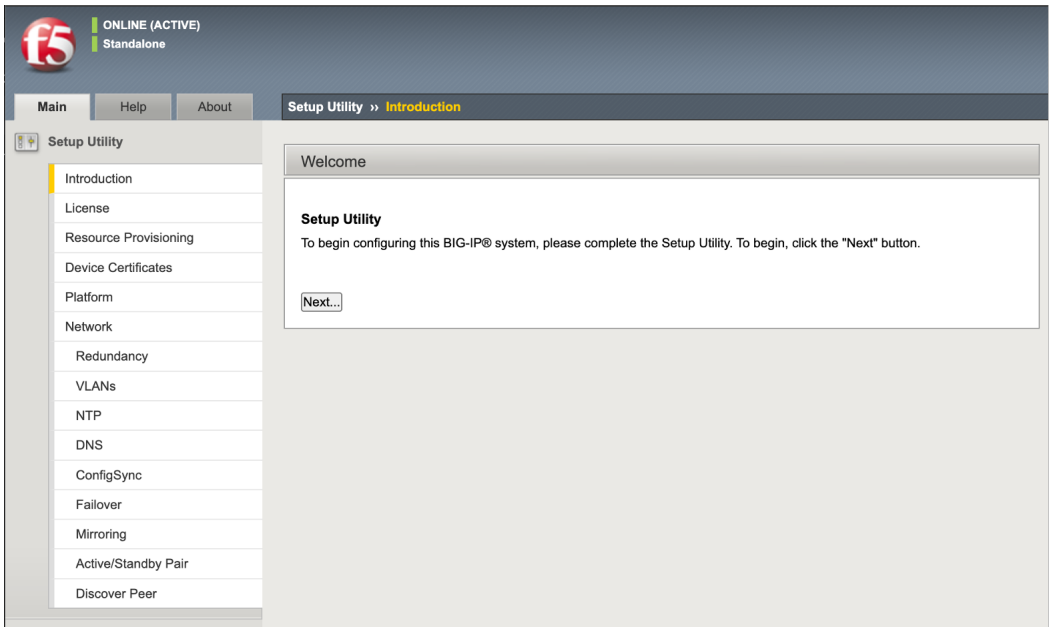
Current Password: **admin**

New Password: **ilovef5**

Confirm: **ilovef5**



- 設定したパスワードでログインします。
- 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。

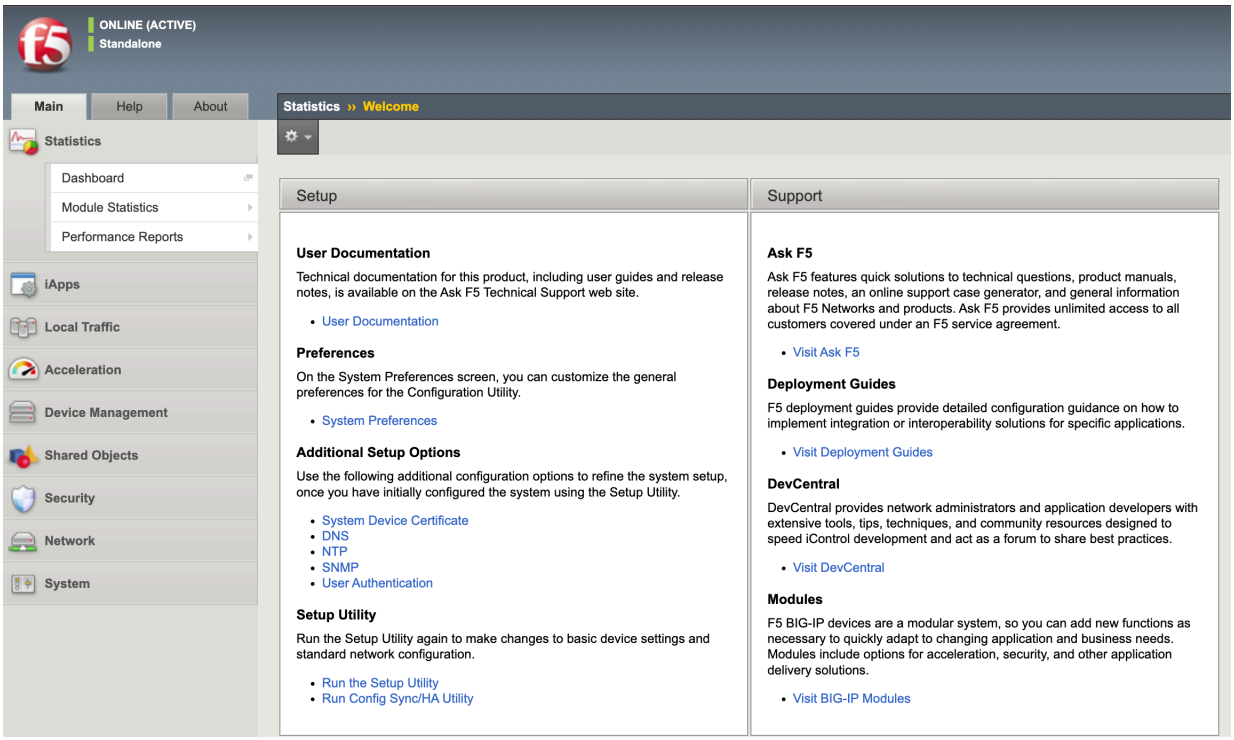


- UCS ファイルで設定を戻すので、ウィザードで設定する必要はありません。よって、このウィザードをコマンドラインで停止します。

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

- もう一度 BIG-IP へ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。)
- 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。

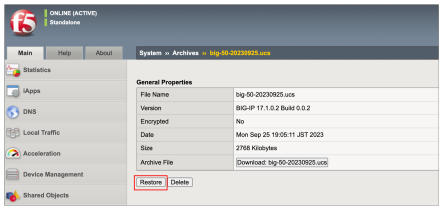
```
[root@localhost:Active:Standalone] config # tail -f /var/log/ltm | grep ucs
```



- 「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。

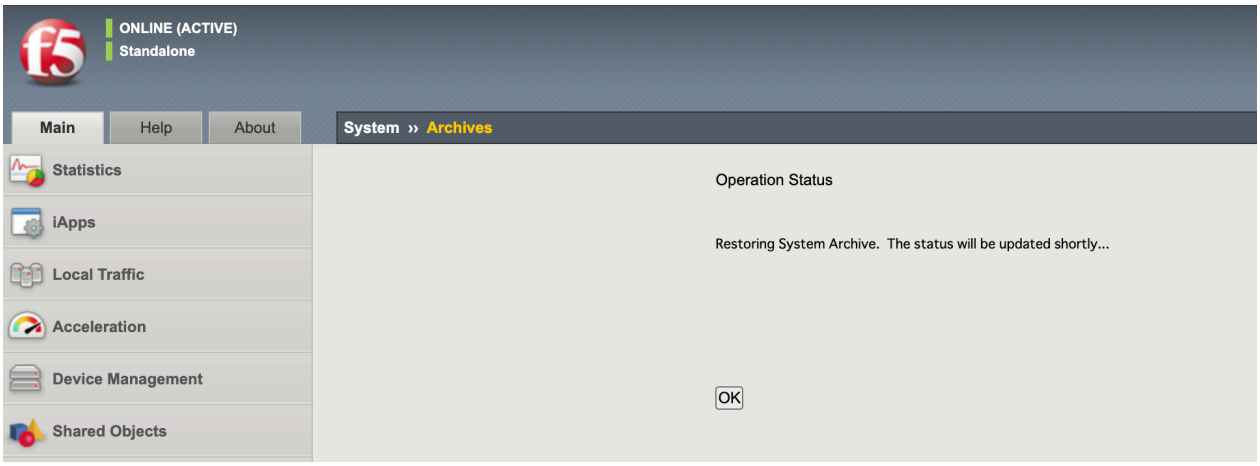
- アップロードした UCS ファイルをクリックします。

- 「Restore」ボタンを押します。

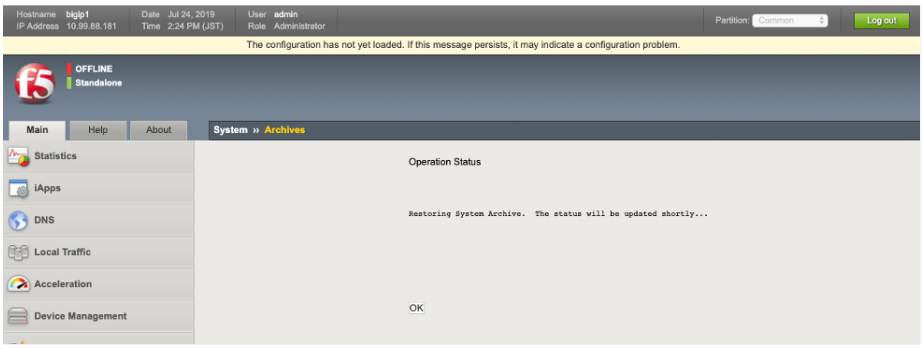


- 以下の状態のときは、「OK」ボタンを押さず、しばらく待ちます。

「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。



注釈: 一時的に以下のようなメッセージが表示されることがありますが、その場合はそのままお待ちください。



- 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。

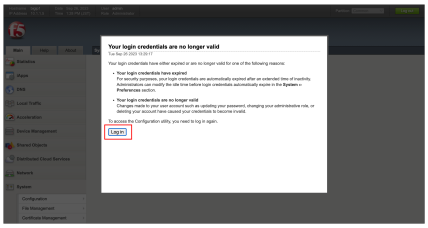
```
[root@localhost:Active:Standalone] config # tail -f /var/log/ltm | grep ucs
Feb  3 22:46:38 localhost.localdomain info tmsh[24320]: Begin config install␣
↪operation: /var/local/ucs/big-50-20220131.ucs
Feb  3 22:46:43 localhost.localdomain notice logger[22221]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪stop named
Feb  3 22:46:43 localhost.localdomain notice logger[22235]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪stop zrd
Feb  4 15:46:47 localhost.localdomain info install_ucs.pm[22079]: Install the license␣
↪file from UCS onto the system.
Feb  4 15:46:49 localhost.localdomain notice logger[23193]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪stop restjavad restnoded
Feb  4 15:46:49 localhost.localdomain notice logger[23312]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪start named
```

(次のページに続く)

(前のページからの続き)

```
Feb  4 15:46:50 localhost.localdomain notice logger[23373]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪start zrd
Feb  4 15:46:53 localhost.localdomain notice logger[23584]: /usr/bin/perl /usr/local/
↪bin/im -exclfrom -q -force /var/local/ucs/big-50-20220131.ucs  ==> /bin/bigstart␣
↪start restjavad restnoded
Feb  4 15:47:35 big50.f5jp.local info install_ucs.pm[22079]: UCS installation success.
```

- 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。

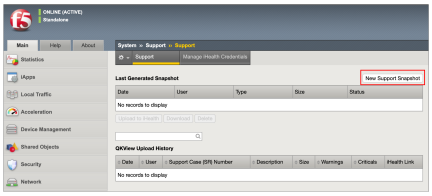


- 設定済みの ID とパスワードでログインし、Virtual Server 等の設定が復元されていることを確認します。

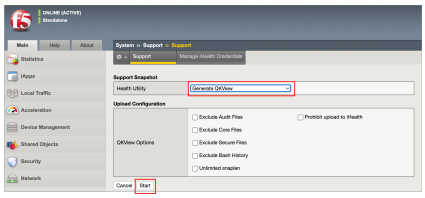
10 QKview の取得

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。

- 「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。



- 「Health Utility」で「Generate QKView」を選択します。

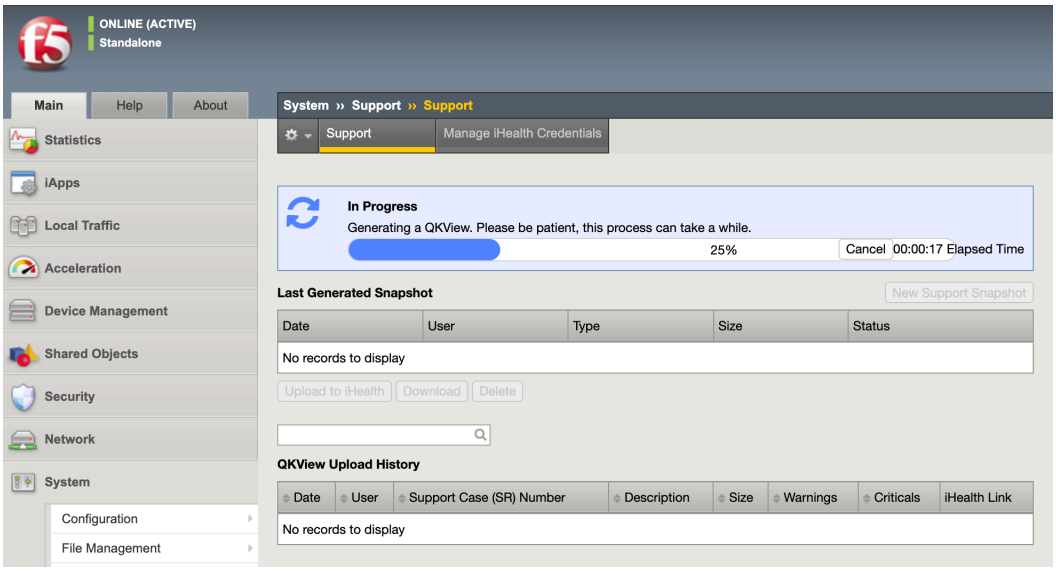


上記で、「Generate and Upload QKView to iHealth」を選択すると、iHealth サイトに QKView を直接アップロード可能となります。

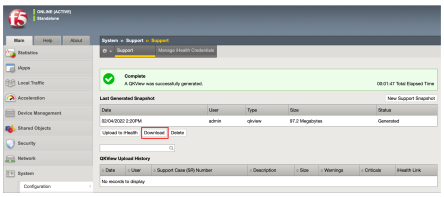
iHealth は BIG-IP の設定データや過去 1 ヶ月分のログデータを閲覧できる大変便利なツールです (予め簡単なユーザ登録が必要です)。iHealth の詳細に関しては、以下の Article に情報が掲載されております。

K12878: Generating diagnostic data using the qkview utility
https://my.f5.com/manage/s/article/K12878

- 「Start」ボタンを押すと、QKView の作成が開始されます。



- 完了すると、以下のような画面が表示されます。「Download」ボタンを押すと、QKview ファイルをダウンロードできます。

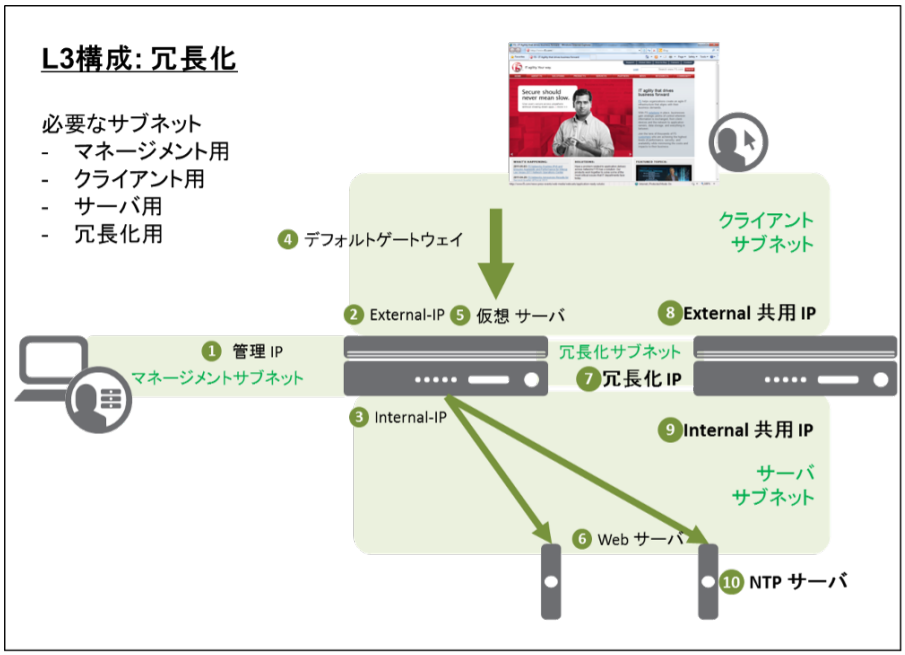


11

L3 構成: 冗長化

11.1 L3 構成: 冗長化イメージ

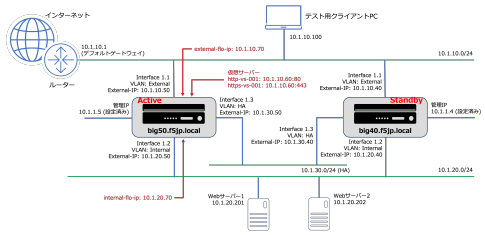
構成イメージは、以下の通りです。



スタンドアローン構成に加え、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 に動作する共用 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。

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。



[Active 機 (big50.f5jp.local) 設定項目]

項目	名称	設定値
ホスト名		big50.f5jp.local
管理インタフェース		10.1.1.5
External インタフェース	external	10.1.10.50
Internal インタフェース	internal	10.1.20.50
デフォルトゲートウェイ	Default-GW	10.1.10.1
仮想サーバ (HTTP)	http-vs-001	10.1.10.60:80
仮想サーバ (HTTPS)	https-vs-001	10.1.10.60:443
Pool Member (Web サーバ 1)		10.1.20.201:80
Pool Member (Web サーバ 2)		10.1.20.202:80
HA 用インタフェース	HA	10.1.30.50
External 共用 (floating)IP アドレス	external-flo-ip	10.1.10.70
Internal 共用 (floating)IP アドレス	internal-flo-ip	10.1.20.70
NTP サーバ		10.1.20.202

[Standby 機 (big40.f5jp.local) 設定項目]

項目	名称	設定値
ホスト名		big40.f5jp.local
管理インタフェース		10.1.1.4
External インタフェース	external	10.1.10.40
Internal インタフェース	internal	10.1.20.40
デフォルトゲートウェイ	Default-GW	10.1.10.1
仮想サーバ (HTTP)		(設定同期によりコピー)
仮想サーバ (HTTPS)		(設定同期によりコピー)
Pool Member (Web サーバ 1)		(設定同期によりコピー)
Pool Member (Web サーバ 2)		(設定同期によりコピー)
HA 用インタフェース	HA	10.1.30.40
External 共用 (floating)IP アドレス		(設定同期によりコピー)
Internal 共用 (floating)IP アドレス		(設定同期によりコピー)
NTP サーバ		10.1.20.202

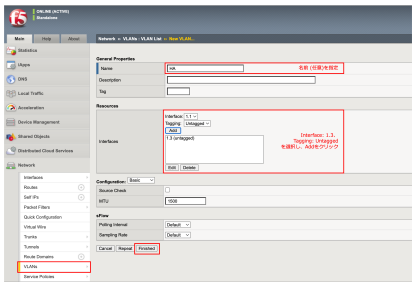
このサンプルでは、NTP サーバを 10.1.20.202 とし、BIG-IP はこのサーバとの時刻同期を行うことします。(冗長化を行う BIG-IP 同士は、時刻を合わせておく必要があります。)

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 (big50.f5jp.local) の設定

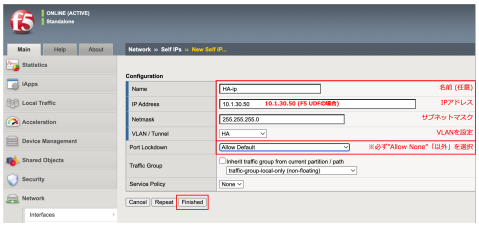
11.3.1 HA VLAN の設定

- 「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。



11.3.2 HA VLAN の IP 設定

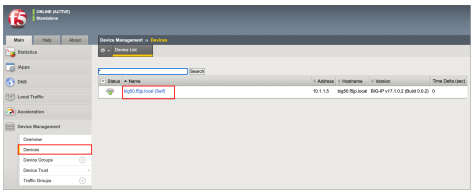
- 「Network」→「Self IPs」で表示された画面の右上にある「Create」ボタンを押し、HA 用 VLAN の IP を設定します。



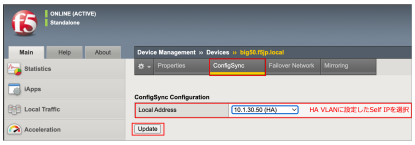
注釈: Allow None を選ぶと HA の通信も止めてしまい、HA が組めません。(ここでは **Allow Default** を選びます)

11.3.3 Device の設定

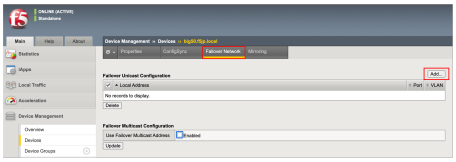
- 次に「Device Management」→「Devices」で、自分自身 (=big50.f5jp.local (Self)) を選択します。



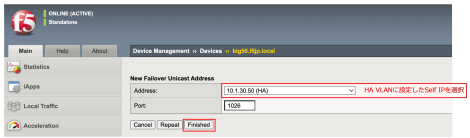
- 「ConfigSync」タブを選択し、HA VLAN に指定した IP アドレスを選択し「Update」を押します。



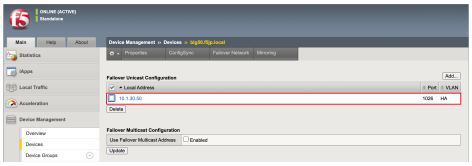
- 「Failover Network」タブを選択し、「Add」ボタンを押します。



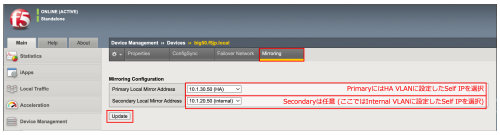
- HA VLAN に設定した IP アドレスを選択します。



- 以下のような状態になります。

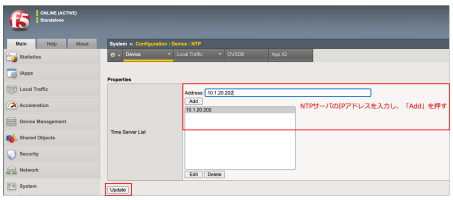


- 「Mirroring」タブを選択し、HA VLAN に指定した IP アドレスをプライマリに指定します。任意ですが、ここでは Secondary として、Internal VLAN に指定した IP アドレスを選択しています。選択後、「Update」を押します。



11.3.4 時刻同期 (NTP) 設定

- 「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。BIG-IP への SSH アクセスの方法については、**管理ポートへの *SSH* アクセス** をご参照ください。

- 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。)

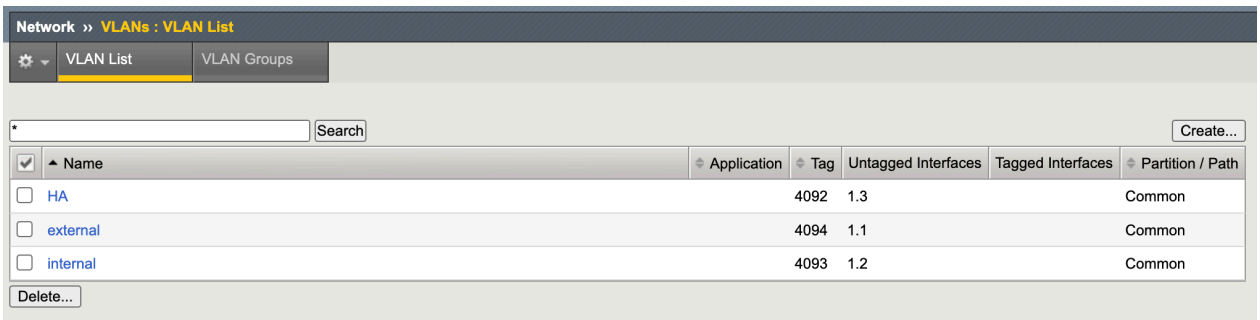
```
[root@big50:Active:Standalone] config # ntpq -np
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.1.20.202     133.243.238.243  2 u   24   64    1    0.594   -0.321   0.299
```

11.4 Standby 機 (big40.f5jp.local) の設定

初期設定 および **ネットワーク設定** を参照して、Standby 機も Active 機と同様の初期設定、ネットワーク設定を行います。

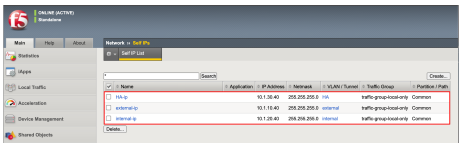
11.4.1 VLAN 設定

- Standby 機 (big40.f5jp.local) に設定された VLAN は以下のようになります。(Active 機と同様です。)



11.4.2 Self-IP 設定

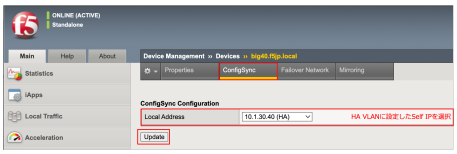
- Standby 機 (big40.f5jp.local) に設定された Self IP アドレスは以下のようになります。



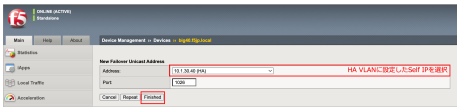
11.4.3 Device 設定

「Device Management」→「Devices」で、自分自身 (=big40.f5jp.local (self)) を選択し、Active 機同様に、Device Connectivity の設定を行います。

- ConfigSync 設定



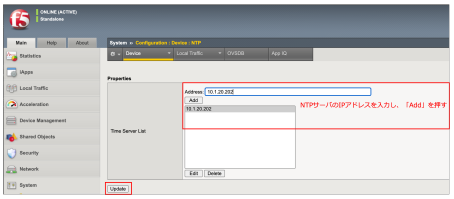
- Failover Network 設定



- Mirroring 設定

11.4.4 NTP 設定

NTP の設定も Active 機同様に行います。

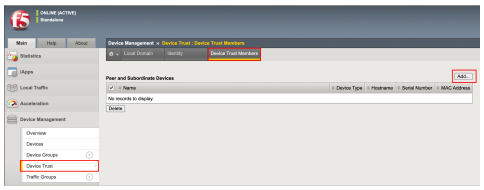


11.5 デバイストラスト設定 ※ Active 機 (big50.f5jp.local) 側から実施

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。

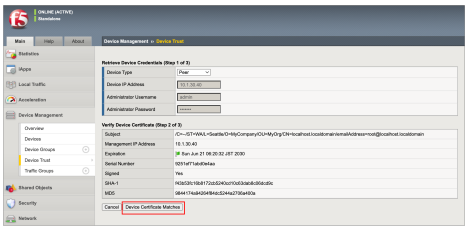
注釈: 以降は、Active 機 (big50.f5jp.local) からのみ、設定します。

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

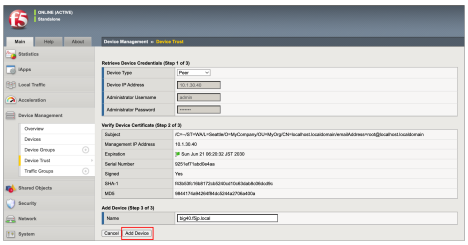


- ” Peer “ を選択し、Standby 機 (big40.f5jp.local) の IP アドレスと管理者 ID(Admin) とパスワードを指定します。「Retrieve Device Information」ボタンを押します。

- Standby 機 (big40.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。

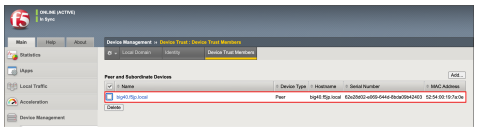


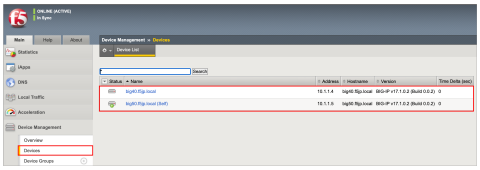
- Standby 機の Hostname を確認し、「Add Device」を押します。



- 承認されたデバイスとして登録された状態です。

- 「Device Management」→「Devices」で見ると、bigip50.f5jp.local (self) に加え、Standby 機 (big40.f5jp.local) も表示されます。 (ここは確認のみです。)





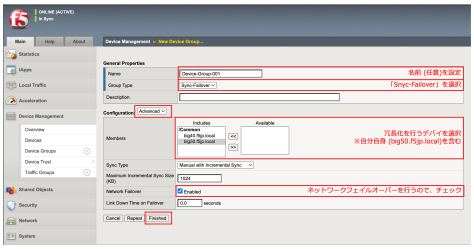
11.6 デバイスグループの設定

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 号機と 2 号機で冗長化を行い、2 号機と 3 号機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。

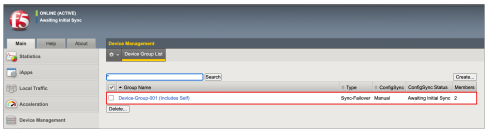
2 台で冗長化を行う場合はデバイスグループの組み方をあまり意識する必要はありませんが、設定は必要です。

注釈: 以降は、Active 機 (big50.f5jp.local) からのみ、設定します。

- 「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。



- デバイスグループが作られた状態です。



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。

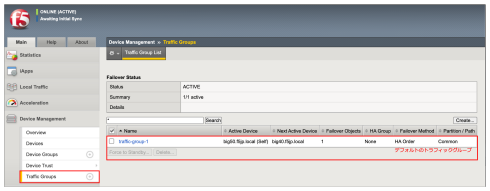
11.7 トラフィックグループの設定

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 と共用 IP (Floating IP) がトラフィックグループのオブジェクトです。

注釈: 以降は、Active 機 (big50.f5jp.local) からのみ、設定します。

11.7.1 トラフィックグループの確認

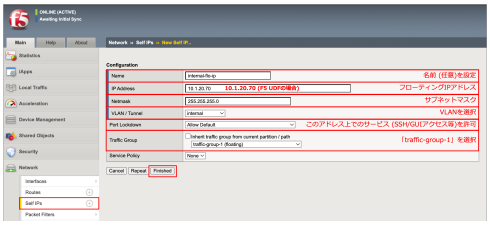
- 「Device Management」→「Traffic Groups」を確認します。
- デフォルトで、「Traffic-group-1」という名前のトラフィックグループが存在しています。以降、この Traffic-group-1 に対して、Floating IP および Virtual Server を割当てていきます。 (ここでは確認のみです。)



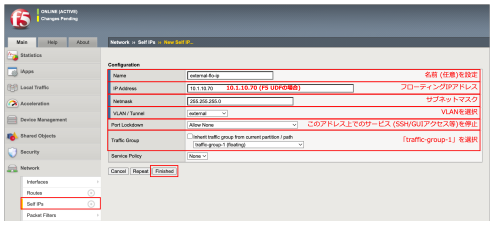
11.7.2 Floating IP の設定

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。

- 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。



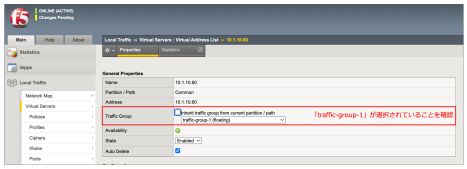
- External VLAN 側の共用 IP(Floating IP) も追加設定します。



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

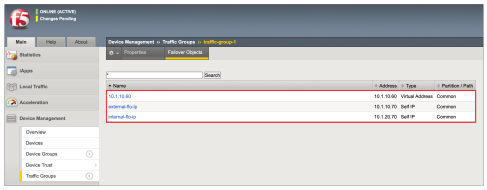
- 「Local Traffic」→「Virtual Servers」→「Virtual Address List」を選択します。

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。



11.7.4 Traffic Group に紐付けられたオブジェクトの確認

- 「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。



11.8 ConfigSync

Active 機 (big50.f5jp.local) のみに行った設定を、Standby 機 (big40.f5jp.local) に同期するために、ConfigSync を行います。

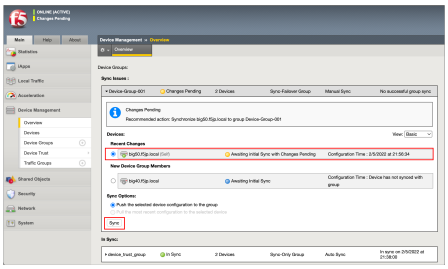
注釈: 以降は、Active 機 (big50.f5jp.local) からのみ、設定します。

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

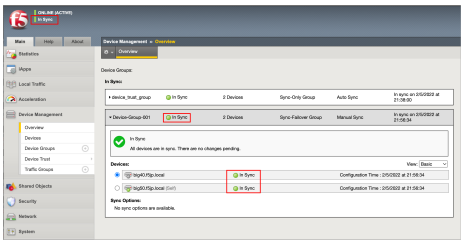
No	Device Group	**説明**
?	device_trust_group	trust group に peer を設定すると、システムによって自動的に作成されます。peer の基本情報を Sync します。
?	Device-Group-001 (任意の名前)	前項で作成したユーザ設定領域のデータを Sync します。

?は自動で Sync されますが、?はデフォルトでマニュアル Sync の設定となっています。?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。

- 「Device Management」→「Overview」を選択します。Active 機 (big50.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。



- しばらく待つと、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。

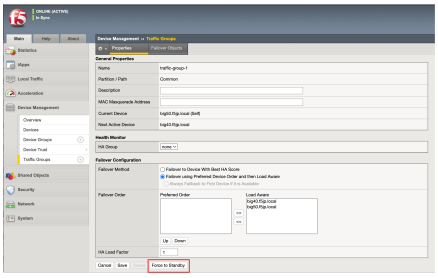


11.9 Traffic-group-1 の Active/Standby の切替え

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

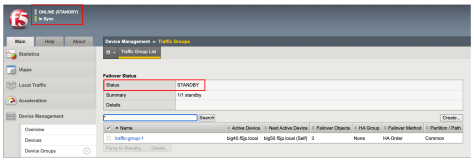
デフォルトでは、管理 IP アドレス設定の大きい値を持つものが Traffic-group-1 の Active 機になりますが、マニュアルで強制的に Active と Standby を切替えます。

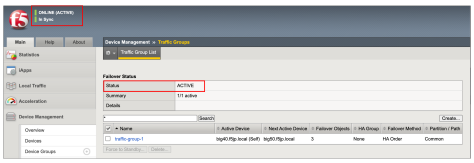
- アクティブ機の「Device Management」→「Traffic Groups」から Traffic-group-1 を選択し、「Force to Standby」ボタンを押します。



- 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。
- その結果、Active から Standby に変わります。

Standby だった BIG-IP は Active になります (※ big40.f5jp.local で確認)。





11.9.2 クライアントからの接続確認

クライアントからの *HTTP* アクセス 参照。

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)

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

- GUI で実行されるウィザードの停止

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

- ホスト名の設定

```
(tmos)# modify sys global-settings hostname big50.f5jp.local
```

- 設定の確認

```
(tmos)# list sys global-settings
sys global-settings {
     gui-setup disabled
     hostname big50.f5jp.local
     mgmt-dhcp disabled
}
```

- 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
}
```

- 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

- 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
}
```

- Self-IP の設定と確認

```
(tmos)# create net self external-ip address 10.1.10.50/24 vlan external
(tmos)# create net self internal-ip address 10.1.20.50/24 vlan internal allow-service␣
↪default

(tmos)# list net self
net self internal-ip {
```

(次のページに続く)

(前のページからの続き)

```
     address 10.1.20.50/24
     allow-service {
          default
     }
     traffic-group traffic-group-local-only
     vlan internal
}
net self external-ip {
     address 10.1.10.50/24
     traffic-group traffic-group-local-only
     vlan external
}
```

- ルーティングの設定と確認

```
(tmos)# create net route default-GW gw 10.1.10.1 network default

(tmos)# list net route
net route default-GW {
    gw 10.1.10.1
    network default
}
```

12.4 Pool と Virtual Server の設定

12.4.1 HTTP (80) 用 Pool と VS

- Pool 設定と確認

```
(tmos)# create ltm pool http-pool-01 { members add { 10.1.20.201:http { } 10.1.20.
↪202:http { } } monitor http }
(tmos)# list ltm pool
ltm pool http-pool-01 {
    members {
        10.1.20.201:http {
            address 10.1.20.201
            session monitor-enabled
            state up
        }
        10.1.20.202:http {
            address 10.1.20.202
            session monitor-enabled
            state up
        }
```

(次のページに続く)

(前のページからの続き)

```
    }
    monitor http
}
```

- VS 設定

```
(tmos)# create ltm virtual http-vs-001 { destination 10.1.10.60: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 10.1.10.60: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
}
```

- 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 10.1.10.60: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 { }
```

(次のページに続く)

(前のページからの続き)

```
        tcp { }
    }
    source 0.0.0.0/0
    source-address-translation {
        type automap
    }
    translate-address enabled
    translate-port enabled
    vs-index 23
}
```

12.4.2 HTTP (80) 用 Pool と 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。

- Pool 設定

```
(tmos)# create ltm pool ssh-pool-001 { members add { 10.1.20.201:ssh { } 10.1.20.
↪202:ssh { } } monitor tcp }
(tmos)# list ltm pool ssh-pool-001
ltm pool ssh-pool-001 {
    members {
        10.1.20.201:ssh {
            address 10.1.20.201
            session monitor-enabled
            state up
        }
        10.1.20.202:ssh {
        address 10.1.20.202
            session monitor-enabled
            state up
        }
    }
    monitor tcp
}
```

- VS 設定

```
(tmos)# create ltm virtual ssh-vs-001 { destination 10.1.20.60: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 10.1.20.60:ssh
    ip-protocol tcp
```

(次のページに続く)

(前のページからの続き)

```
    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 Active 機 (big50) での設定

- 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 10.1.30.50/24 vlan HA allow-service default
```

- 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 big50.f5jp.local
```

- Device Mangement 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 big50.f5jp.local { configsync-ip 10.1.30.50 mirror-ip 10.1.30.
↪50 mirror-secondary-ip 10.1.20.50 unicast-address {{ ip 10.1.30.50 }} }
```

- 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
```

- NTP 同期の設定をします。

```
(tmos)# modify sys ntp servers add { 10.1.20.202 }
```

- 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
==============================================================================
*10.1.20.202     133.243.238.164  2 u   39  256  377    0.537    4.167   2.251
```

- 再び、TMSH へ戻ります。

```
config # tmsh
(tmos)#
```

- コンフィグ保存

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

12.6.2 Standby 機 (big40) での設定

Standby 機で、冗長化に必要な設定を実施します。

- 初期設定

```
(tmos)# modify sys global-settings gui-setup disabled
(tmos)# modify sys global-settings hostname big40.f5jp.local
(tmos)# modify sys ntp timezone Japan
```

- 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 }
```

- Self-IP 設定

```
(tmos)# create net self external-ip address 10.1.10.40/24 vlan external
(tmos)# create net self internal-ip address 10.1.20.40/24 vlan internal allow-service␣
↪default
(tmos)# create net self HA-ip address 10.1.30.40/24 vlan HA allow-service default
```

- 冗長化用の設定

```
(tmos)# mv cm device bigip1 big40.f5jp.local
(tmos)# modify cm device big40.f5jp.local { configsync-ip 10.1.30.40 mirror-ip 10.1.30.
↪40 mirror-secondary-ip 10.1.20.40 unicast-address { { ip 10.1.30.40 }}}
(tmos)# delete cm trust-domain all
```

- NTP 設定

```
(tmos)# modify sys ntp servers add { 10.1.20.202 }
```

- admin のパスワード変更

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

- コンフィグ保存

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

12.6.3 Active 機 (big50) での設定 (再度)

- Device-Trust の実施

```
(tmos)# modify cm trust-domain Root add-device { device-ip 10.1.30.40 device-name␣
↪big40.f5jp.local username admin password ilovef5 ca-device true }
```

- Device-Group の設定

```
(tmos)# create cm device-group Device-Group-001 { type sync-failover devices add {␣
↪big50.f5jp.local big40.f5jp.local }}
```

- Floating-IP の設定

```
(tmos)# create net self external-flo-ip address 10.1.10.70/24 traffic-group traffic-
↪group-1 vlan external
(tmos)# create net self internal-flo-ip address 10.1.20.70/24 traffic-group traffic-
↪group-1 vlan internal allow-service default
```

- コンフィグ保存

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

- Config-Sync の実行

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

12.6.4 Active 機 (big50) での実行

冗長化を構成した最初だけ、アドレスの大きいほうが Active になります。よって、本ガイドでは、1 号機 (big50) が Active となるので、Traffic-Group を 2 号機 (big40) へ切り替えてみます。

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

12.7 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。

- 現存する全コネクションの確認

```
(tmos)# show sys connection
10.1.30.40:12028  10.1.30.50:1026  10.1.30.40:18649  10.1.30.50:1026  udp  0  (tmm: 1)
 none  none
```

(次のページに続く)

(前のページからの続き)

```
10.1.20.50:123  10.1.20.202:123  10.1.20.50:123  10.1.20.202:123  udp  2  (tmm: 0) ␣
↪none  none
10.1.30.50:38234  10.1.30.40:1026  10.1.30.50:38234  10.1.30.40:1026  udp  0  (tmm: 0)
 none  none
Total records returned: 3
```

- 確認したいコネクションの絞込み

```
(tmos)# show sys connection cs-client-addr 10.1.10.100
Sys::Connections
10.1.10.100:49930  10.1.10.60:80  any6.any  any6.any  tcp  5  (tmm: 1)  none  none
10.1.10.100:49931  10.1.10.60:80  10.1.20.70:49931  10.1.20.202:80  tcp  5  (tmm: 0) ␣
↪none  none
Total records returned: 2
```

- 絞り込んだコネクションの詳細

```
(tmos)# show sys connection cs-client-addr 10.1.10.100 all-properties
Sys::Connections
10.1.10.100:49931 - 10.1.10.60:80 - 10.1.20.70:49931 - 10.1.20.202:80
------------------------------------------------------------------------
  TMM            0
  Type           any
  Acceleration   none
  Neuron Rules   none
  Protocol       tcp
  Idle Time      19
  Idle Timeout   300
  Unit ID        1
  Lasthop        /Common/external 52:54:00:65:ad:80
  Server Nexthop /Common/internal 52:54:00:d4:7d:9f
  Ingress Dest   none
  Virtual Path   10.1.10.60:80
  Conn Id 0

                      ClientSide         ServerSide
  Client Addr   10.1.10.100:49931   10.1.20.70:49931
  Server Addr       10.1.10.60:80     10.1.20.202:80
  Bits In                  5.0K              34.8K
  Bits Out                35.2K               5.0K
  Packets In                  6                  5
  Packets Out                 6                  6

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

MyF5: ナレッジベース総合サイト (英語)
https://my.f5.com/

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://community.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

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改変する場合がありま 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。