

BIG-IP APM

ネットワークアクセス

かんたんセットアップガイド (v11.4.1 対応)

初級編 & 中級編

F5 Networks Japan

V1.0



目次

1. はじめに	4
1.1. APM ネットワークアクセス動作概要	4
2. スタンドアローン	5
2.1. スタンドアローンイメージ	5
2.2. 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. 管理ポートの IP アドレス設定	7
3.2. 管理ポートへの GUI アクセス→ライセンスの取得	11
4. ネットワーク設定	19
4.1. VLAN の作成	19
4.2. Self IP の設定	20
4.3. ルーティングの設定	22
4.3.1. デフォルトゲートウェイの設定	22
4.3.2. オフィス内サーバへのルーティング設定	22
5. 初級編	23
5.1. ウィザードを使って設定する方法	23
5.2. クライアントからのアクセス	30
5.2.1. Windows の Web ブラウザからのアクセス	30
5.2.2. Windows 用 Edge Client ソフトウェアからのアクセス	31
5.2.3. Apple iPad からのアクセス	37
5.3. Local User DB による認証	41
5.3.1. クライアント PC からのアクセス	46
5.4. [参考]アンチウイルスソフトウェアのチェックについて	47
5.5. SSL サーバ証明書の設定	49
5.5.1. CSR の作成	49
5.5.2. サーバ証明書の取得手続き	50
5.5.3. 証明書のインポート	51
5.5.4. Client SSL Profile の生成と VS への割当て	52
5.5.4.1. クライアント PC からのアクセス	54
6. 中級編	55
6.1. APM オブジェクトを一つ一つ設定していく方法	55
6.1.1. 設定が必要な APM オブジェクトたち	55
6.1.2. 各オブジェクトの設定	56
6.1.2.1. DNS / NTP 設定	56
6.1.2.2. 認証サーバ: Active Directory の設定	57
6.1.2.3. Lease Pool の設定	58
6.1.2.4. Network Access の設定	59
6.1.2.5. Webtop の設定	61
6.1.2.6. Connectivity Profile の設定	62
6.1.2.7. Access Profile と Access Policy の設定	63
6.1.2.8. APM 用 Virtual Server の設定	69
6.1.2.9. リダイレクト用 Virtual Server の設定	70
6.1.2.10. クライアント PC からのアクセス	71
6.1.3. SSL サーバ証明書の設定	71
6.2. クライアント証明書認証の設定	72
6.2.1. クライアント証明書の発行	72
6.2.2. クライアント PC へクライアント証明書をインポート	72
6.2.3. BIG-IP の設定	75
6.2.3.1. 認証局の証明書のインポート	75
6.2.4. クライアントからのアクセス	77
6.3. セッション変数について	78
6.4. [VPE サンプル-1] クライアント証明書の OU で ACL を割当てる	80
6.4.1. ACL の作成	80
6.4.2. VPE の設定	82
6.4.3. クライアントからのアクセス	86

6.5.	[VPE サンプル-2] Active Directory の Group で ACL を割当てて	87
6.5.1.	ACL の作成	87
6.5.2.	Active Directory ユーザ: test1001	87
6.5.3.	VPE の設定	88
6.5.4.	クライアントからのアクセス	93
6.5.5.	AD Query がうまく行かない場合: AAA 設定の変更	94
6.6.	[VPE サンプル-3] アクセスできるクライアント端末を限定する	95
6.6.1.	クライアント端末固有の情報の取得	95
6.6.2.	Active Directory の設定	98
6.6.3.	クライアントからのアクセス	100
6.7.	[VPE サンプル-4] クライアント OS の種類に応じてポリシーを変える	102
6.8.	[VPE サンプル-5] マクロを使う	104
6.8.1.	AD 認証の誤り回数カウント	104
6.8.1.1.	クライアントからのアクセス	110
6.8.2.	同じ設定をまとめる	112
7.	冗長化	114
7.1.	冗長化イメージ	114
7.2.	冗長化のネットワークサンプル	115
7.3.	Active 機(big208.f5jp.local)の設定	116
7.4.	Standby 機(big209.f5jp.local)の設定	120
7.5.	デバイストラスト設定 (Active 機: big208.f5jp.local 側から実施)	123
7.6.	デバイスグループの設定	126
7.7.	トラフィックグループの設定	127
7.8.	ConfigSync	130
7.9.	Traffic-group-1 の優先度設定	131
7.10.	クライアント PC からのアクセス	133
8.	おわりに	134

1. はじめに

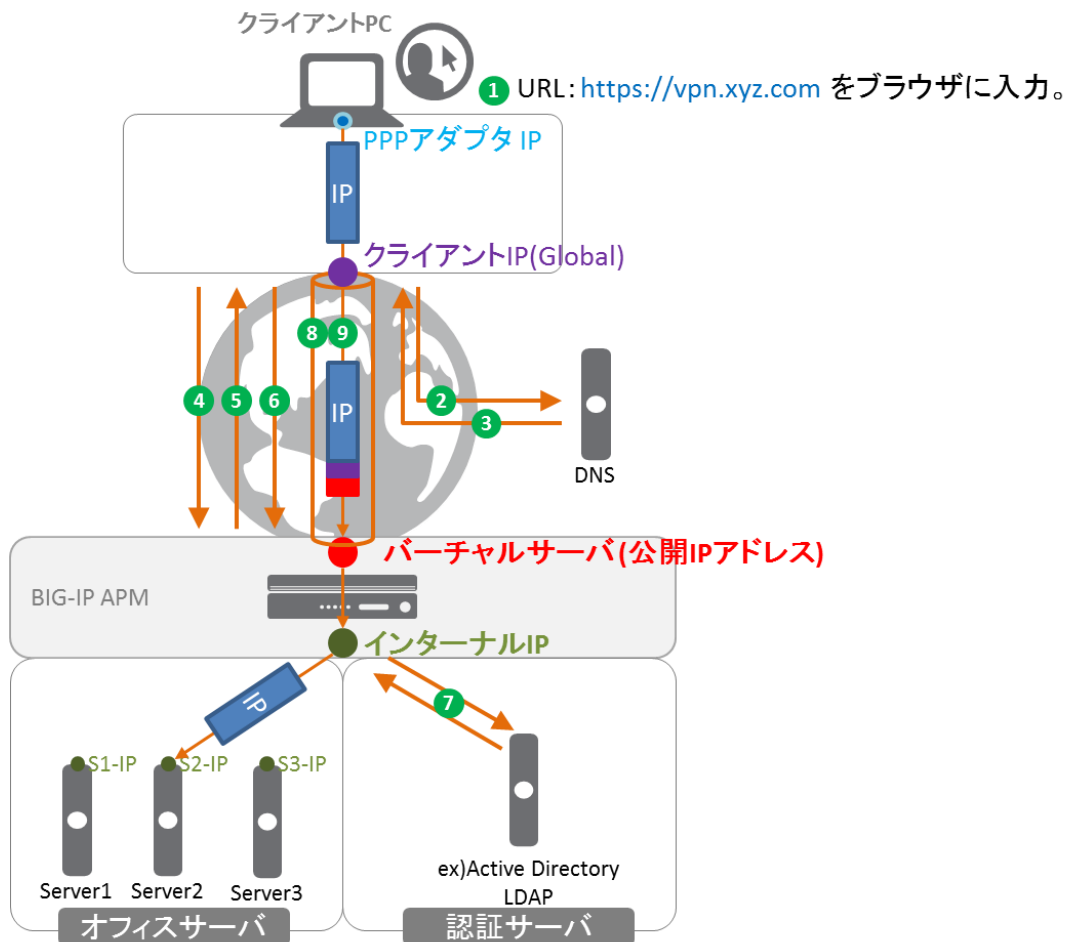
本セットアップガイドにて BIG-IP Access Policy Manager (以下、APM) のネットワークアクセスの設定方法についてご案内します。

BIG-IP APM は、SSL-VPN トンネルによるリモートアクセス(これをネットワークアクセスと呼びます)をはじめとして、高度な認証機能(例: クレデンシアルキャッシング方式シングルサインオン, SAML シングルサインオン等)も兼ね備えています。

本ガイドでは、BIG-IP APM をご購入いただいてすぐにネットワークアクセスを始められるように、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。

1.1. APM ネットワークアクセス動作概要

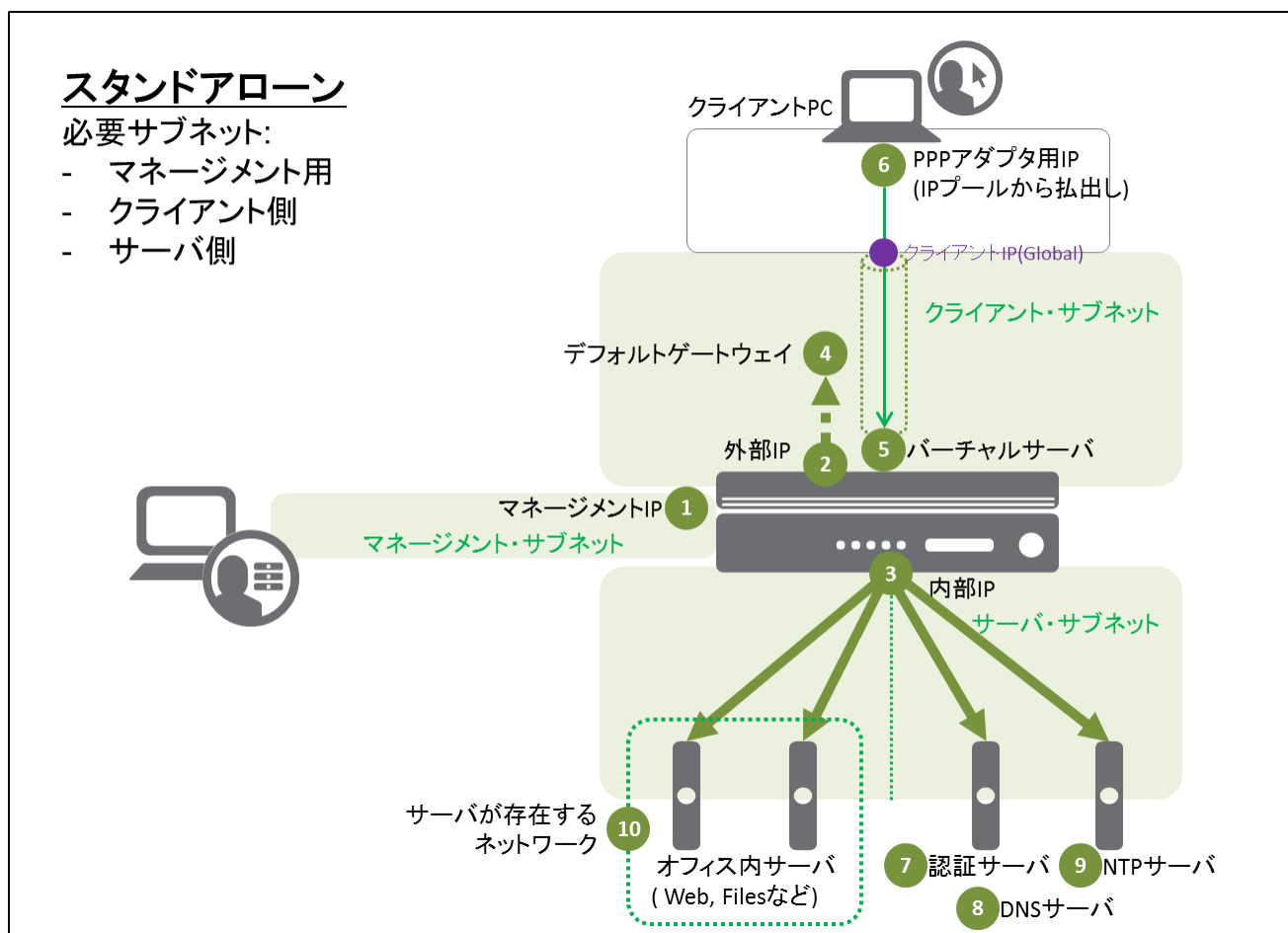
APM のネットワークアクセスは以下のような流れで動作します。



- ① クライアントが Web ブラウザに、URL: <https://vpn.xyz.com> を入力。
- ② クライアント PC は、vpn.xyz.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 vpn.xyz.com の IP アドレスを得る。
- ④ Web ブラウザは、その IP アドレス(バーチャルサーバ)宛に HTTPS リクエストを送信。
- ⑤ BIG-IP APM は、ログインページを表示。
- ⑥ クライアントは、ユーザ名とパスワードを入力。
- ⑦ BIG-IP APM は認証サーバに問合せを行い、認証が正しく行われたことのレスポンスを得る。
- ⑧ BIG-IP APM は、クライアント PC との間で SSL-VPN トンネルを確立する。このとき、クライアント PC の PPP アダプタには、事前に APM に設定された IP アドレスプールの中から一つ IP アドレスが払い出される。(この後、クライアント PC は、PPP アダプタを使って、オフィスサーバ群へアクセスができるようになる。)
- ⑨ PPP アダプタから出た IP パケットは、インターネット上のグローバル IP アドレスでカプセル化(=トンネル化)され、BIG-IP APM に到着。APM はそのカプセル化を解き、APM のルーティングテーブルに従って、そのカプセル化が解かれた IP パケットを送り出す。

2. スタンドアローン

2.1. スタンドアローンイメージ

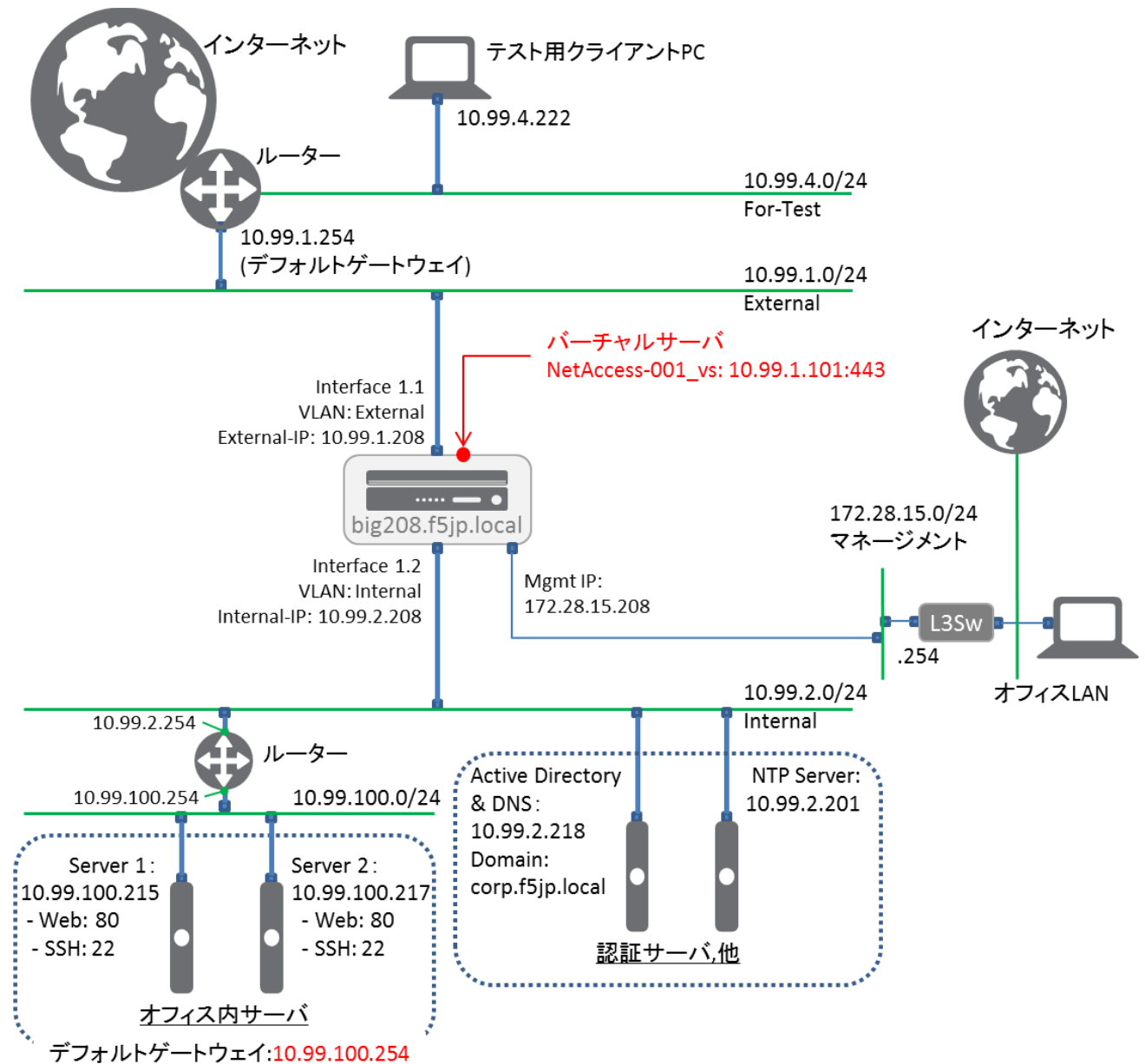


上図①～⑨の IP アドレスが必要になりますので、あらかじめご用意ください。
 なお、①管理 IP は工場出荷時に 192.168.1.245/24 がプリセットされています。

項目	名前(サンプル)	値
- ホスト名	Big208.f5jp.local	
① 管理 IP	---	172.28.15.208/24
② External インタフェース	external	10.99.1.208
③ Internal インタフェース	internal	10.99.2.208
④ デフォルトゲートウェイ	default-GW	10.99.1.254
⑤ バーチャルサーバアドレス	NetAccess-001_vs	10.99.1.101:443
⑥ PPP アダプタ用 IP アドレスプール	NetAccess-001_ip	10.99.99.11-20
⑦ 認証サーバ (Active Directory)	NetAccess-001_aaa_srvr	10.99.2.218
⑧ DNS サーバ (Active Directory)	---	10.99.2.218
⑨ NTP サーバ	---	10.99.2.201
⑩ サーバが存在するネットワーク	---	10.99.100.0/24
CLI パスワード (デフォルト)	---	ID/Password : root/default
GUI パスワード (デフォルト)	---	ID/Password : admin/admin

2.2. スタンドアローンのネットワークサンプル

まずは、冗長化しない状態を想定して、1 台のみ設定していきます。



BIG-IP の APM リモートアクセス用 Virtual Server は 10.99.1.101:443 とします。

Active Directory のドメインは、「corp.f5jp.local」とします。
Active Directory には、以下 3 つのユーザが登録されています。

ユーザ名	パスワード	グループ
test1001	test1001	CorpA-Group
test1002	test1002	CorpB-Group
test1003	test1003	CorpC-Group

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。

オフィス内サーバのデフォルトゲートウェイは、直上のルーター: 10.99.100.254 に設定されているものとします。

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」)から行うこととします。

3. 初期設定

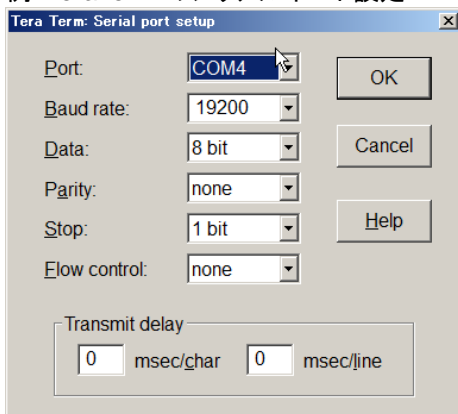
3.1. 管理ポートの IP アドレス設定

BIG-IP へ、専用コンソールケーブル(同梱)を使用し、Baud Rate 19,200 で接続します。

例: BIG-IP2000S



例: TeraTerm のシリアルポート設定



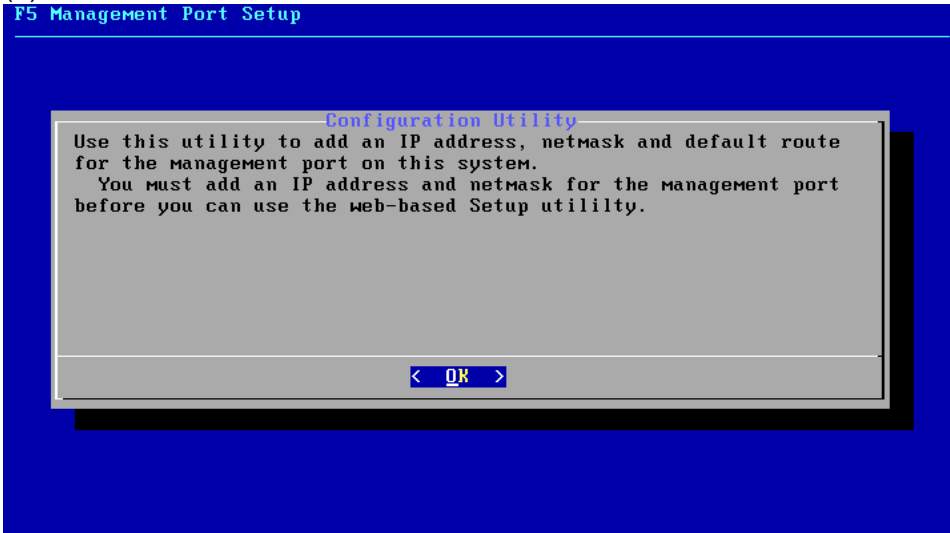
(1) デフォルトログインは、以下です。

ID: root
Password: default

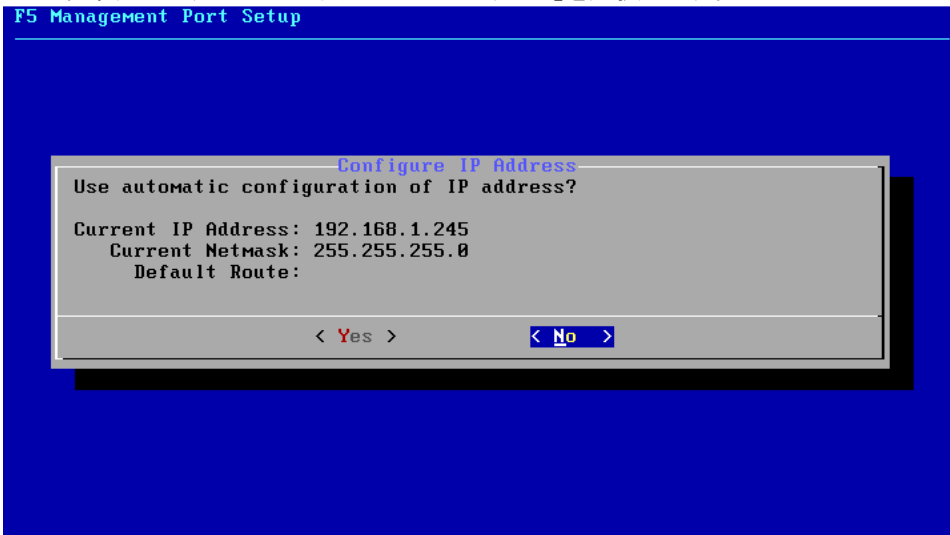
(2) 管理ポートの IP アドレスを設定するために、コマンド: config を入力し、Enter します。

```
BIG-IP 11.4.0 Build 142.0
Kernel 2.6.32-220.el6.f5.x86_64 on an x86_64
localhost login: root
Password:
Last login: Mon May 13 08:29:02 on tty1
[root@localhost:~]# config #
[root@localhost:~]# config # config_
```

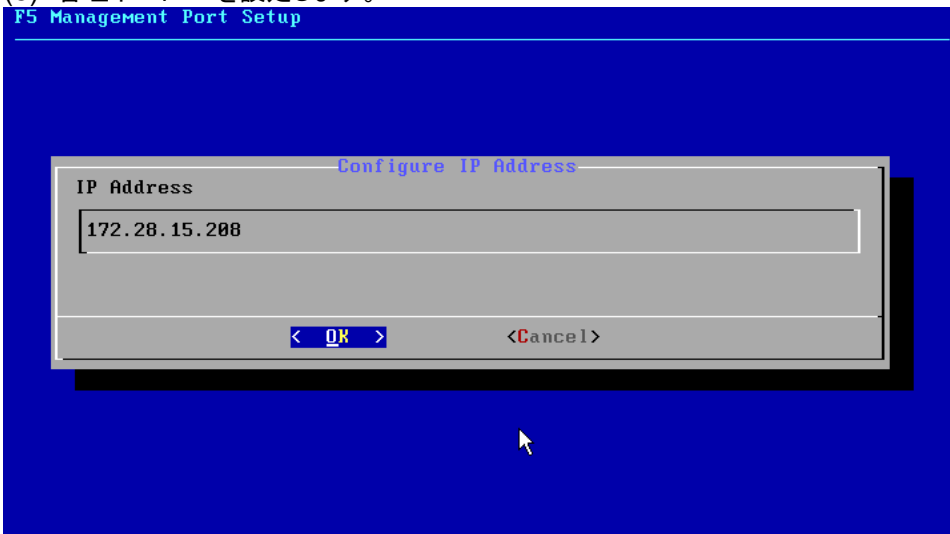
(3) OKします。



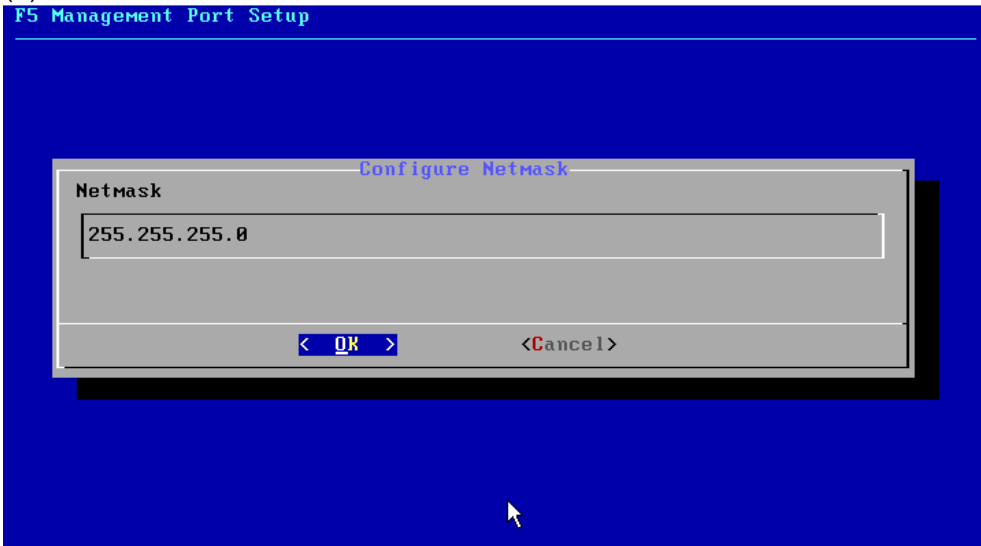
(4) DHCP を利用するかどうかを聞いてきますので、環境に合わせて設定します。本環境では、DHCP は利用しないので、「No」を選択します。



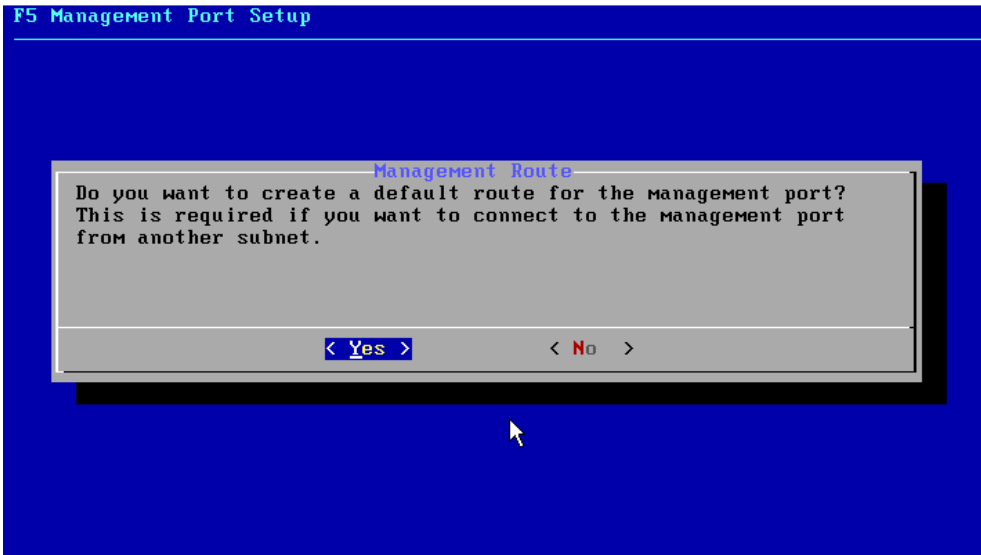
(5) 管理ポート IP を設定します。



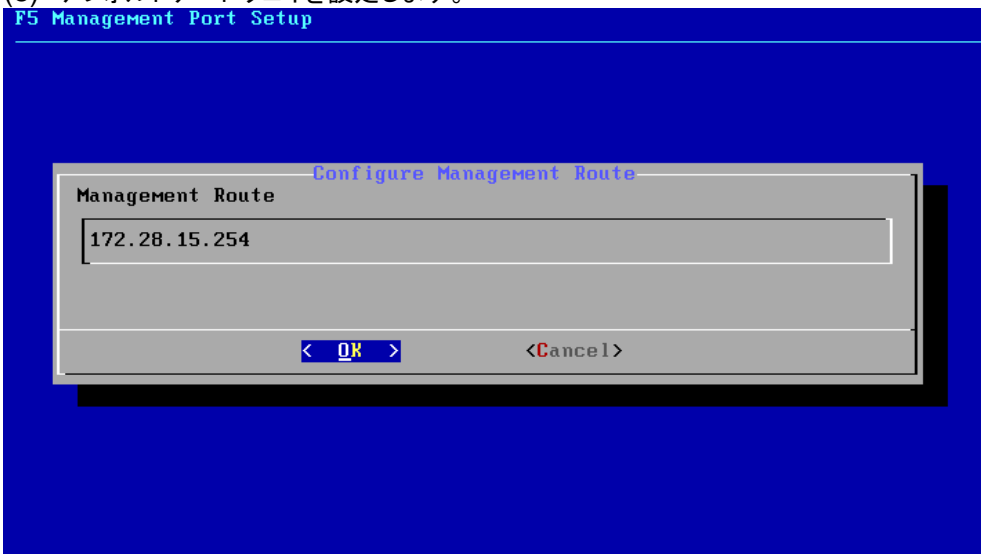
(6) サブネットマスクを設定します。



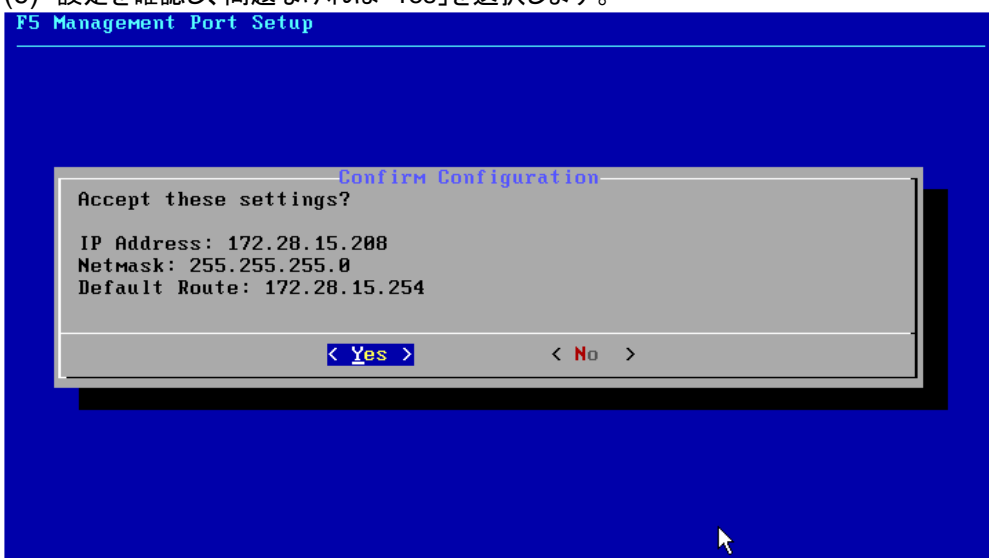
(7) デフォルトゲートウェイを設定するかどうかを聞いてきますので、環境に合わせて設定します。
本環境では必要なので、「Yes」を選択します。



(8) デフォルトゲートウェイを設定します。



(9) 設定を確認し、問題なければ「Yes」を選択します。



3.2. 管理ポートへの GUI アクセス→ライセンスの取得

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。

管理用 PC はライセンスアクティベーションの為、インターネットへ接続できる環境である必要があります。

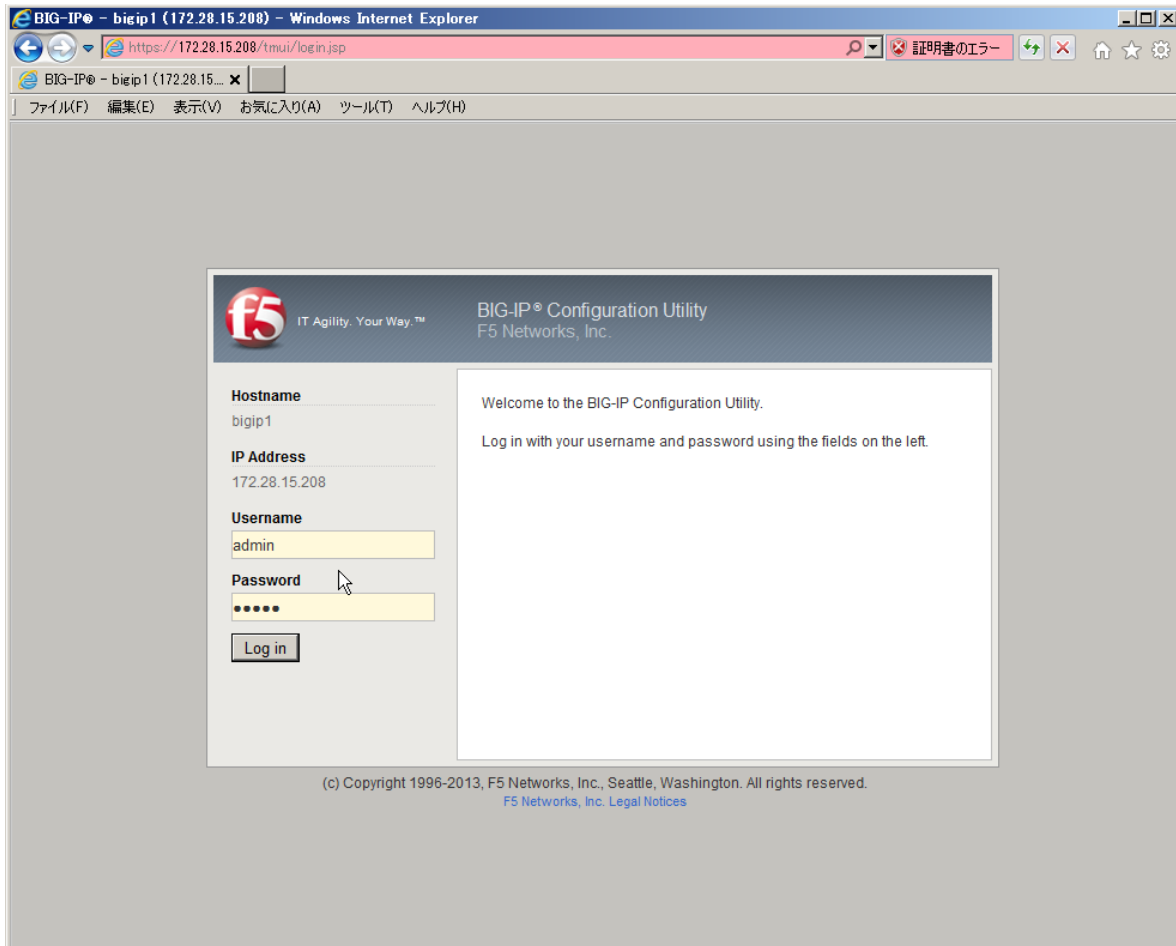
デフォルトの証明書は、正式に取得した証明書ではないため、以下のような画面が現れますが、「続行する」を選択してください。



(1) 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



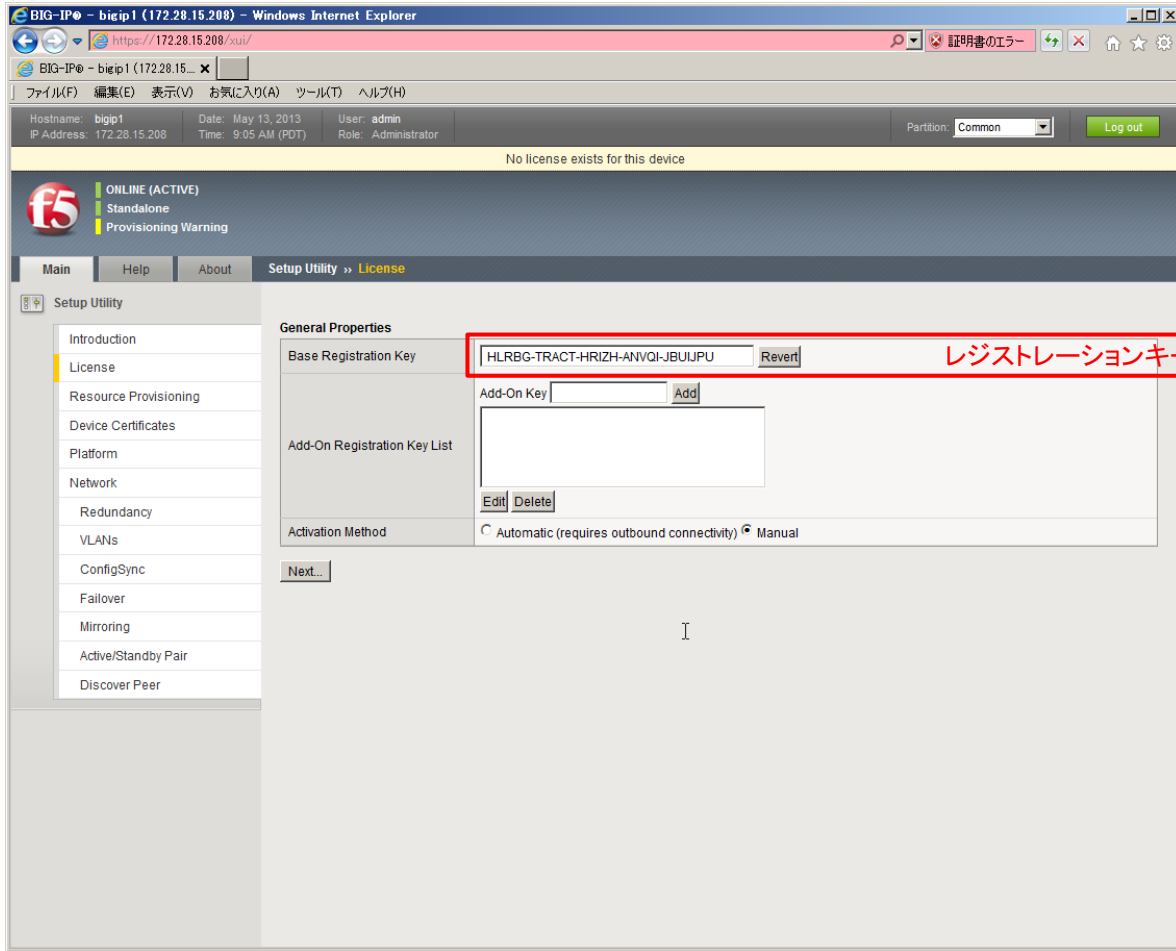
(2) 「Next」ボタンを押します。

The screenshot shows the BIG-IP Setup Utility web interface in Internet Explorer. The browser address bar shows `https://172.28.15.208/xui/`. The page header includes system information: Hostname: bigip1, IP Address: 172.28.15.208, Date: May 13, 2013, Time: 9:03 AM (PDT), User: admin, Role: Administrator, and Partition: Common. A yellow banner at the top states "No license exists for this device". Below this, the status is "ONLINE (ACTIVE)", "Standalone", and "Provisioning Warning". The navigation menu shows "Setup Utility >> Introduction" selected. The main content area has a "Welcome" box with the text: "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 welcome box.

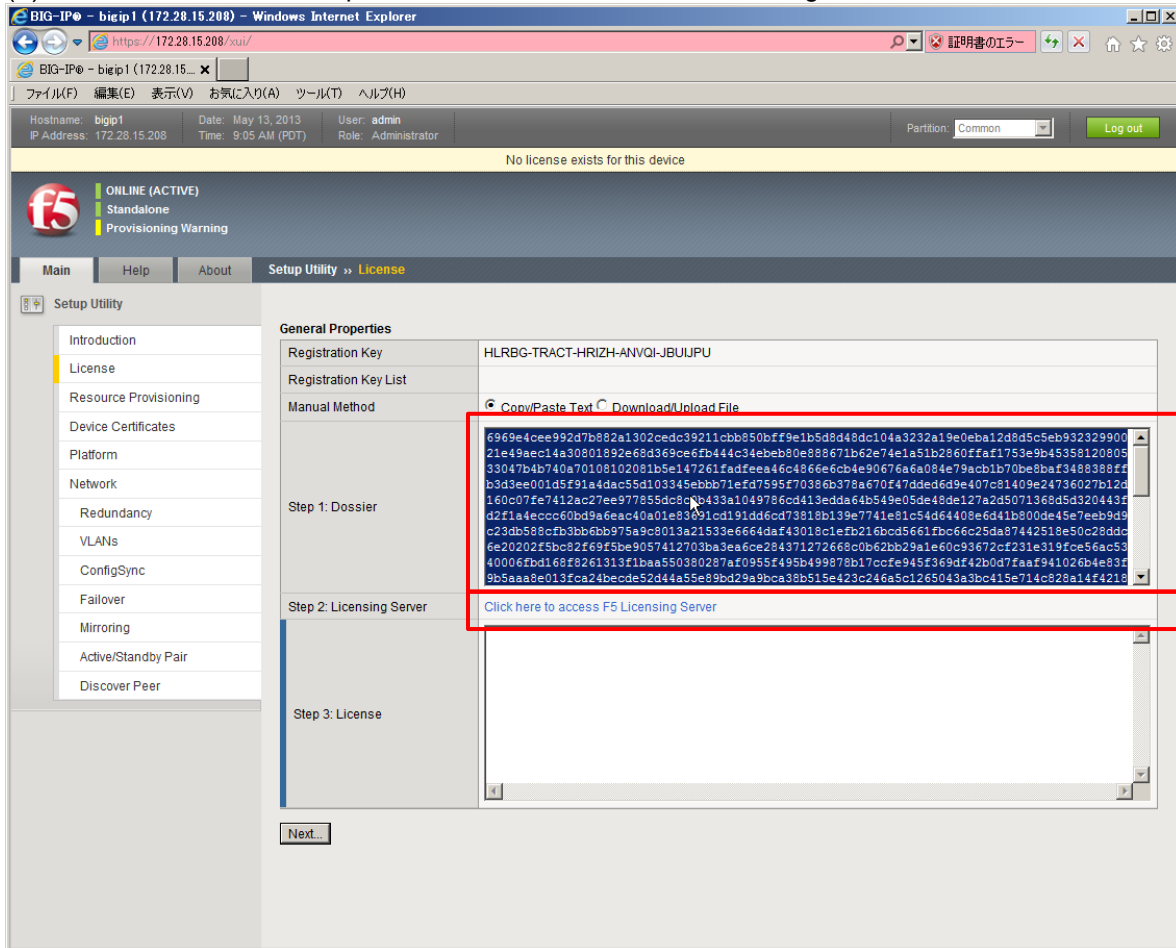
(3) ライセンスがないことを表示しています。「Activate」ボタンを押します。

The screenshot shows the BIG-IP Setup Utility web interface with the "License" section selected in the navigation menu. The "General Properties" section displays "License" as "Not Activated". An "Activate..." button is located below the license status. The system information and "No license exists for this device" banner are consistent with the previous screenshot.

(4) 購入したライセンスのレジストレーションキーを入力し、「Next」ボタンを押します。



(5) 「Dossier」をコピーし、Step2 の「Click here to access F5 Licensing Server」をクリックします。



(6) ライセンス取得するための Web サイト: activate.f5.com へ飛びますので、「Enter your dossier」フィールドの中に、上記でコピーした Dossier を貼り付けます。「Next」ボタンを押します。

The screenshot shows the 'Activate F5 Product' page on the F5 website. The page title is 'Activate F5 Product'. Below the title, it states: 'This page may be used to license the following products:' followed by a list of products including ARX 5.3.0 and higher, BIG-IP 9.x and higher, BIG-IQ, Enterprise Manager, FirePass 5.x - 6.x, Management Pack, TrafficShield, WANJet 4.x, and WebAccelerator. Below this list, it says: 'If you are attempting to activate a license for BIG-IP V4.x or iSMAN, please click [here](#). To activate your product you will need your product dossier.' A red box highlights the 'Enter your dossier' text input field, which contains a long alphanumeric string. A red arrow points to the 'Next' button. The page also includes a sidebar with various product categories and a main content area with a navigation menu and a search bar.

Enter your dossier

8accdddfbf6991a5b0327973aa3d4d2e264e86d73e3f910117122b2865efe888b
e0436c2eef06617f3906781c46d39613366369d2cd976ae264ff888508c6f1bce5
a1746bd10135a824c5315f72c5e5515770a155b699a5fc69c9137b4158c7abc33f
be3b8f765516e764bbd5d00ce1cce0177d2da2dc1ca9bb7c926fd16f6f914ce6c
cbbb2283b705187629399560cce818773b2c7dc6d596899bc3621eae5abe796a
6f4d175a636d4aa2b881008ef05ba7f5b3c349a88e5be52f79c19f076e5efc9f2ccc
2a13157f34492694f9f1c81875a879a7f5f290a796c31ac734b0d63bd666a41723d
2c18772652301cac59010f4bd9bf420e6a1a69d47a34e493680309b011c281
0d91670c8cc494b64ed485f40c7a3641cbea69440eae6a23b5174575c9d1114
ad3131543a8d0da2ff6d64acd291a9413df3be6197983f6df839e

or

Select your dossier file

If you are not activating a license for the versions mentioned above, please go to license.f5.com for more options.

<https://activate.f5.com/license/license.do;jsessionid=6336ADF8790D5AB83F97C...>

(7) チェックボックスをチェックして「Next」ボタンを押します。

Home / Product Licensing / Activate F5 Product / Accept EULA

Activate F5 Product

Step 2: Accept User Legal Agreement

Please agree to the terms of use

I have read and agree to the terms of this license

Next >

チェックして「Next」

PRODUCT LICENSE STATUS

- License Information
- TRAFFIC MANAGEMENT PRODUCTS
 - Activate License for BIG-IP v9.0 and higher
 - Activate License for BIG-IP v4.5 or v4.6
 - Upgrade License to v9.0
 - Upgrade License to BIG-IP v4.5 or v4.6
 - Downgrade License to BIG-IP v4.2 or Earlier
 - Add SSL to BIG-IP v4.2 or Earlier
- ISMAN PRODUCTS
 - Activate License
- FIREPASS PRODUCTS
 - Activate License for FirePass v5.x - v6.x
- TRAFFICSHIELD PRODUCTS
 - Activate License
- WEBACCELERATOR PRODUCTS
 - Activate License
- WANJET PRODUCTS
 - Activate License for WANJet 4.x
- CENTRALIZED MANAGEMENT PRODUCTS
 - Activate License for BIG-IQ
 - Activate License for Enterprise Manager
- ARX PRODUCTS
 - Activate License for ARX v5.3.0 and higher
 - Upgrade License to ARX v6.x.x

(8) ライセンスキーが表示されるので、全てをコピー(またはファイルをダウンロード)します。

Home / Product Licensing / Activate F5 Product / Finished

Activate F5 Product

Cut and paste your license key from the form below, or click the download button to download a copy of the license file.

Download license

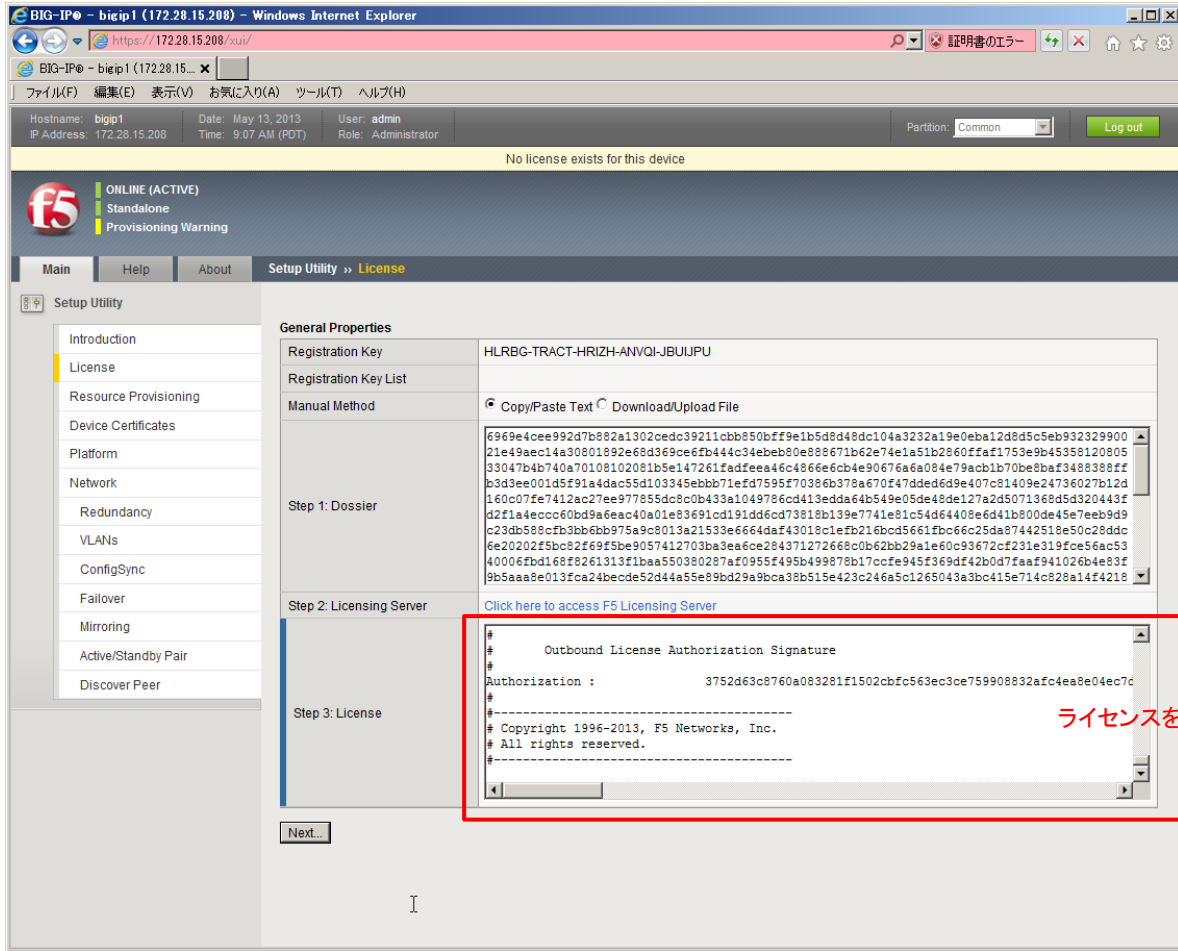
```
Auth vers : 5b
BIG-IP System License Key File
DO NOT EDIT THIS FILE!
Install this file as "/config/bigip.license".
Contact information in file /CONTACTS
Warning: Changing the system time while this system is running
with a time-limited license may make the system unusable.
Usage : Evaluation
Only the specific use referenced above is allowed. Any other uses are prohibited.
Vendor : F5 Networks, Inc.
Module List
active module : LTM, 1 Gbps, VE[NKHRPOT-MNYRRDL]IPV6 Gateway|Rate
Shaping|Ram Cache|50 MBPS COMPRESSION|SSL 500 TPS Per Core|Anti-Virus
Checks|Base Endpoint Security Checks|Firewall Checks|Network Access|Secure Virtual
Keyboard|APM, Web Application|Machine Certificate Checks|Protected
Workspace|Remote Desktop|App Tunnel
optional module : Acceleration Manager, VE
optional module : APM, VE
optional module : APM, Base, VE
```

ライセンス情報。
コピーまたは、
ファイルを
ダウンロード。

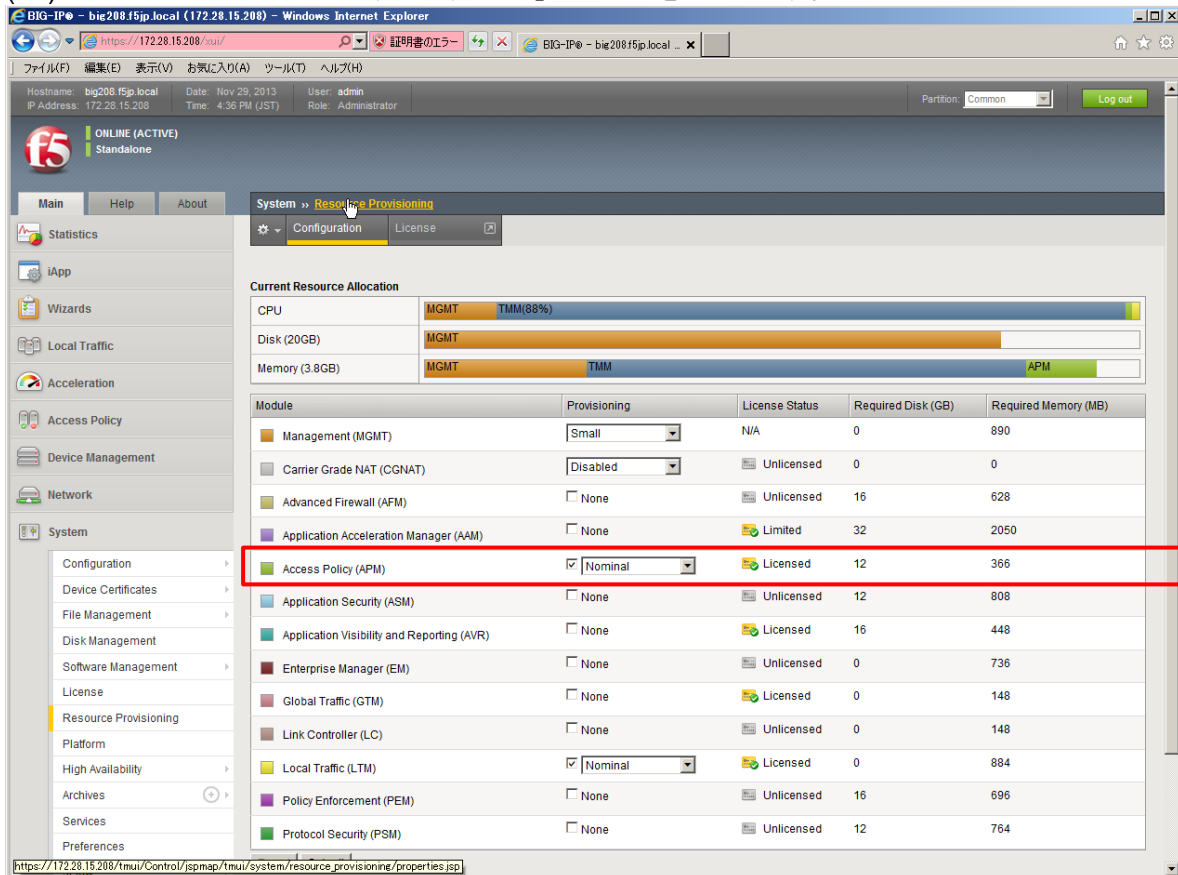
OPTIONS

Start

(9) Web サイトでコピーしたライセンスを、「Step3:License」欄に貼り付けます。「Next」ボタンを押します。



(10) プロビジョニング画面がでますので、「APM」にチェックを入れます。



(11)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
IP Address: 172.28.15.208
Date: May 13, 2013
Time: 9:11 AM (PDT)
User: admin
Role: Administrator
Partition: Common
Log out

ONLINE (ACTIVE)
Standalone

Main Help About Setup Utility >> Device Certificates

Setup Utility

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

General Properties

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

Certificate Properties

Public Key	2048 bits
Expires	May 11 15:28:06 2023 GMT
Version	3
Serial Number	e9:e6:5f:8d:e9:ef:ad:9b
Subject	Common Name: localhost.localdomain Organization: MyCompany Division: MyOrg Locality: Seattle State Or Province: WA Country: --
Issuer	Self
Subject Alternative Name	
Public Key Type	RSA

Back Import... Next...

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

Hostname: bigip1
IP Address: 172.28.15.208
Date: May 13, 2013
Time: 9:12 AM (PDT)
User: admin
Role: Administrator
Partition: Common
Log out

ONLINE (ACTIVE)
Standalone

Activation Complete
Configure your platform.

Main Help About Setup Utility >> Platform

Setup Utility

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

General Properties

Management Port Configuration: Automatic (DHCP) Manual

Management Port: IP Address[/prefix]: 172.28.15.208
Network Mask: 255.255.255.0
Management Route: 172.28.15.254

Host Name: big208.f5.jp.local (ホスト名を FQDN で指定。)

Host IP Address: Use Management Port IP Address

Time Zone: AsiaTokyo (タイムゾーンを指定。)

User Administration

Root Account: Password:
Confirm:

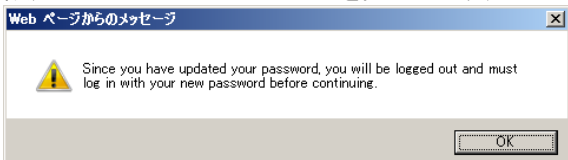
Admin Account: Password:
Confirm:

SSH Access: Enabled

SSH IP Allow: * All Addresses

Back Next...

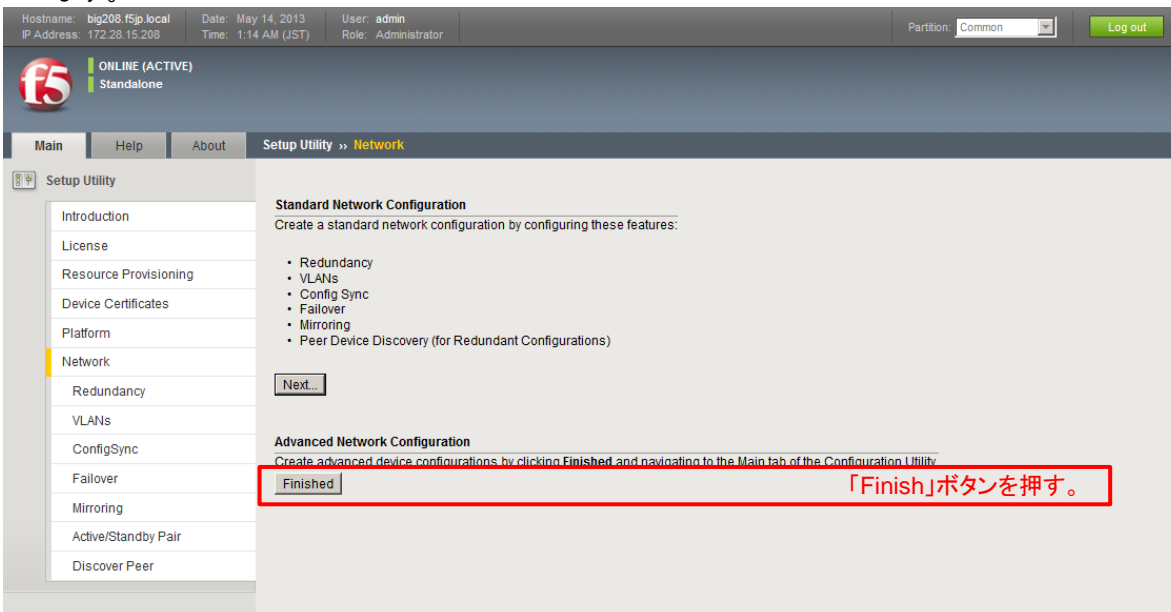
設定したパスワードでログインを試みるよう、ログアウト→ログインするように指示があります。「OK」ボタンを押します。



(13)Username = Admin と、設定したパスワードで再度ログインします。



(14)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

まず、VLAN を作成します。

「Main」メニュー → 「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 の設定

Hostname: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 2:19 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

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

General Properties

Name: external 名前(任意)を指定。
Description:
Tag:

Resources

Interfaces: Untagged: 1.1 Available: 1.2, 1.3 Tagged:
ポートを選択。

Configuration: Basic

Source Check:
MTU: 1500

sFlow

Polling Interval: Default Default Value: 10 seconds
Sampling Rate: Default Default Value: 2048 seconds

Cancel Repeat Finished

(2) Internal VLAN の設定

Hostname: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 2:20 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

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

General Properties

Name: internal 名前(任意)を指定。
Description:
Tag:

Resources

Interfaces: Untagged: 1.2 Available: 1.1, 1.3 Tagged:
ポートを選択。

Configuration: Basic

Source Check:
MTU: 1500

sFlow

Polling Interval: Default Default Value: 10 seconds
Sampling Rate: Default Default Value: 2048 seconds

Cancel Repeat Finished

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。
BIG-IP 自身に設定する IP アドレスを、Self IP と呼びます。

「Main」メニュー → 「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 IP 設定

The screenshot shows the 'New Self IP' configuration page in the BIG-IP web interface. The 'Name' field is set to 'external-ip', 'IP Address' to '10.99.1.208', and 'Netmask' to '255.255.255.0'. The 'VLAN / Tunnel' dropdown is set to 'external'. The 'Port Lockdown' dropdown is set to 'Allow None'. The 'Traffic Group' dropdown is set to 'traffic-group-local-only (non-floating)'. The 'Inherit traffic group from current partition / path' checkbox is unchecked. The 'Self IPs' menu item in the left sidebar is highlighted with a red box. Red annotations with arrows point to the configuration fields: '名前(任意)、IP アドレス、サブネットマスク、VLAN を設定。' points to the Name, IP Address, and Netmask fields; 'このアドレス上でのサービス(SSH/GUI アクセス等)を拒否。' points to the Port Lockdown field.

(2) Internal VLAN の IP 設定

The screenshot shows the 'New Self IP' configuration page in the BIG-IP web interface. The 'Name' field is set to 'internal-ip', 'IP Address' to '10.99.2.208', and 'Netmask' to '255.255.255.0'. The 'VLAN / Tunnel' dropdown is set to 'internal'. The 'Port Lockdown' dropdown is set to 'Allow Default'. The 'Traffic Group' dropdown is set to 'traffic-group-local-only (non-floating)'. The 'Inherit traffic group from current partition / path' checkbox is unchecked. The 'Self IPs' menu item in the left sidebar is highlighted with a red box. Red annotations with arrows point to the configuration fields: '名前(任意)、IP アドレス、サブネットマスク、VLAN を設定。' points to the Name, IP Address, and Netmask fields; 'このアドレス上でのサービス(SSH/GUI アクセス等)を許可。' points to the Port Lockdown field.

(3) 一覧では、以下のような状態になります。

Hostname: big208.f5jp.local Date: Jul 23, 2013 User: admin
IP Address: 172.28.15.208 Time: 9:03 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics
iApp
Local Traffic
Acceleration
Device Management

Network

- Interfaces
- Routes
- Self IPs
- Packet Filters
- Trunks
- Tunnels
- Route Domains
- VLANs
- ARP
- IPsec
- WCCP

System

Network >> Self IPs

Self IP List Create...

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	external-ip		10.99.1.208	255.255.255.0	external	traffic-group-local-only	Common
<input type="checkbox"/>	internal-ip		10.99.2.208	255.255.255.0	internal	traffic-group-local-only	Common

Delete...

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

「Main」メニュー → 「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 'New Route...' configuration page in the f5 management console. The 'Properties' section is filled with the following values:

Name	default-GW	任意の名称を入力。
Description		
Destination	0.0.0.0	左記の通りに入力。
Netmask	0.0.0.0	
Resource	Use Gateway...	
Gateway Address	IP Address 10.99.1.254	ゲートウェイのアドレスを入力。
MTU	0	

Buttons: Cancel, Repeat, Finished

4.3.2. オフィス内サーバへのルーティング設定

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。

The screenshot shows the 'New Route...' configuration page in the f5 management console. The 'Properties' section is filled with the following values:

Name	Office-Servers	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	0	

Buttons: Cancel, Repeat, Finished

5. 初級編

5.1. ウィザードを使って設定する方法

ウィザード(Wizards)を利用すると、ネットワークアクセス設定に必要な情報が一通りそろっていれば、簡単に 10 分程度で設定することができます。

(1) 「Main」メニュー → 「Wizards」 → 「Device Wizards」で、「Network Access Setup ...」を選択します。

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
IP Address: 172.28.15.208 Time: 8:07 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Wizards » Device Wizards

Wizard List

Wizard Section

Access Policy Manager Configuration

Network Access Setup Wizard for Remote Access
 Portal Access Setup Wizard
 Web Application Access Management for Local Traffic Virtual Servers

Description

Description: Configure a network access VPN connection for remote access. Creates an access policy and local traffic virtual server so that end users can establish a full network access VPN connection to internal resources.

Next...

Network Access...を選択。

(2) 以下の情報を入力 (または選択) します。

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
IP Address: 172.28.15.208 Time: 8:08 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Warning!
Self IP (IPv6 Address) is not configured. If you require IPv6 connectivity, please complete the Basic Network Configuration with IPv6 addresses.

Main Help About

Wizards » Device Wizards » Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

1. Basic Properties

Specify basic properties for the access policy.

2. System DNS/NTP Configuration

3. Select Authentication

4. Lease Pool

5. Network Access

6. DNS Hosts

7. Virtual Server (HTTPS connection)

8. Review

9. Setup Summary

Tips and Resources

Understanding the Network Access Wizard
Testing your Network Access configuration
More editing...

For help on specific configuration options click the Help tab located above this section.

Basic Properties

The Policy Name specifies the name of the access policy to be created, and is used as the naming prefix for other objects tied to the access policy (e.g. my_ap, my_ap_vs, my_ap_aaa_svr, my_ap_webtop, etc.). This name must be unique, and not already in use on the system.

The Default Language specifies the language to be displayed to end users by default. Choices are English (en), Japanese (jp), Simplified Chinese (zh-cn), and Traditional Chinese (zh-tw).

The Client Side Checks checkbox allows you to add a simple antivirus client-side check to the access policy, to ensure end users connecting have antivirus software enabled. You can later configure this antivirus check for specific antivirus vendor products, versions, and virus definition dates.

Policy Name: NetAccess-001

Default Language: en

Full Webtop: Enabled

Caption: NetAccess-001

Client Side Checks: Enable Antivirus Check in Access Policy

Cancel Next

任意の名称を入力。

クライアント PC で表示される認証画面の言語を選択。

(自動的に Policy Name が入る。)

※ クライアント PC のアンチウイルスソフトウェアのチェック。
本例では、テスト用クライアント PC にアンチウイルスソフトがインストールされていないので、チェックを外します。

※このチェックボックスを有効にしておくことで、クライアント PC 内にインストールされているアンチウイルスソフトウェアのチェックが行われます。詳しくは、[\[参考\]アンチウイルスソフトウェアのチェックについて](#) を参照ください。

(3) DNS と Time Server(NTP)の IP アドレスを入力します。

The screenshot shows the 'System DNS/NTP Configuration' step of the Network Access Setup wizard. The interface includes a sidebar with navigation steps (Basic Properties, System DNS/NTP Configuration, Select Authentication, Lease Pool, Network Access, DNS Hosts, Virtual Server, Review, Setup Summary) and a main configuration area. The main area is divided into three sections: DNS Lookup Server List, DNS Search Domain List, and Time Server List. Each section has an 'Add' button and a list of entries. Red boxes highlight the 'Add' buttons and the IP addresses entered in the 'Address' fields. Japanese annotations provide instructions on how to use these buttons.

System DNS/NTP Configuration

Please configure system DNS and NTP server settings. These system settings are critical for correct operation of created access policies.

Properties

DNS Lookup Server List

Address: 10.99.2.218
Add
10.99.2.218

DNS Search Domain List

Address
Add
localhost

DNS Cache

Time Server List

Address: 10.99.2.201
Add
10.99.2.201

Cancel Previous Next

DNS の IP アドレスを入力し、「Add」ボタンを押す。

NTP の IP アドレスを入力し、「Add」ボタンを押す。

(4) 利用する認証サーバ(Active Directory)を選択します。

The screenshot shows the 'Select Authentication' step of the Network Access Setup wizard. The interface includes a sidebar with navigation steps (Basic Properties, System DNS/NTP Configuration, Select Authentication, Lease Pool, Network Access, DNS Hosts, Virtual Server, Review, Setup Summary) and a main configuration area. The main area is divided into two sections: Authentication Options and Select Authentication. The Authentication Options section has radio buttons for 'Create New' and 'Use Existing'. The Select Authentication section has radio buttons for various authentication methods: RADIUS, LDAP, Active Directory, Second, HTTP, OCSP Responder, CRLDP, TACACS, and No Authentication. Red boxes highlight the 'Create New' and 'Active Directory' options. A red dashed box highlights the 'No Authentication' option with a Japanese annotation. Japanese annotations provide instructions on how to select the authentication method.

Select Authentication

Please select the type of authentication you would like to configure for your access policy. When end users access the virtual server they will be shown a logon page to enter credentials. These credentials are checked against a preconfigured external authentication server.

If you would like to test a basic access policy without authentication, you are not authenticating users at all, or you will configure authentication later, you can select No Authentication. To add authentication later, create a new AAA server, then edit your access policy and add an authentication action.

Authentication Options

Create New Use Existing

Select Authentication

RADIUS
 LDAP
 Active Directory
 Second
 HTTP
 OCSP Responder
 CRLDP
 TACACS
 No Authentication

Cancel Previous Next

Create New を選択。

Active Directory を選択。

※Local User DB を利用する場合は、ここでは一旦「No Authentication」を選択。

※Local User DB を使いたい場合、ウィザード形式には Local User DB を選択する項目が存在しない(V11.4.1)ので、ウィザード設定完了後に設定変更を行います。よって、ここでは一時的に「No Authentication」を選択します。

- (5) Active Directory による認証に必要な情報を入力します。
 (Local User DB を利用する場合、「No Authentication」を選択しますので、このステップはありません。)

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
 IP Address: 172.28.15.208 Time: 8:21 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
 Standalone

Main Help About Wizards » Device Wizards » Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

- Basic Properties ✓
- System DNS/NTP Configuration ✓
- Select Authentication ✓
- Configure AAA Server** →
- Lease Pool
- Network Access
- DNS Hosts
- Virtual Server (HTTPS connection)
- Review
- Setup Summary

Configure AAA Server

Configure the authentication details for the selected authentication type. For configuration details on each authentication type, click the Help tab.

Domain Name: corp.f5.jp.local
 Server Connection: Use Pool Direct
 Domain Controller: 10.99.2.218
 Admin Name:
 Admin Password:
 Verify Admin Password:
 Kerberos Preauthentication Encryption Type: None

Cancel Previous Next

Tips and Resources

- Understanding the Network Access Wizard
- Testing your Network Access configuration
- More editing...

For help on specific configuration options click the Help tab located above this section.

- (6) IP アドレスプールを設定します。

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
 IP Address: 172.28.15.208 Time: 8:22 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
 Standalone

Main Help About Wizards » Device Wizards » Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

- Basic Properties ✓
- System DNS/NTP Configuration ✓
- Select Authentication ✓
- Configure AAA Server ✓
- Lease Pool** →
- Network Access
- DNS Hosts
- Virtual Server (HTTPS connection)
- Review
- Setup Summary

Configure Lease Pool

Lease pools are collections of IP addresses that the system assigns to users who make network access connections (client PPP addresses). A lease pool IP address is assigned to each client when the network access connection is established.

Create a lease pool that contains enough IP addresses to support your total number of expected concurrent connections. You must also ensure that there is no overlap between the IP addresses you define, and other networks within your organization.

By default these IP addresses are treated as a SNAT auto map pool and translated to the configured Self IP address when traffic is sent to your internal network. With this configuration, a return route to the lease pool from your internal network is not required. For more information on configuring SNAT and routing options, see the [Configuration Guide for BIG-IP® Access Policy Manager](#).

Supported IP Version: IPv4

Type: IP Address IP Address Range
 Start IP Address: 10.99.99.11
 End IP Address: 10.99.99.20
 Add
 10.99.99.11 - 10.99.99.20
 Edit Delete

Cancel Previous Next

Tips and Resources

- Understanding the Network Access Wizard
- Testing your Network Access configuration
- More editing...

For help on specific configuration options click the Help tab located above this section.

(7) スプリット・トンネルを設定します。

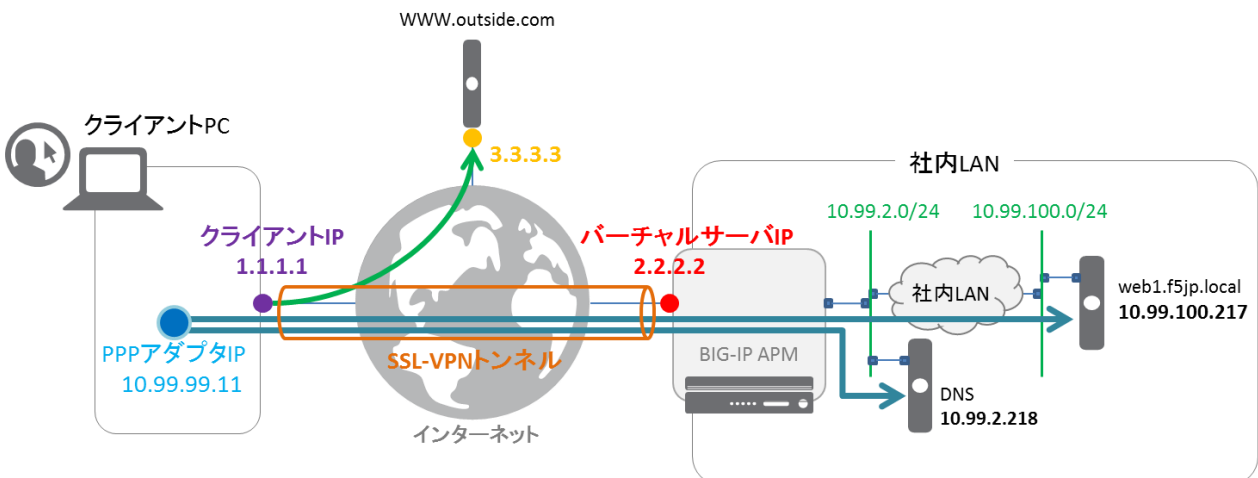
<スプリット・トンネルとは>

SSL-VPN トンネルを使う通信と、使わない通信を分けたいときにつかいます。

例えば、以下のような要件があったとします。

- ① 社内 LAN のサーバは、10.99.2.0/24 と 10.99.100.0/24 に設置されているので、それらは SSL-VPN トンネルを使いたい。
- ② しかし、同時にインターネットも使いたい。

このような要件を実現するのがスプリット・トンネルです。



「Use split Tunneling for Traffic」を選択し、トンネルに向かわせたいネットワーク帯(10.99.2.0/24, 10.99.100.0/24)を指定することで、そのネットワークだけは SSL-VPN トンネルを通り、それ以外は、クライアント IP(上図の 1.1.1.1)を使ってインターネット(上図 3.3.3.3 の web サーバへの通信)を使う、ということが可能になります。

(8) クライアント PC に割り当てたい情報を設定します。

The screenshot shows the 'Configure DNS Hosts for Network Access' step of the Network Access Setup wizard. The left sidebar lists steps 1 through 10, with '7. DNS Hosts' selected. The main area contains the following fields:

- IPv4 Primary Name Server: 10.99.2.218
- IPv4 Secondary Name Server: (empty)
- Primary WINS Server: (empty)
- Secondary WINS Server: (empty)
- DNS Default Domain Suffix: f5jp.local
- Static Hosts: (empty table with 'Add', 'Edit', and 'Delete' buttons)

Navigation buttons at the bottom include 'Cancel', 'Previous', and 'Next'.

クライアント PC の PPP アダプタに、SSL-VPN トンネル確立後に割り当てられる DNS サーバと DNS サフィックス※。

※ここに指定した DNS サフィックス宛の通信(f5jp.local)は、この DNS サーバを利用する、という設定です。

(9) バーチャルサーバを設定します。

The screenshot shows the 'Virtual Server (HTTPS connection)' step of the Network Access Setup wizard. The left sidebar lists steps 1 through 10, with '8. Virtual Server (HTTPS connection)' selected. The main area contains the following fields:

- Virtual Server IP Address: 10.99.1.101
- Redirect Server: Create Redirect Virtual Server (HTTP to HTTPS)

Navigation buttons at the bottom include 'Cancel', 'Previous', and 'Next'.

バーチャルサーバの IP アドレス。

※HTTP(80)から HTTPS(443)へリダイレクトする VS も同時に設定。

※このチェックボックスを有効にすることで、HTTP(80)で Virtual Server へアクセスしても、自動的に HTTPS(443)へリダイレクトする Virtual Server が生成されます。不要であれば、チェックを外してください。

(10) 設定のレビュー(確認のみ)です。

Hostname: big208.f5jp.local Date: Dec 4, 2013 User: admin
IP Address: 172.28.15.208 Time: 8:42 PM (JST) Role: Administrator Partition: Common Log out

f5 ONLINE (ACTIVE)
Standalone

Main Help About Wizards » Device Wizards » Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

- Basic Properties ✓
- System DNS/NTP Configuration ✓
- Select Authentication ✓
- Configure AAA Server ✓
- Lease Pool ✓
- Network Access ✓
- DNS Hosts ✓
- Virtual Server (HTTPS connection) ✓
- Review** →
- Setup Summary

Review your configuration.

Tips and Resources

- Understanding the Network Access Wizard
- Testing your Network Access configuration
- More editing...

For help on specific configuration options click the Help tab located above this section.

Review Configuration

Please check your configuration below. To change a setting, use the **Previous** button to go back to the page you want to edit. Click **Next** to complete the configuration and apply the settings. Click **Cancel** to quit the wizard without making any changes.

General Properties

Policy Name	NetAccess-001
Default Language	en
Enable Antivirus Check in Access Policy	Disabled
Full Webtop	Disabled

System DNS/NTP Configuration

DNS Lookup Server List	10.99.2.218
DNS Search Domain List	localhost
DNS Cache	Disabled
Time Server List	10.99.2.201

Authentication

Type	Active Directory
Domain Controller	10.99.2.218
Domain Name	corp.f5jp.local
Admin Name	
Admin Password	
accesscontrol.aaaservers.padataEncType	0

Network Access

Compression	No Compression
Traffic Options	Use split tunneling for traffic
IPv4 LAN Address Space	10.99.2.0 / 255.255.255.0 10.99.100.0 / 255.255.255.0
Allow Local Subnet	Disabled
Prohibit routing table changes during Network Access connection	Disabled
DTLS	Disabled
Assigned IPv4 Lease Pool	NetAccess-001_ip
IPv4 Primary Name Server	10.99.2.218
IPv4 Secondary Name Server	
Primary WINS Server	
Secondary WINS Server	
DNS Default Domain Suffix	f5jp.local

Virtual Server

Virtual Server IP Address	10.99.1.101
Create Redirect Virtual Server (HTTP to HTTPS)	Enabled

Cancel Previous **Next**

(11)設定のサマリ(これも確認のみ)です。

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
IP Address: 172.28.15.208 Time: 8:42 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Wizards » Device Wizards » Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

1. Basic Properties ✓
2. System DNS/NTP Configuration ✓
3. Select Authentication ✓
4. Configure AAA Server ✓
5. Lease Pool ✓
6. Network Access ✓
7. DNS Hosts ✓
8. Virtual Server (HTTPS connection) ✓
9. Review ✓
10. Setup Summary **▶**

View Access Policy and objects created by wizard.

Tips and Resources

- Understanding the Network Access Wizard
- Testing your Network Access configuration
- More editing...

For help on specific configuration options click the Help tab located above this section.

Setup Summary

This screen displays the configuration for the access policy you created.

To edit an object associated with this access policy from this screen, click the object link. Clicking a link on this page finishes the wizard configuration, like clicking the **Finished** button. You will not return to this page.

To see a summary of objects associated with an access policy after completing this wizard, navigate to **Access Policy : Access Profiles**, click on the access policy name, and then click the **Access Policy** tab. To edit an object associated with the access policy, click on the object name.

Later, you can configure your own objects. The virtual servers are created on the navigation pane under **Local Traffic**. All other objects are created on the navigation pane under **Access Policy**.

Click **Finished** to close this screen.

Access Profile	Access Policy
NetAccess-001	Edit Access Policy in Visual Policy Editor

AAA Servers

Name	Type
NetAccess-001_aaa_srv	Active Directory

Network Access

Name	Description	IPv4 Lease Pool	IPv6 Lease Pool	Client Traffic Classifiers
NetAccess-001_na_res		NetAccess-001_ip		

Lease Pools

Name	IP Version	Members
NetAccess-001_ip	IPv4 LeasePool	1

Webtops

Name	URI
NetAccess-001_webtop	

Profiles

Name	Type	Parent Profile
NetAccess-001_cp	Connectivity Profile	connectivity

Virtual Servers

Status	Name	Partition	Destination	Service Port	Type
On	NetAccess-001_vs	Common	10.99.1.101	443 (HTTPS)	Standard
On	NetAccess-001_vs_redirect	Common	10.99.1.101	80 (HTTP)	Standard

Finished

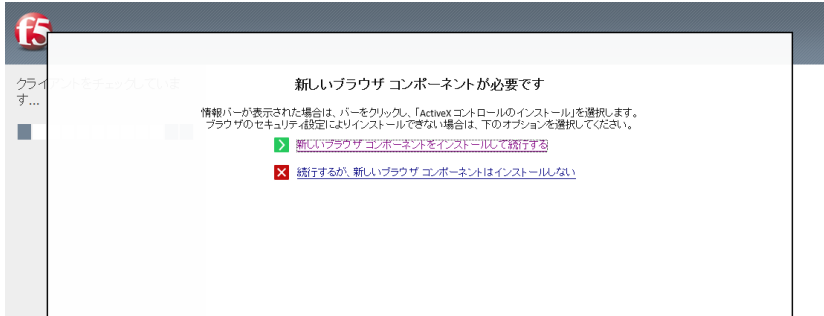
以上でネットワークアクセス設定は完了です。

5.2. クライアントからのアクセス

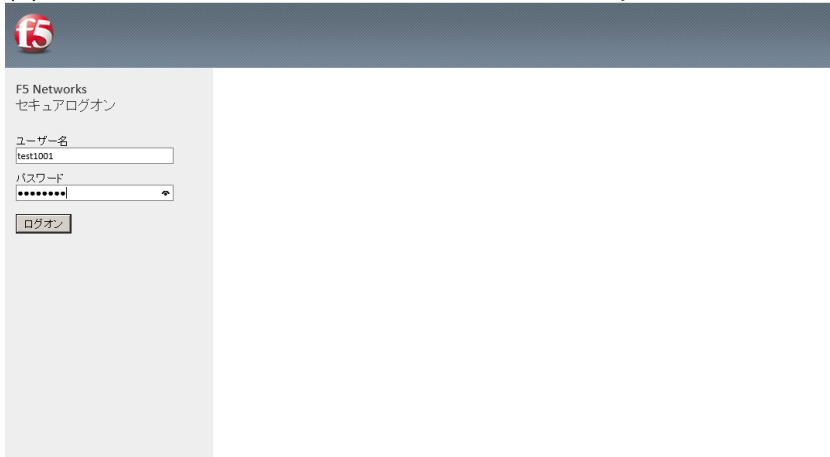
5.2.1. Windows の Web ブラウザからのアクセス

クライアント PC の Web ブラウザから、設定した Virtual Server へアクセスします。
Windows 7 + Internet Explorer を使った場合の例です。

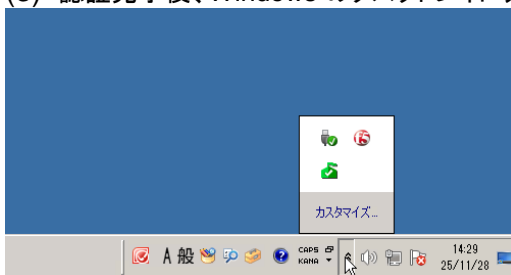
- (1) 初アクセス時には、SSL-VPN クライアント用の ActiveX コンポーネントをインストールする必要があります。
インストールするためには、Windows の管理者権限が必要です。



- (2) 認証フォーム画面が現れますので Active Directory に登録されているユーザ名とパスワードを入力します。



- (3) 認証完了後、Windows のタスクトレイに入ります。



5.2.2. Windows 用 Edge Client ソフトウェアからのアクセス

Windows クライアント用ソフトウェア: Edge Client を利用する手順を以下に示します。

このソフトウェアは、BIG-IP APM からクライアント PC (Windows または Mac) へダウンロードして利用するソフトウェアです。

このソフトウェアは、プロトコルレベルで行っていることは Web ブラウザと同様ですが、Web ブラウザでは実現できない、いくつかの便利な機能を実装しています。

例えば、Windows へのログイン時に利用する ID と Password を使うように Edge Client に設定すると、BIG-IP APM へのログイン時には、ID/Password の入力を求められることなく、自動的に APM へ接続することが可能です。

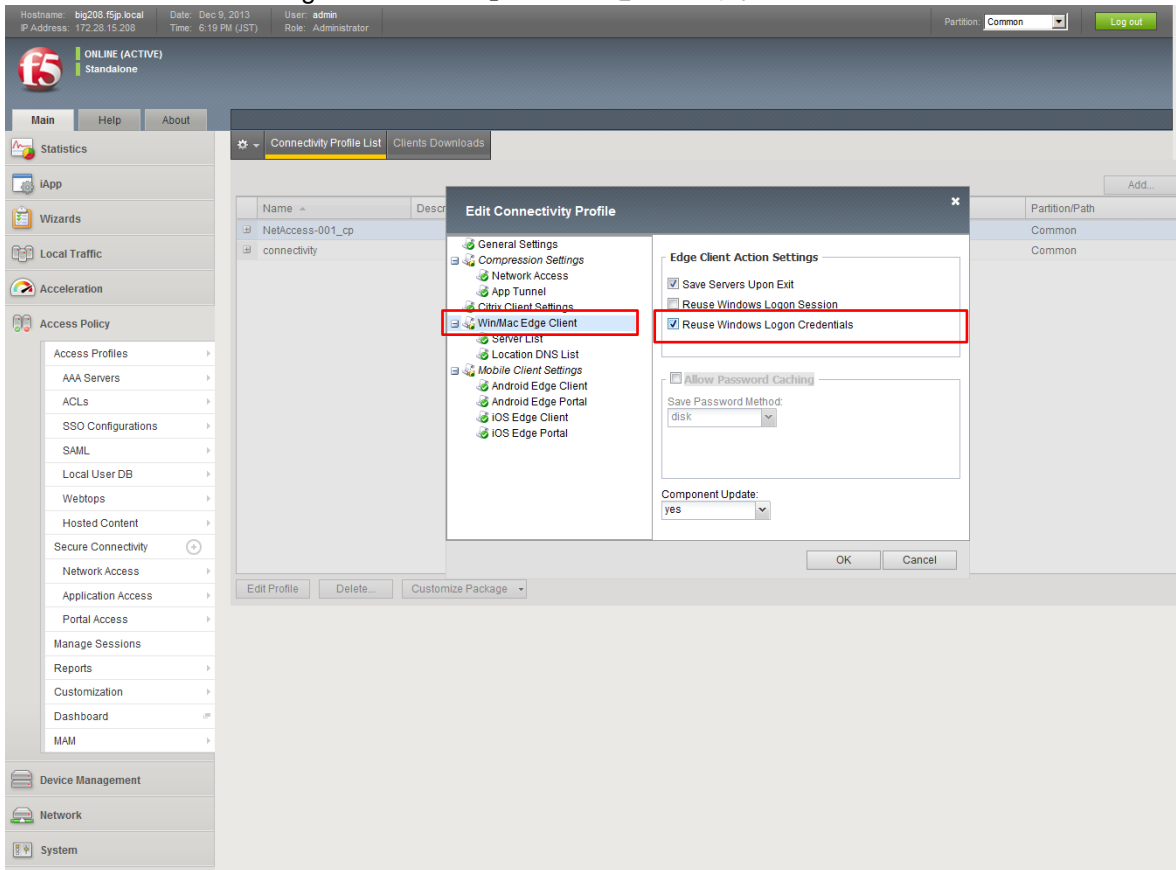
サンプルとして、以下にその設定方法を示します。

- (1) 「Main」メニュー → 「Access Policy」 → 「Secure Connectivity」で、以下の画面が表示されます。
該当する Connectivity Profile をクリックし、「Edit Profile」ボタンを押します。

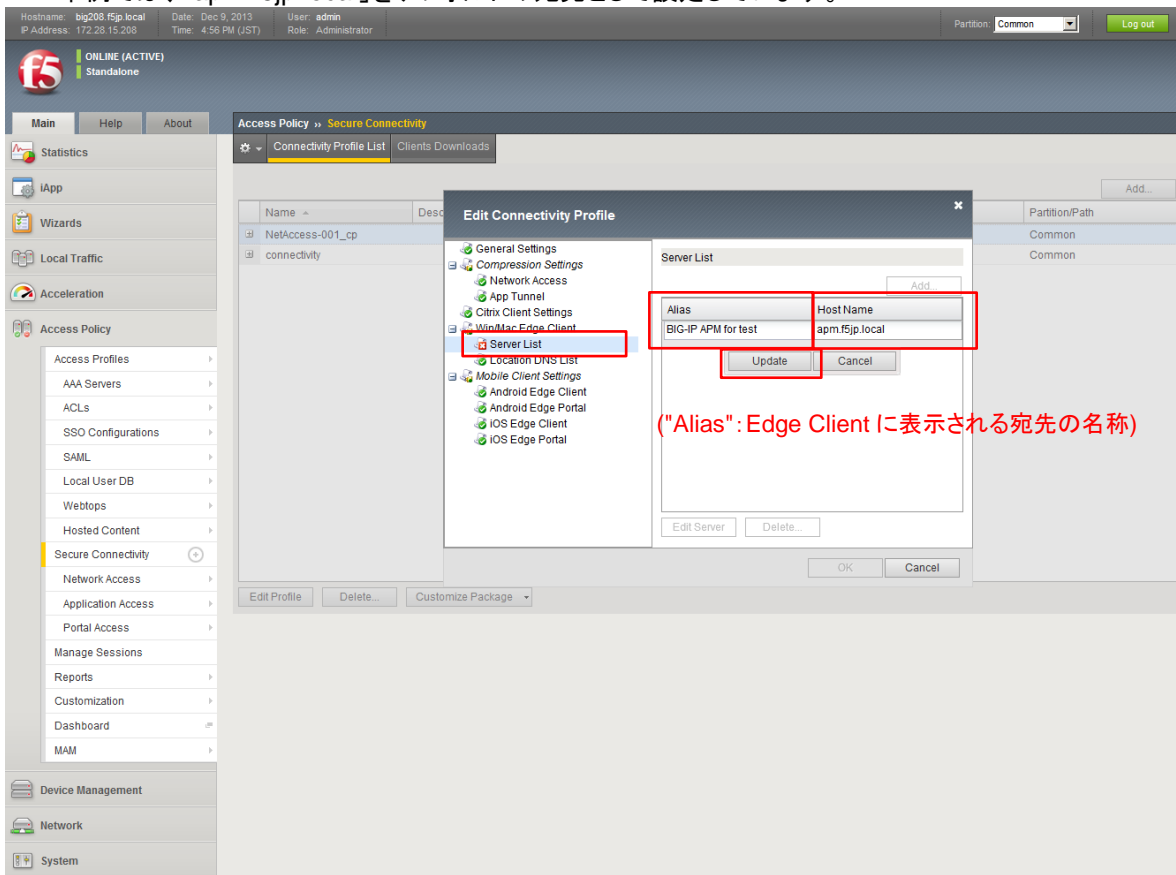
The screenshot shows the BIG-IP APM web interface. The top navigation bar includes 'Main', 'Help', and 'About'. The left sidebar contains various menu items, with 'Access Policy' expanded to show 'Secure Connectivity'. The main content area displays the 'Connectivity Profile List' table. The table has columns for Name, Description, Parent Profile, Application, Virtual Servers, and Partition/Path. The row for 'NetAccess-001_cp' is selected and highlighted in blue. A red box highlights the 'Edit Profile' button at the bottom of the table. A red arrow points to the selected row with the text 'クリック。' (Click).

Name	Description	Parent Profile	Application	Virtual Servers	Partition/Path
NetAccess-001_cp		/Common/connectivity		NetAccess-001_vs	Common
connectivity					Common

- (2) 「Win/Mac Edge Client」をクリックすると、以下の画面が現れます。
「Reuse Windows Logon Credentials」にチェックを入れます。



- (3) Edge Clientを使う際に、デフォルトの宛先を指定しておきます。
「Server List」をクリックすると、以下の画面が現れます。
本例では、「apm.f5jp.local」をデフォルトの宛先として設定しています。



- (4) 「Customize Package」横の▼をクリックすると、「Windows」用か「Mac」用かの選択が現れます。
ここでは、「Windows」を選択します。

The screenshot shows the F5 NetAccess configuration interface. The top status bar displays: Hostname: big208.f5.jp.local, Date: Dec 9, 2013, Time: 7:25 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation menu includes Main, Help, and About. The left sidebar contains various configuration categories like Statistics, iApp, Wizards, Local Traffic, Acceleration, and Access Policy. The 'Access Policy' section is expanded to show 'Secure Connectivity'. The main content area is titled 'Access Policy >> Secure Connectivity' and contains a 'Connectivity Profile List' table. The table has columns for Name, Description, Parent Profile, Application, Virtual Servers, and Partition/Path. Two rows are visible: 'NetAccess-001_cp' and 'connectivity'. Below the table, there are buttons for 'Edit Profile', 'Delete...', and 'Customize Package'. The 'Customize Package' button has a dropdown arrow pointing down, which is highlighted with a red box. The dropdown menu is open, showing two options: 'Windows' and 'Mac', with 'Windows' selected and highlighted by a red box.

- (5) 本例では、この設定はデフォルトのままです。

The screenshot shows the F5 NetAccess configuration interface with the 'Customize Windows Client Package' dialog box open. The top status bar displays: Hostname: big208.f5.jp.local, Date: Dec 7, 2013, Time: 8:11 AM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation menu includes Main, Help, and About. The left sidebar contains various configuration categories like Statistics, iApp, Wizards, Local Traffic, Acceleration, and Access Policy. The 'Access Policy' section is expanded to show 'Secure Connectivity'. The main content area is titled 'Access Policy >> Secure Connectivity' and contains a 'Connectivity Profile List' table. The table has columns for Name, Description, Parent Profile, Application, Virtual Servers, and Partition/Path. Two rows are visible: 'NetAccess-001_cp' and 'connectivity'. Below the table, there are buttons for 'Edit Profile', 'Delete...', and 'Customize Package'. The 'Customize Package' button has a dropdown arrow pointing down, which is highlighted with a red box. The dropdown menu is open, showing two options: 'Windows' and 'Mac', with 'Windows' selected and highlighted by a red box. The 'Customize Windows Client Package' dialog box is open, showing a list of available components and their status. The components are: Available Components..., BIG-IP Edge Client (checked), Dialup Settings (checked), BIG-IP Edge Client (checked), BIG-IP Edge Client COM API (checked), Web Browser Add-ons for BIG-IP Edge Client (checked), Dialup Entry/ Windows Logon Integration (checked), Endpoint Security (checked), Component Installer Service (checked), DNS Relay Proxy Service (checked), Traffic Control Service (checked), User Logon Credentials Access Service (unchecked), and Machine Certificate Checker Service (unchecked). The dialog box has 'Download' and 'Cancel' buttons at the bottom.

(6) 「BIG-IP Edge Client」をクリックします。

こちらの設定もデフォルトのままですが、「Auto launch after Windows Logon」に注目してください。この設定によって、Windows にログインすると Edge Client が自動的に起動し、APM への接続を試みます。

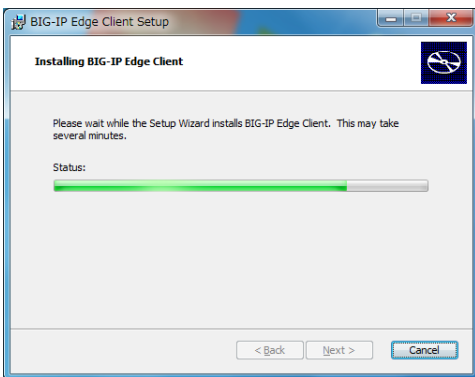
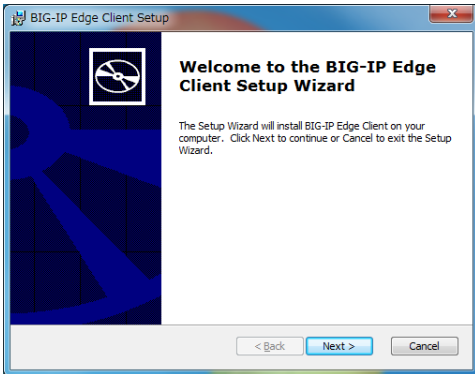
The screenshot shows the 'Customize Windows Client Package' dialog box in the BIG-IP management console. The 'Available Components' section on the left has 'BIG-IP Edge Client' selected. The 'Auto launch after Windows Logon' checkbox is checked. The 'Download' button is highlighted with a red box. A red text box at the bottom right says: 「Download」をクリックして、Windows 用 Edge Client コンポーネントをダウンロードします。

(7) 少し待つと、ダウンロードが可能な状態になります。

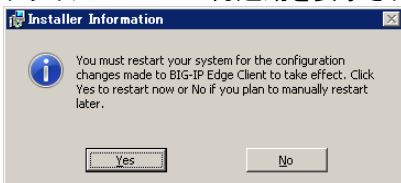
The screenshot shows the 'Connectivity Profile List' table in the BIG-IP management console. The table has columns for Name, Description, Parent Profile, Application, Virtual Servers, and Partition/Path. The 'connectivity' profile is listed. A yellow dialog box at the bottom asks for confirmation to run or save BIGIPEdgeClient.exe.

Name	Description	Parent Profile	Application	Virtual Servers	Partition/Path
NetAccess-001_cp		/Common/connectivity		NetAccess-001_vs	Common
connectivity					Common

(8) ダウンロードしたコンポーネントをクライアント PC にコピーし、インストールを行います。



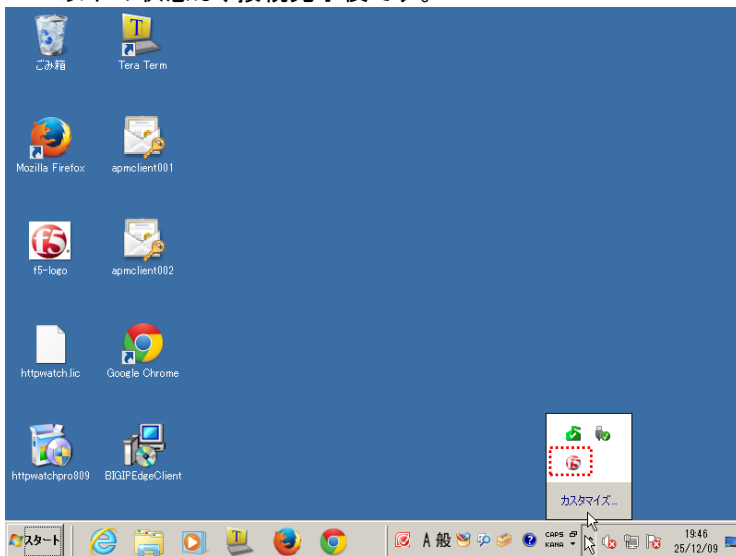
クライアント PC の再起動を要求されますので、「Yes」を選択して再起動してください。



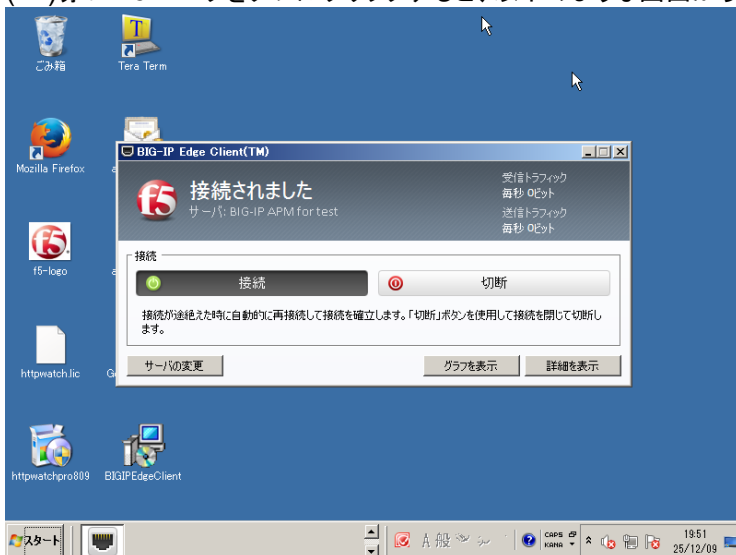
(9) 再起動後、Windows7 にログインします。



(10)Windows ログオン時の ID とパスワードを使って、自動的に APM への接続が行われます。
以下の状態は、接続完了後です。



(11)赤い F5 マークをダブルクリックすると、以下のような画面が現れます。接続されていることが分かります。

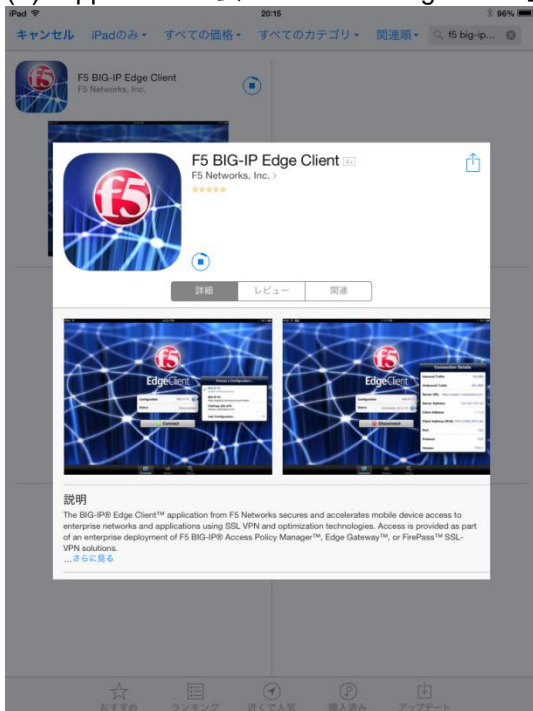


5.2.3. Apple iPad からのアクセス

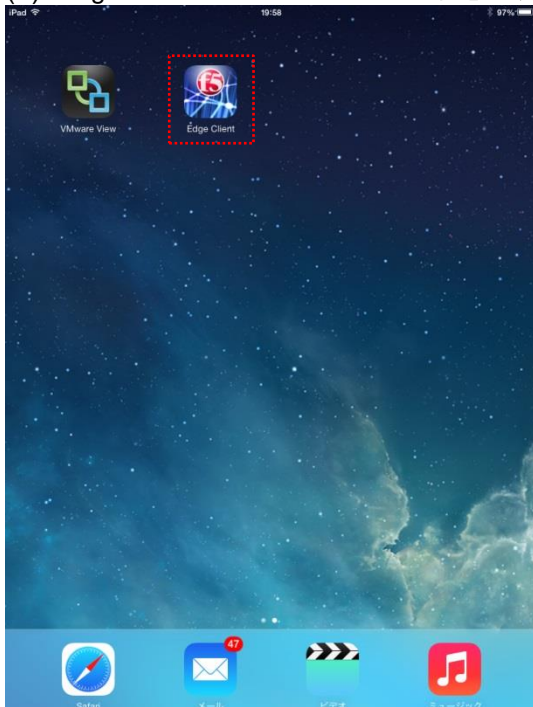
BIG-IP APM へのネットワークアクセスは、Apple iPad や Google Android からの接続も可能です。

サンプルとして、Apple iPad からの接続方法を以下に示します。

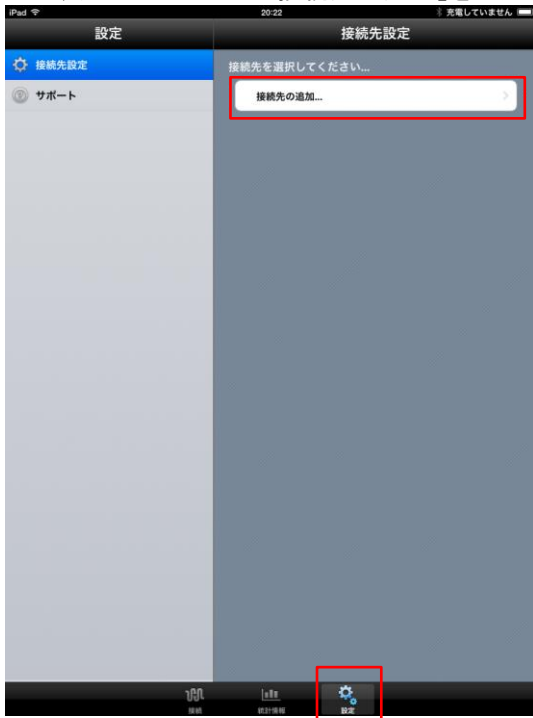
(1) App Store から、「F5 BIG-IP Edge Client」をダウンロード&インストールします。



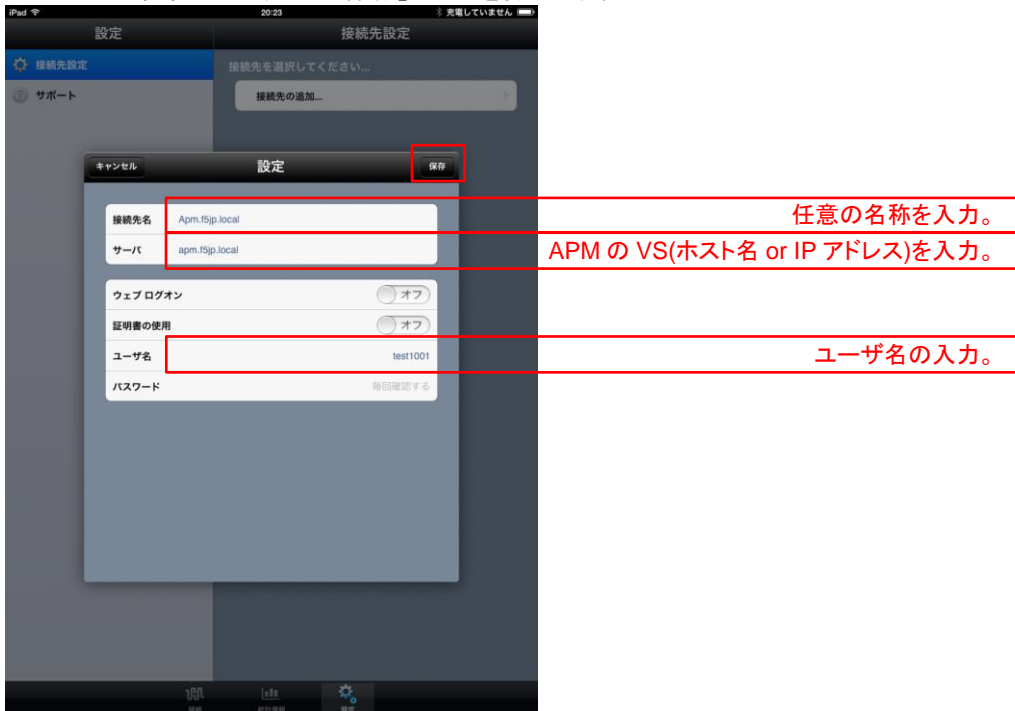
(2) Edge Client がインストールされた状態です。



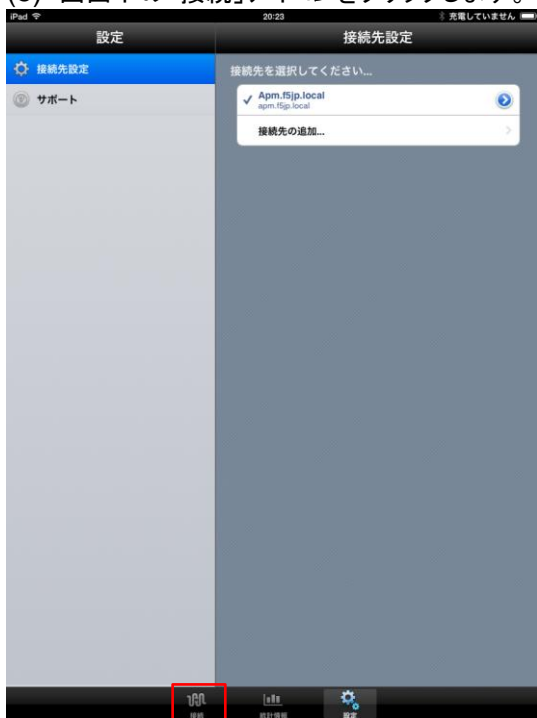
- (3) 画面下の「設定」アイコンをクリックすると、以下の画面が現れます。
表示された画面の「接続先の追加」をクリックします。



- (4) 以下の「設定」画面が現れます。必要項目を設定します。
入力が終わったら、右上「保存」ボタンを押します。



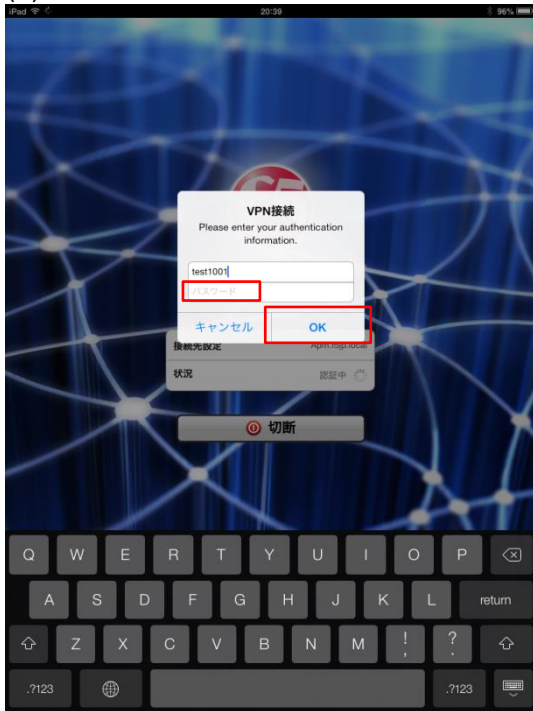
(5) 画面下の「接続」アイコンをクリックします。



(6) 「接続」ボタンを押します。



(7) パスワードを入力し、「OK」をクリックします。



(8) ネットワークアクセスの接続が成功した状態です。



以降、サファリブラウザなどから、社内サーバへのアクセスが可能となります。

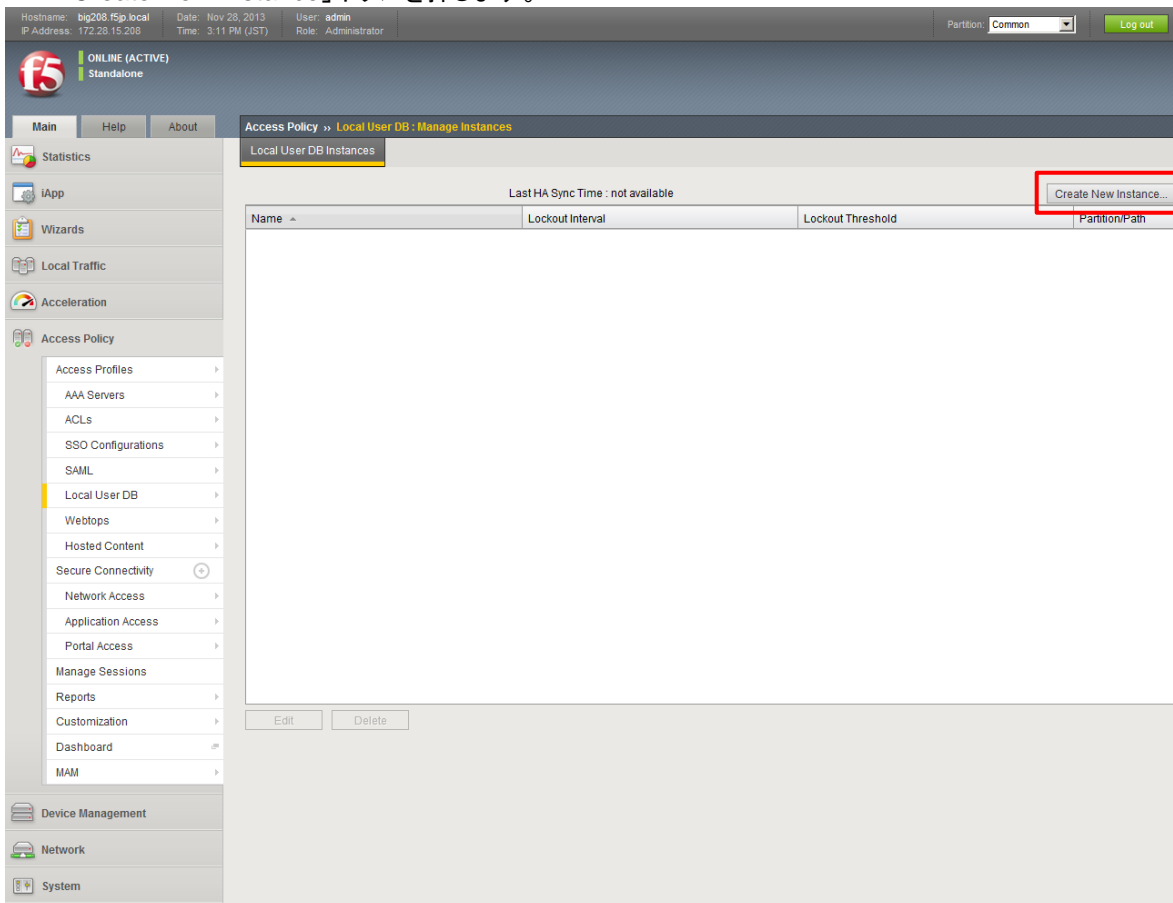
Google Android の場合もほぼ同様の手順でご利用頂けます。
Android 用 Edge Client は、Google Play からダウンロードしてください。

5.3. Local User DB による認証

Active Directory のような認証サーバがない場合、APM が持つ Local User DB を利用する方法があります。しかし、ウィザード設定では、Local User DB が選択できません(V11.4.1)。

以下に、Local User DB を利用する方法を記載します。

- (1) 既述のウィザード設定手順の中で、「Select Authentication」ページで「No Authentication」を選び、最後まで進みます。
- (2) Local User DB を設定します。
「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Instances」で以下の画面が現れます。まずは Instance (User DB の名前のようなもの) を設定します。
「Create New Instance」ボタンを押します。



(3) 「Name」欄に名称を入力し、「OK」ボタンを押します。

Hostname: big208.f5jp.local Date: Nov 28, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:11 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Access Policy >> Local User DB : Manage Instances

Local User DB Instances

Last HA Sync Time : not available Create New Instance...

Name	Lockout Interval	Lockout Threshold	Partition/Path
------	------------------	-------------------	----------------

Create New Local User DB Instance

Name: f5jp-local-user-db 任意の名称を入力。

Lockout Interval (in seconds): 600

Lockout Threshold: 3

OK Cancel

Edit Delete

(4) 以下の状態になります。

Hostname: big208.f5jp.local Date: Nov 28, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:23 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Access Policy >> Local User DB : Manage Instances

Local User DB Instances

Last HA Sync Time : not available Create New Instance...

Name	Lockout Interval	Lockout Threshold	Partition/Path
/Common/f5jp-local-user-db	600	3	Common

Edit Delete

- (5) 「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Users」で、以下の画面が現れます。「Create New User」ボタンを押します。

The screenshot shows the F5 management console interface. At the top, it displays system information: Hostname: big208.f5.jp.local, Date: Nov 28, 2013, Time: 3:12 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation menu on the left includes Statistics, iApp, Wizards, Local Traffic, Acceleration, Access Policy, Device Management, Network, and System. The 'Access Policy' menu is expanded to show 'Local User DB'. The main content area is titled 'Local User List' and contains a table with columns: User Name, First Name, Last Name, Groups, Locked Out, Locked Out At, Logon Failure, Email Address, DB Instance, and Partition/Path. Above the table are buttons for 'Import from CSV', 'Export to CSV', and 'Create New User...'. The 'Create New User...' button is highlighted with a red box. Below the table are buttons for 'Edit', 'Delete', and 'Unlock User', along with pagination information: 'Page 1 of 1'. A message at the bottom right of the table area says 'No data to display'.

- (6) Username, Passwordを入力します。「*」の部分が必須項目です。
Instanceも必須項目ですが、一つしか設定していない場合は、デフォルトでそのInstanceが選択されています。

The screenshot shows the same F5 management console interface as in the previous image, but with the 'Create New Local User' dialog box open. The dialog box has a title bar 'Create New Local User' and a close button. It contains several sections: 'User Information...' (with a plus icon), 'Personal Information...' (with a plus icon), and 'User Groups' (with a plus icon). The 'User Information...' section has three input fields: 'User Name:' (containing 'test1001'), 'Password:' (with masked characters), and 'Confirm Password:' (with masked characters). These three fields are highlighted with a solid red box. Below them is a checkbox for 'Force Password Change' which is unchecked. The 'Instance:' dropdown menu is highlighted with a red dashed box and shows the selected value '/Common/f5jp-local-user-db'. At the bottom of the dialog box are 'OK' and 'Cancel' buttons. The background of the console shows the 'Local User List' table and the 'Create New User...' button, which is now partially obscured by the dialog box.

(7) 3つのユーザを設定した状態です。

Hostname: big208.f5.jp.local Date: Nov 28, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:30 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Access Policy >> Local User DB

Local User List

Search Last HA Sync Time : not available Import from CSV Export to CSV Create New User...

<input type="checkbox"/>	User Name	First Name	Last Name	Groups	Locked Out	Locked Out At	Logon Failure	Email Address	DB Instance	Partition/Path
<input type="checkbox"/>	test1001				no	N/A	0		f5jp-local...	Common
<input type="checkbox"/>	test1002				no	N/A	0		f5jp-local...	Common
<input type="checkbox"/>	test1003				no	N/A	0		f5jp-local...	Common

Edit Delete Unlock User Page 1 of 1

No data to display

(8) 「Main」メニュー → 「Access Policy」 → 「Access Profiles」で表示された、「NetAccess-001」の行にある「Edit」をクリックします。

Hostname: big208.f5.jp.local Date: Nov 28, 2013 User: admin
IP Address: 172.28.15.208 Time: 2:50 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

Access Policy >> Access Profiles : Access Profiles List

Access Profile List Access Policy Sync Windows Group Policy List CAPTCHA Configuration List NTLM

Search Create... Import...

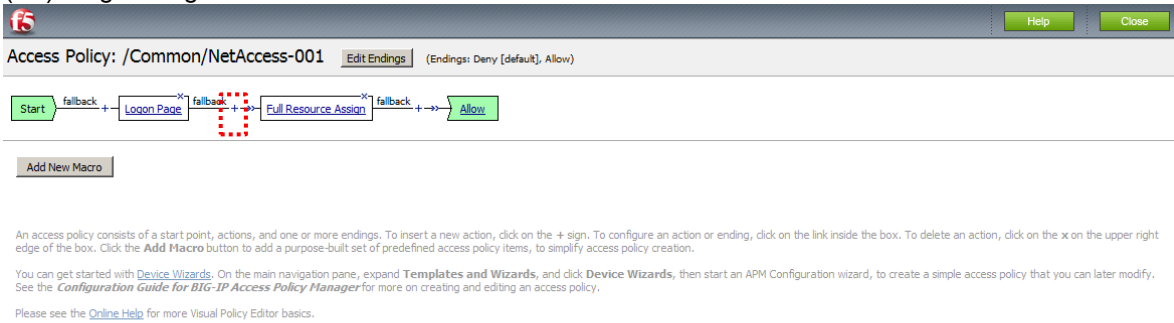
<input checked="" type="checkbox"/>	Status	Name	Application	Access Profile	Export	Copy	Virtual Servers	Partition / Path
<input type="checkbox"/>		NetAccess-001		Edit	Export...	Copy...	NetAccess-001_vs	Common
<input type="checkbox"/>		access	(none)	(none)	(none)	(none)		Common

Delete... Apply Access Policy

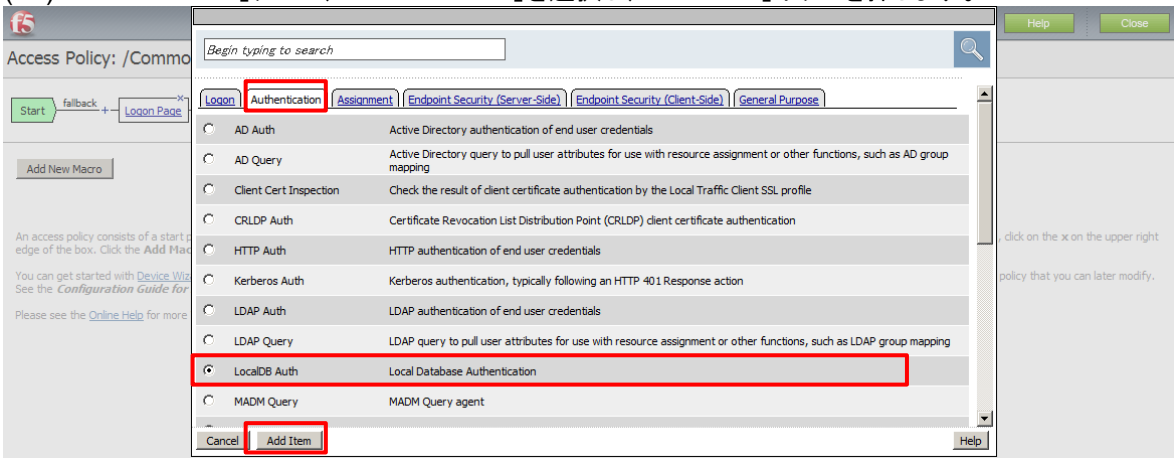
(9) 新しいウィンドウが開き、以下のような証明書に関する警告画面が表示されますが、「このサイトの閲覧を続行する」を選択してください。



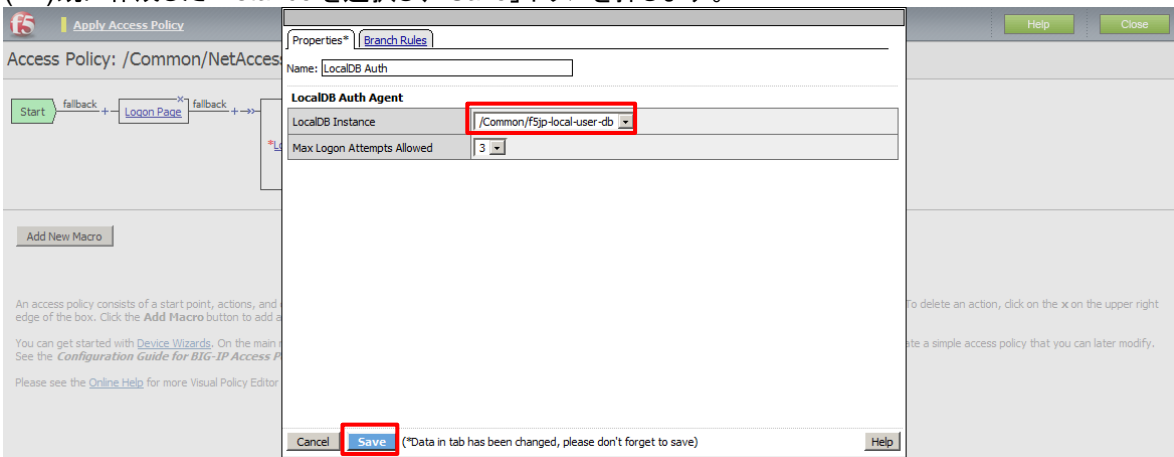
(10)「Logon Page」の後ろにある「+」ボタンをクリックします。



(11)「Authentication」タブで、「LocalDB Auth」を選択し、「Add Item」ボタンを押します。



(12)既に作成した Instance を選択し、「Save」ボタンを押します。



(13)以下の状態になります。

この段階では、設定した内容が適用されていません。

「Apply Access Policy」をクリックすることで、設定が適用されます。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(14)「Apply Access Policy」の表示が消えます。

Local User DB 認証の設定はこれで完了です。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

5.3.1. クライアント PC からのアクセス

クライアント PC から、Local User DB に登録したユーザでアクセスできることを確認します。

F5 Networks
セキュアログオン

ユーザー名
test1001

パスワード

ログオン

本製品は、F5 Networksからライセンスが付与されています。© 1999-2013 F5 Networks. All rights reserved.

5.4. [参考]アンチウイルスソフトウェアのチェックについて

BIG-IP APM では、クライアント PC 上にインストールされているアンチウイルスソフトウェアをチェックすることもできます。

そのアンチウイルスソフトウェアの一覧は、以下の画面から確認できます。

(1) 左上の「f5」の赤いマークをクリックすると、以下の画面が現れますので、「OPSWAT application integration support charts」をクリックします。

The screenshot shows the F5 configuration utility interface. At the top, there is a status bar with the following information: Hostname: big208.f5jp.local, Date: Dec 4, 2013, Time: 8:49 PM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. Below this, the 'f5' logo is highlighted with a red box, and the text 'ONLINE (ACTIVE) Standalone' is visible. The main content area is divided into several sections: 'Welcome', 'How to Use Help', 'About', 'Common Screen Elements', 'Setup', 'Support', 'Plug-ins', and 'Downloads'. The 'Support' section is expanded, showing 'Ask F5', 'Solution Center', 'DevCentral', 'Modules', 'OPSWAT Application Security Integration Support Charts', and 'Downloads'. The 'OPSWAT Application Security Integration Support Charts' link is highlighted with a red box. The 'Downloads' section is also expanded, showing 'BIG-IP Edge Client™ Components', 'SNMP MIBs', and 'SSH Clients'.

- (2) 以下のような、アンチウイルスソフトウェアの一覧が表示されます。
 ウィザード設定で、アンチウイルスソフトウェアをチェックする設定を入れる(以下の"[参考]ウィザード画面の～"を参照ください)と、この一覧上のソフトウェアがクライアント PC にインストールされているかどうかのチェックが行われます。

Antivirus integration for Windows show

OPSWAT Antivirus Integration SDK 3.6.7371.2

Product Name	Product Version	Product ID	Database Age	Check Realtime Protection State	Last Scan Time
Microsoft Corp.					
Microsoft Forefront Client Security	1.5.x	6011	Implemented	Implemented	Not Implemented
Microsoft Forefront Endpoint Protection 2010	2.x	6019	Implemented	Implemented	Implemented
Microsoft Security Essentials	2.x	6020	Implemented	Implemented	Not Implemented
Microsoft Security Essentials Microsoft Forefront Endpoint Protection 2012 System Center Endpoint Protection 2012	4.x	6020	Implemented	Implemented	Implemented
Microsoft Security Essentials [Antivirus]	1.x	6012	Implemented	Implemented	Implemented
System Center Endpoint Protection	2.x	6023	Implemented	Implemented	Implemented
System Center Endpoint Protection	4.x	6023	Implemented	Implemented	Implemented
Windows Defender	4.x	6009	Implemented	Implemented	Implemented
Windows Intune Endpoint Protection Windows Intune	2.x	6021	Implemented	Implemented	Not Implemented
Windows Intune Malware Protection [Antivirus] Windows Intune	1.x	6018	Implemented	Implemented	Implemented
Windows Live OneCare	1.5.x	6013	Not Implemented	Implemented	Not Implemented
Windows Live OneCare	1.x	6013	Not Supported	Implemented	Not Supported
Windows Live OneCare	2.x	6013	Implemented	Implemented	Not Implemented
Windows OneCare Live	0.8.x	6014	Not Implemented	Not Implemented	Not Supported
Other Microsoft Corp. Antivirus	x	6999	Implemented on Windows with Security Center (MMC)	Implemented on Windows with Security Center (MMC)	Not Implemented

[参考]ウィザード画面の Client Side Check : Enable Antivirus Check in Access Policy

Hostname: big208.f5.jp.local Date: Dec 4, 2013 User: admin
 IP Address: 172.28.15.208 Time: 8:08 PM (JST) Role: Administrator Partition: Common Log out

Warning! Self IP (IPv6 Address) is not configured. If you require IPv6 connectivity, please complete the Basic Network Configuration with IPv6 addresses.

Wizards >> Device Wizards >> Network Access Setup

Network Access Setup

Use this Setup Wizard to configure simple Access Policy for Network Access.

- Basic Properties
- System DNS/NTP Configuration
- Select Authentication
- Lease Pool
- Network Access
- DNS Hosts
- Virtual Server (HTTPS connection)
- Review
- Setup Summary

Basic Properties

The **Policy Name** specifies the name of the access policy to be created, and is used as the naming prefix for other objects tied to the access policy (e.g. my_ap, my_ap_vs, my_ap_aaa_srv, my_ap_webtop, etc.). This name must be unique, and not already in use on the system.

The **Default Language** specifies the language to be displayed to end users by default. Choices are English (en), Japanese (jp), Simplified Chinese (zh-cn), and Traditional Chinese (zh-tw).

The **Client Side Checks** checkbox allows you to add a simple antivirus client-side check to the access policy, to ensure end users connecting have antivirus software enabled. You can later configure this antivirus check for specific antivirus vendor products, versions, and virus definition dates.

Policy Name	NetAccess-001
Default Language	en
Full Webtop	<input type="checkbox"/> Enabled
Caption	NetAccess-001
Client Side Checks	<input type="checkbox"/> Enable Antivirus Check in Access Policy

Cancel Next

Tips and Resources

- Understanding the Network Access Wizard
- Testing your Network Access configuration
- More editing...

For help on specific configuration options click the Help tab located above this section.

5.5. SSL サーバ証明書の設定

BIG-IP が持つデフォルトのサーバ証明書は、正式な認証局で取得したものではないため、クライアント PC の Web ブラウザで Virtual Server へアクセスすると、以下のような警告が出ます。



以降、正式な認証局(例: Verisign, CyberTrust 等)にて署名されたサーバ証明書をインポートして利用するまでの手順を示します。

5.5.1. CSR の作成

認証局(CA)に対して、サーバ証明書の発行を依頼するための CSR(Certificate Signing Request)を作成します。「Main」メニュー → 「System」 → 「File Management」 → 「SSL Certificate List」タブで表示された画面右上の「Create」を押すと、以下の画面が表示されます。

(1) CSR 作成画面。

Hostname: big208.f5.jp.local | Date: Nov 14, 2013 | User: admin | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE) Standalone

Main Help About System > File Management > SSL Certificate List > New SSL Certificate...

General Properties

Name: NetAccess-001_cert **名前(任意)を指定。**

Certificate Properties

Issuer: Certificate Authority **Certificate Authority を選択。**

Common Name: apm.f5.jp.local **以下の項目へ値を入力。Common Name(Web サーバの FQDN)**

Division: FSE **Organization**

Organization: FSJJK **Locality**

Locality: Minato-ku **State Or Province**

State Or Province: Tokyo **Country**

Country: Japan | JP

E-mail Address:

Subject Alternative Name:

Challenge Password:

Confirm Password: **その他の値は、申請する認証局へ必須かどうかを確認ください。**

Key Properties

Key Type: RSA **申請する RSA 鍵長。**

Size: 2048 bits

Cancel Finished

5.5.3. 証明書のインポート

(1) 認証局から発行された SSL サーバ証明書をインポートします。

「Main」メニュー → 「System」 → 「File Management」 → 「SSL Certificate List」から該当するもの(本例では、NetAccess-001_cert)を選択すると、以下の画面になります。

認証局から発行されたサーバ証明書ファイルを Certificate Source で指定し、「Import」を押します。

The screenshot shows the 'SSL Certificate/Key Source' dialog box. The 'Certificate Name' is 'NetAccess-001_cert'. The 'Certificate Source' is set to 'Upload File' with the path '/Common/NetAccess-001_cert.pem'. A red box highlights the 'Certificate Source' field with the text '認証局から発行されたサーバ証明書を指定。' (Specify the server certificate issued by the certification authority). Another red box highlights the 'Import' button with the text 'Import を押す。' (Press Import).

(2) サーバ証明書がインポートされた状態です。

The screenshot shows the 'SSL Certificate List' table. The first row, 'NetAccess-001_cert', is highlighted with a red box. The table has columns for Name, Contents, Common Name, Organization, Expiration, and Partition / Path.

Name	Contents	Common Name	Organization	Expiration	Partition / Path
NetAccess-001_cert	RSA Certificate & Key	apm.f5.jp.local	F5JKK	Nov 14, 2014	Common
ca-bundle	Certificate Bundle			Aug 13, 2018 - Aug 13, 2018	Common
default	RSA Certificate	localhost.localdomain	MyCompany	May 11, 2023	Common
f5-irule	RSA Certificate	support.f5.com	F5 Networks	Aug 13, 2031	Common

5.5.4. Client SSL Profile の生成と VS への割当て

(1) Client SSL Profile の生成

「Main」メニュー → 「Local Traffic」 → 「Profile」 → 「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。以下のように設定します。

General Properties

Name: NetAccess-001-Client-SSL

Parent Profile: clientssl

Configuration: Basic

Certificate: NetAccess-001_cert

Key: NetAccess-001_cert

Enabled Options

Don't insert empty fragments

Options List

Available Options

NetScape® reuse cipher change bug workaround

Microsoft® big SSLV3 buffer

Microsoft® IE SSLV2 RSA padding

SSLv3 080 client DH bug workaround

TLS DS bug workaround

Proxy SSL

SSL Forward Proxy: Basic

SSL Forward Proxy Feature

CA Certificate: Select...

CA Key: Select...

Certificate Lifespan: 30 day(s)

Enabled Extensions

Basic Constraints

Subject Alternative Name

Certificate Extensions List

Available extensions

Authority Key Identifier

Certificate Policies

CRL Distribution Points

Extended Key Usage

Fresh CRL (a.k.a. Delta CRL Distribution Point)

Cache Certificate by Addr-Port

Client Authentication

Client Certificate: ignore

Frequency: once

Retain Certificate: Enabled

Certificate Chain Traversal Depth: 0

Trusted Certificate Authorities: None

Advertised Certificate Authorities: None

Certificate Revocation List (CRL): None

Cancel Repeat Finished

名前(任意)を指定。

右のチェックボックスをチェック。→
← 左のプルダウンメニューから証明書とキーを選択。

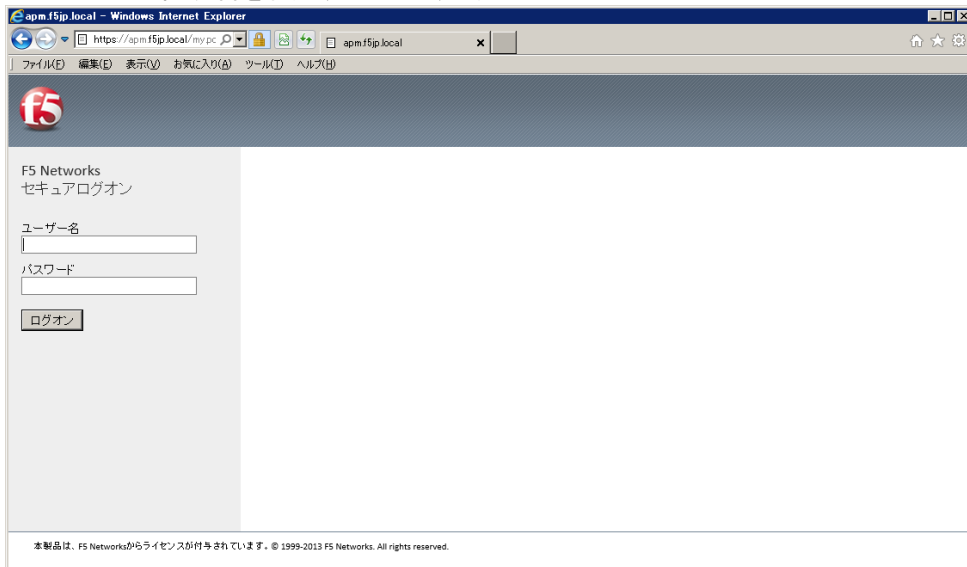
(2) Virtual Server への Client SSL Profile の割当て

「Main」メニュー → 「Local Traffic」 → 「Virtual Servers」 を選択し、APM 用に設定した Virtual Server をクリックすると、以下の画面が表示されます。

The screenshot displays the configuration interface for a Virtual Server. The left sidebar contains navigation menus for Statistics, iApp, Wizards, Local Traffic, Acceleration, Access Policy, Device Management, Network, and System. The main content area is titled 'Local Traffic >> Virtual Servers: Virtual Server List >> NetAccess-001_vs' and shows the 'Properties' tab. The 'General Properties' section includes fields for Name, Partition/Path, Description, Type, Source, Destination, Service Port, Availability, and State. The 'Configuration: Basic' section contains settings for Protocol, HTTP Profile, FTP Profile, RTSP Profile, SSL Profile (Client), SSL Profile (Server), VLAN and Tunnel Traffic, and Source Address Translation. The 'Content Rewrite' section includes Rewrite Profile and HTML Profile. The 'Access Policy' section includes Access Profile, Connectivity Profile, MAM ID Bridge, VDI & Java Support, and OAM Support. The 'Acceleration' section includes Rate Class, OneConnect Profile, NTLM Conn Pool, HTTP Compression Profile, Web Acceleration Profile, and SPDY Profile. A red box highlights the 'SSL Profile (Client)' section, showing a list of profiles with 'NetAccess-001-Client-SSL' selected. A red text box next to it says '作成した Client SSL Profile を選択。'

5.5.4.1. クライアント PC からのアクセス

正式なサーバ証明書を利用することで、クライアント PC から Virtual Server へのアクセス時に、警告が出なくなります。



初級編は以上で終了です。

ここまでで、ご要件を満たす設定になっていれば、「[冗長化](#)」へ進んでください。

6. 中級編

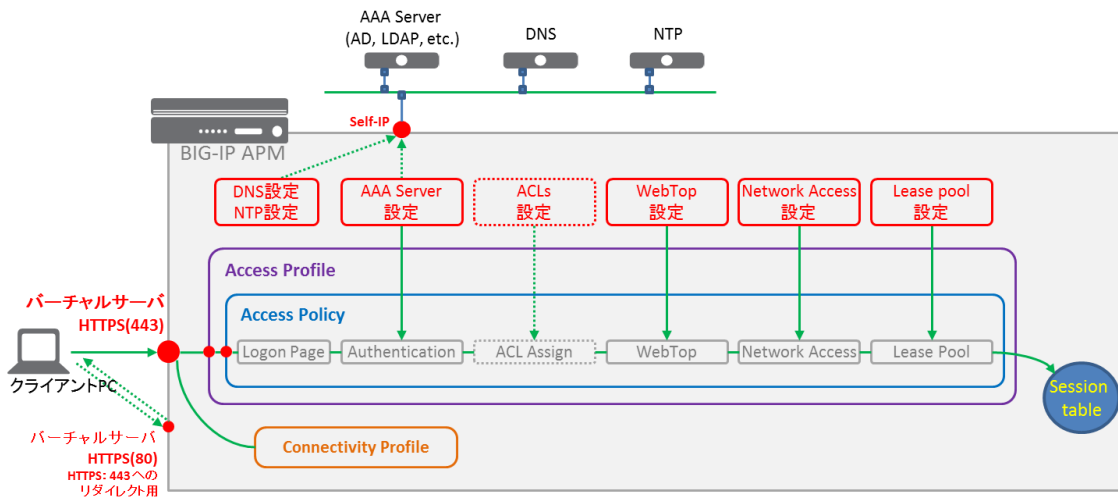
6.1. APM オブジェクトを一つ一つ設定していく方法

ウィザードを利用せず、一つ一つオブジェクトを設定していき、ウィザード設定と同等の状態にする方法を示します。

6.1.1. 設定が必要な APM オブジェクトたち

APM のバーチャルサーバにアクセスしてから、ネットワークアクセス(SSL-VPNトンネル)を確立するまでには、下図に示すような、様々なオブジェクトを経由します。

このことで、BIG-IP APM に設定したポリシーが適用された、ネットワークアクセスセッションが生成されます。



設定が必要な各オブジェクトの概要を以下に記載します。

- (1) DNS/NTP 設定
BIG-IP 自身が問合せを行うサーバ設定です。
- (2) AAA Server 設定
Active Directory 認証に必要な設定を行います。
- (3) ACL 設定
パケットフィルタリング設定です。このセクションでは設定しませんが、後の「VPE サンプル」で設定します。
- (4) WebTop 設定
BIG-IP APM へのアクセス後に稼働する Web アプリケーションです。
- (5) Network Access 設定
SSL-VPNトンネルを行うための設定です。
- (6) Lease Pool 設定
クライアント PPP アダプタに割当てられるアドレス群です。
- (7) Access Policy
上記のオブジェクトをフローチャート形式で紐づける設定です。
- (8) Access Profile
Access Policy の親的位置づけです。利用する言語をここで設定します。
- (9) Connectivity Profile
コネクション上の圧縮設定やクライアント用ソフトウェアの設定を行います。

以降、上記の各オブジェクトを設定していきます。
尚、既述の「[ネットワーク設定](#)」は完了しているものとして進めます。

6.1.2. 各オブジェクトの設定

6.1.2.1. DNS / NTP 設定

(1) DNS を設定します。

「Main」メニュー → 「System」 → 「Configuration」 → 「Device」タブから「DNS」を選択します。

Hostname: big208 fsp.local Date: Nov 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 5:56 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

System >> Configuration : Device : DNS

Device Local Traffic AWS

Properties

DNS Lookup Server List

Address: 10.99.2.218
Add
10.99.2.218

Edit Delete Up Down

Address:
Add

Address:
Add

DNS Search Domain List

localhost

Edit Delete Up Down

DNS Cache

IP Version IPV4

Update

DNS の IP アドレスを入力し、「Add」ボタンを押す。

(2) NTP を設定します。

「Device」タブから「NTP」を選択します。

Hostname: big208 fsp.local Date: Nov 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 5:56 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About

System >> Configuration : Device : NTP

Device Local Traffic AWS

Properties

Time Server List

Address: 10.99.2.201
Add
10.99.2.201

Edit Delete

Update

NTP の IP アドレスを入力し、「Add」ボタンを押す。

6.1.2.2. 認証サーバ: Active Directory の設定

「Main」メニュー → 「Access Policy」 → 「AAA Servers」へ移動し、「AAA Server by Type」タブから、「Active Directory」を選択します。

The screenshot shows the NetAccess configuration interface. The top status bar displays: Hostname: big208.f5.jp.local, Date: Dec 6, 2013, User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation bar includes Main, Help, About, and a breadcrumb trail: Access Policy » AAA Servers » New Server... The left sidebar contains various system management categories like Statistics, iApp, Wizards, Local Traffic, Acceleration, Access Policy, Secure Connectivity, Network Access, Application Access, Portal Access, Manage Sessions, Reports, Customization, Dashboard, MAM, Device Management, Network, and System. The main content area is titled 'General Properties' and 'Configuration'. The 'General Properties' section has a 'Name' field containing 'NetAccess-001_aaa_srv' and a 'Type' dropdown set to 'Active Directory'. The 'Configuration' section includes: 'Domain Name' (corp.f5.jp.local), 'Server Connection' (radio buttons for 'Use Pool' and 'Direct', with 'Direct' selected), 'Domain Controller' (10.99.2.218), 'Admin Name', 'Admin Password', 'Verify Admin Password', 'Kerberos Preauthentication Encryption Type' (None), and 'Timeout' (15 seconds). Red boxes highlight the 'Name' field and the 'Domain Name' and 'Server Connection' fields. Red text annotations provide instructions: '任意の名称を入力。' (Enter an arbitrary name.) for the Name field, and 'ドメイン名を入力。Server Connection は"Direct"を選択し、Active Directory の IP アドレスを入力。' (Enter domain name. Select "Direct" for Server Connection and enter the IP address of Active Directory.) for the Domain Name and Server Connection fields.

Field	Value	Annotation
Name	NetAccess-001_aaa_srv	任意の名称を入力。
Type	Active Directory	
Domain Name	corp.f5.jp.local	ドメイン名を入力。
Server Connection	Direct	Server Connection は"Direct"を選択し、Active Directory の IP アドレスを入力。
Domain Controller	10.99.2.218	Active Directory の IP アドレスを入力。
Admin Name		
Admin Password		
Verify Admin Password		
Kerberos Preauthentication Encryption Type	None	
Timeout	15 seconds	

6.1.2.3. Lease Pool の設定

クライアントに割当てする IP アドレス群:リースプールを設定します。

「Main」メニュー → 「Access Policy」 → 「Network Access」へ移動します。

「Lease Pool List」タブから「IPv4 Lease Pools」を選択します。

Hostname: big308-f5.jp.local Date: Dec 6, 2013 User: admin
IP Address: 172.28.15.208 Time: 4:35 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Access Policy >> Network Access : Lease Pools : IPv4 Lease Pools >> New IPv4 Lease Pool...

Statistics
iApp
Wizards
Local Traffic
Acceleration
Access Policy
 Access Profiles >
 AAA Servers >
 ACLs >
 SSO Configurations >
 SAML >
 Local User DB >
 Webtops >
 Hosted Content >
 Secure Connectivity >
 Network Access >
 Application Access >
 Portal Access >
 Manage Sessions >
 Reports >
 Customization >
 Dashboard >
 MAM >
Device Management
Network
System

General Properties

Name: NetAccess-001_ip 任意の名称を入力。

Configuration

Type: IP Address IP Address Range

Start IP Address: 10.99.99.11 割当てする IP アドレス範囲の最初のアドレス(Start IP Address)と、最後のアドレス(End IP Address)を入力し、「Add」ボタンを押す。

End IP Address: 10.99.99.20

Add

10.99.99.11 - 10.99.99.20

Edit Delete

Cancel Repeat Finished

6.1.2.4. Network Access の設定

- (1) 「Main」メニュー → 「Access Policy」 → 「Network Access」へ移動します。
「Network Access List」タブを選択し、左に表示された「Create」ボタンを押すと、以下の画面が出ます。
以下のように、値を入力し、「Finished」ボタンを押します。

Hostname: big208 fsjp.local | Date: Nov 14, 2013 | User: admin | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)
Standalone

Main Help About | Access Policy >> Network Access : Network Access List >> New Resource...

General Properties

Name	NetAccess-001_na_res
Description	
Auto launch	<input type="checkbox"/> Enable

Customization Settings for English

Language	English
Caption	NetAccess-001_na_res
Detailed Description	
Image	<input type="text"/> 参照 ViewHide Restore Default

Cancel Finished

- (2) その後、以下のような画面(タブメニューが追加された画面)に遷移します。

Hostname: big208 fsjp.local | Date: Nov 14, 2013 | User: admin | Role: Administrator | Partition: Common | Log out

ONLINE (ACTIVE)
Standalone

Main Help About | Access Policy >> Network Access : Network Access List >> NetAccess-001_na_res

Properties Network Settings Optimization DNS/Hosts Drive Mappings Launch Applications

General Properties

Name	NetAccess-001_na_res
Partition / Path	Common
Description	
Auto launch	<input type="checkbox"/> Enable

Customization Settings for English

Language	English
Caption	NetAccess-001_na_res
Detailed Description	
Image	<input type="text"/> 参照 ViewHide Restore Default

Update Delete

(3) Network Settings タブでの設定。

ここで、既に設定した Lease Pool を選択します。スプリット・トンネルの設定もここで行います。

設定した Lease Pool を選択。

Use split tunneling for traffic を選択。
トンネルに通じたいネットワーク帯を設定し、「Add」ボタンを押す。

(4) クライアントに割り当てる DNS や hosts の設定。

クライアントに割り当てる DNS。

クライアントに割り当てる DNS ドメインサフィックス。

6.1.2.5. Webtop の設定

「Main」メニュー → 「Access Policy」 → 「Webtops」を選択します。
右上に表示された「Create」ボタンを押すと、以下の画面が現れます。
以下の 2 ヶ所を設定し、「Finished」ボタンを押します。

The screenshot shows the Fortinet FortiGate Webtop configuration page. The breadcrumb navigation is 'Access Policy > Webtops > New Webtop...'. The left sidebar shows the 'Access Policy' menu with 'Webtops' selected. The main content area is titled 'General Properties' and contains the following fields:

- Name:** NetAccess-001_webtop
- Type:** Network Access
- Configuration:** Minimize To Tray Enabled

Buttons at the bottom include 'Cancel', 'Repeat', and 'Finished'. Two red boxes highlight the 'Name' and 'Type' fields with the following annotations:

- 任意の名称を入力。
- 「Network Access」を選択。

6.1.2.6. Connectivity Profile の設定

「Main」メニュー → 「Access Policy」 → 「Secure Connectivity」で以下の画面が現れます。
右上に表示される「Add」ボタンを押すと、以下の画面が現れます。
以下 2ヶ所を設定し、「OK」ボタンを押します。

The screenshot shows the Fortinet FortiGate web interface. The main menu is 'Access Policy > Secure Connectivity'. A 'Create New Connectivity Profile' dialog box is open. The dialog has a tree view on the left with categories like 'General Settings', 'Compression Settings', 'Network Access', etc. The right side of the dialog has input fields for 'Profile Name' (containing 'NetAccess-001_cp'), 'Parent Profile' (a dropdown menu showing '/Common/connectivity'), 'FEC Profile (Not Licensed)', 'Description', and 'Partition' (set to 'Common'). At the bottom are 'OK' and 'Cancel' buttons. Two red boxes with Japanese text point to the 'Profile Name' and 'Parent Profile' fields. The 'OK' button is also highlighted with a red box.

6.1.2.7. Access Profile と Access Policy の設定

- (1) 「Main」メニュー → 「Access Policy」 → 「Access Profile」 → 「Access Profile List」を選択。
右上に表示された「Create」ボタンを押すと、以下の画面が現れます。
以下 2ヶ所を設定し、「Finished」ボタンを押します。

The screenshot shows the configuration page for a new Access Profile. The breadcrumb navigation is "Access Policy > Access Profiles: Access Profiles List > New Profile...".

General Properties

- Name: (Red box highlights this field with the text "任意の名称を入力。")
- Parent Profile: access

Settings

- Inactivity Timeout: 900 seconds
- Access Policy Timeout: 300 seconds
- Maximum Session Timeout: 0 seconds
- Minimum Authentication Failure Delay: 2 seconds
- Maximum Authentication Failure Delay: 5 seconds
- Max Concurrent Users: 0
- Max Sessions Per User: 0
- Max In Progress Sessions Per Client IP: 0
- Restrict to Single Client IP:

Configurations

- URI:
- Logout URI Include:
- Logout URI Timeout: 5 seconds
- Microsoft Exchange: None

SSO Across Authentication Domains (Single Domain mode)

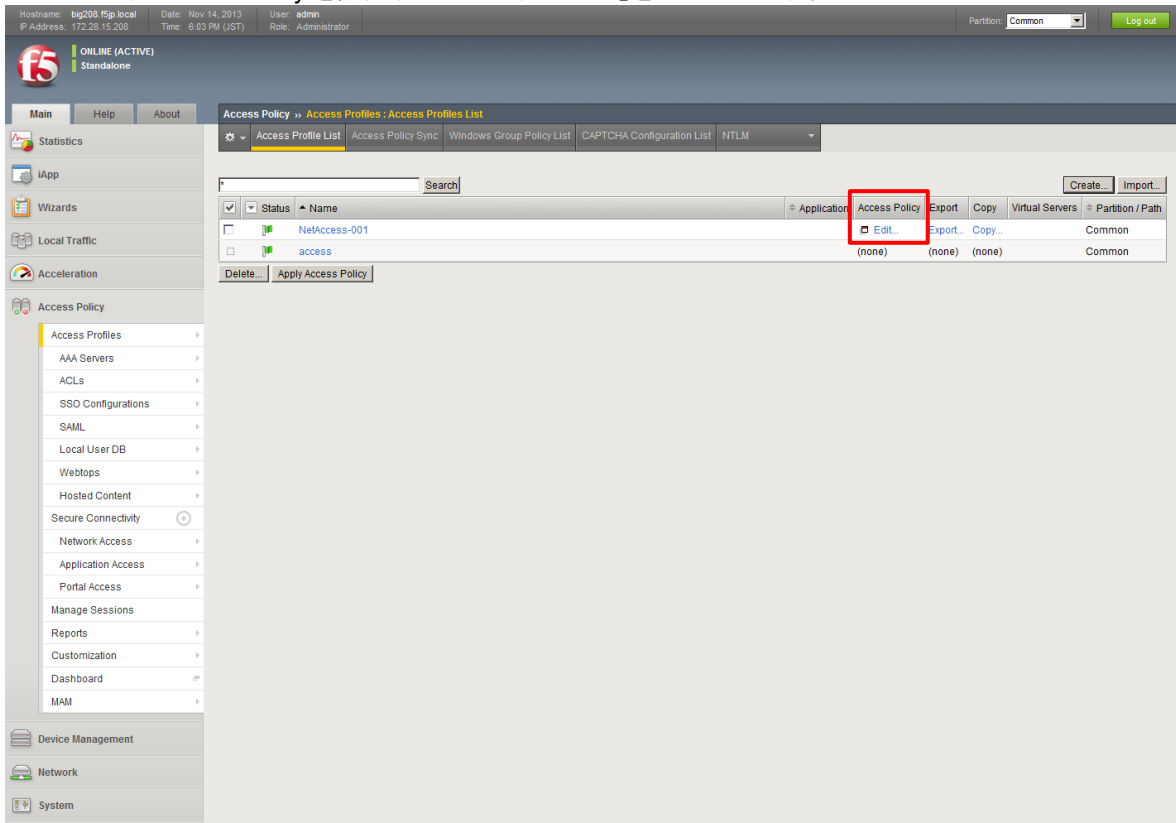
- Domain Cookie:
- Cookie Options: Secure, Persistent, HTTP Only
- SSO Configuration: None

Language Settings

- Additional Languages: Afaar (aa) (Add)
- Languages: (Red box highlights this section with the text "言語を選択。")
- Accepted Languages: Japanese (ja)
- Factory Built-in Languages: English (en), Chinese (Simplified) (zh-cn), Chinese (Traditional) (zh-tw), Korean (ko), Spanish (es), French (fr), German (de)
- Default Language: Japanese (ja)

Buttons: Cancel, Finished

- (2) その後、以下の画面に遷移します。
 ここで、Access Policy を設定するために、「Edit...」をクリックします。



- (3) 以下のような証明書に関わる警告画面が表示されますが、「このサイトの閲覧を続行する」を選択してください。

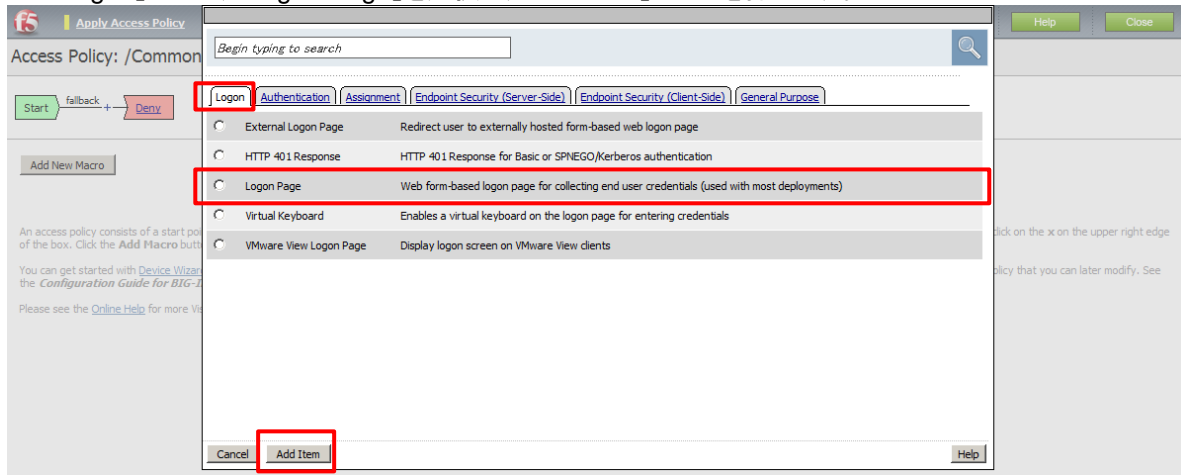


- (4) 以下の画面: Visual Policy Editor (VPE) が表示されます。
 "Start"と"Deny"の線上にある、「+」をクリックします。



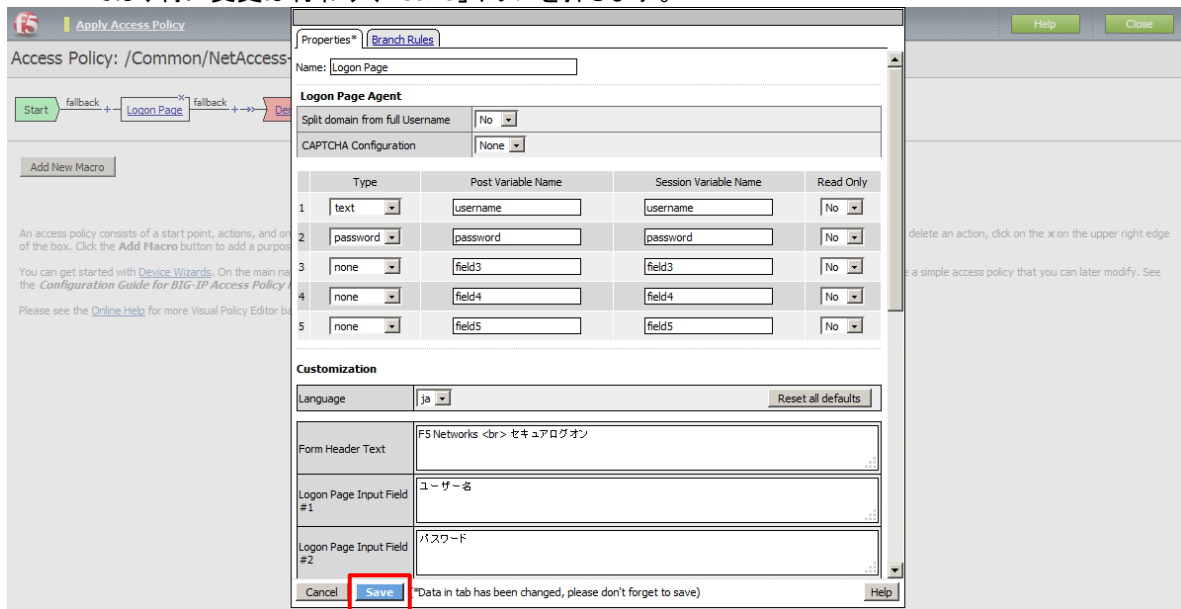
(5) その後、以下の画面が現れます。

「Logon」タブで、「Logon Page」を選択し、「Add Item」ボタンを押します。



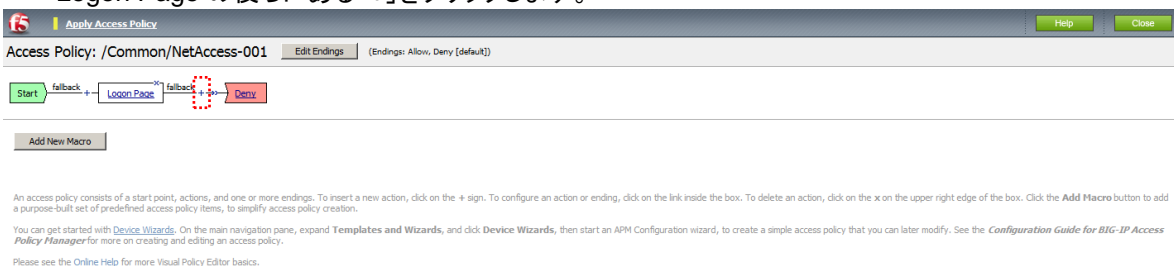
(6) その後、以下の画面が現れます。

ここでは、特に変更は行わず、「save」ボタンを押します。



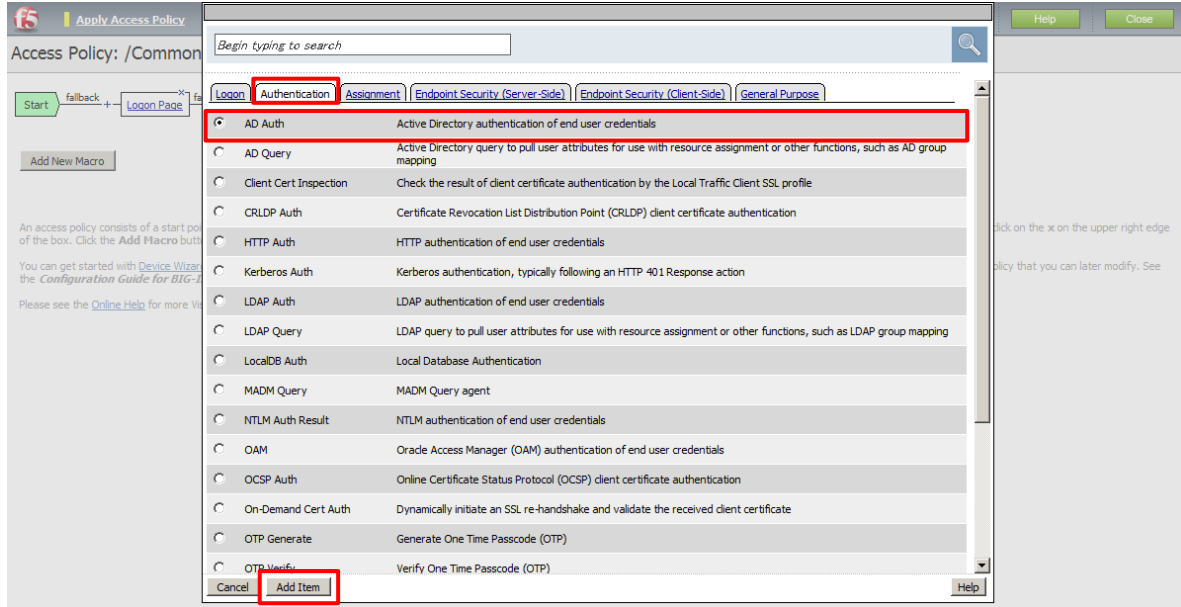
(7) 以下のような状態になります。

Logon Page の後ろにある「+」をクリックします。



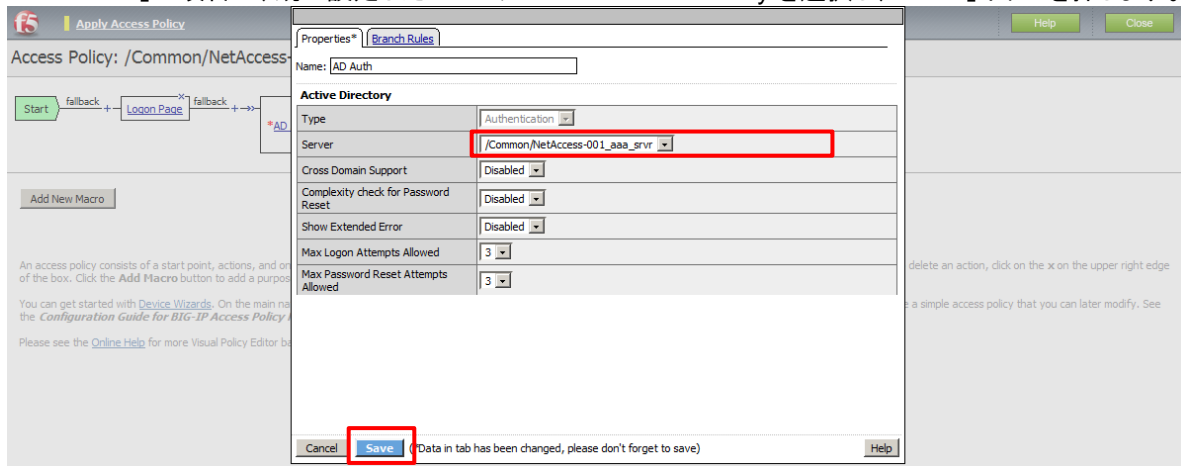
(8) その後、以下の画面が現れます。

「Authentication」タブで、「AD Auth」を選択し、「Add Item」ボタンを押します。



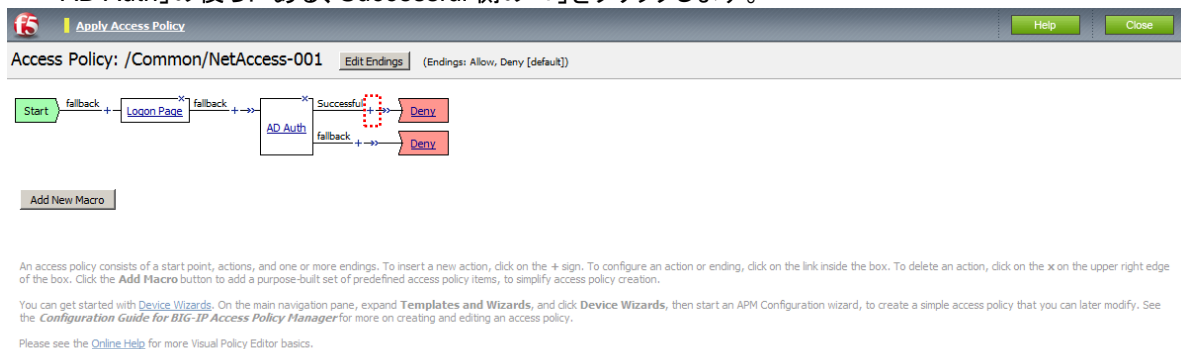
(9) その後、以下の画面が現れます。

「Server」の項目で、既に設定した AAA サーバ: Active Directory を選択し、「Save」ボタンを押します。



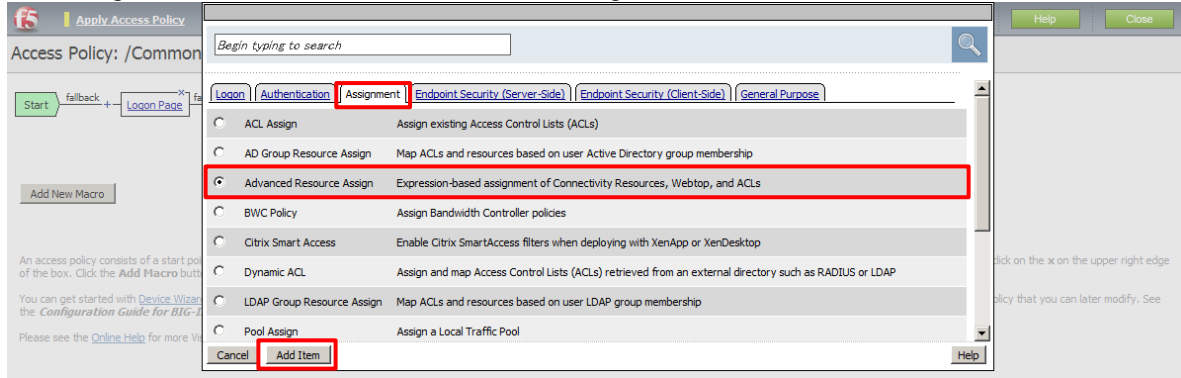
(10) 以下のような状態になります。

「AD Auth」の後ろにある、Successful 側の「+」をクリックします。



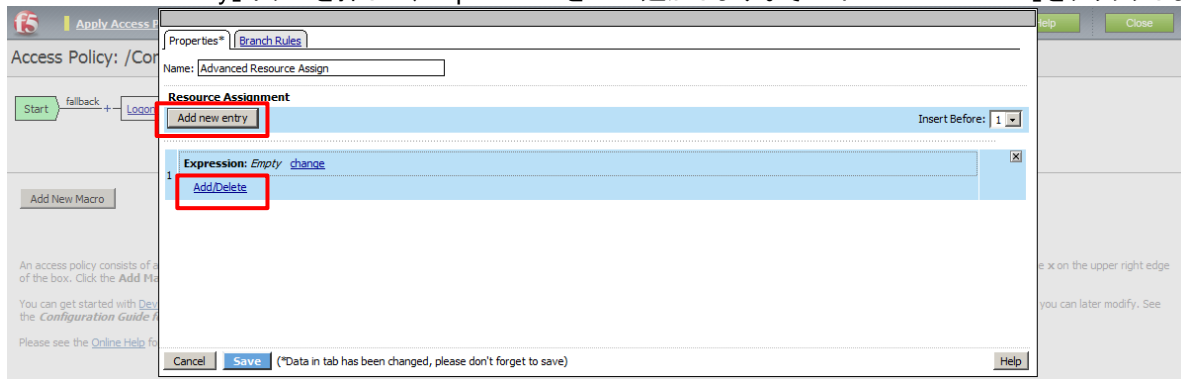
(11)その後、以下の画面が現れます。

「Assignment」タブで、「Advanced Resource Assign」を選択し、「Add Item」ボタンを押します。



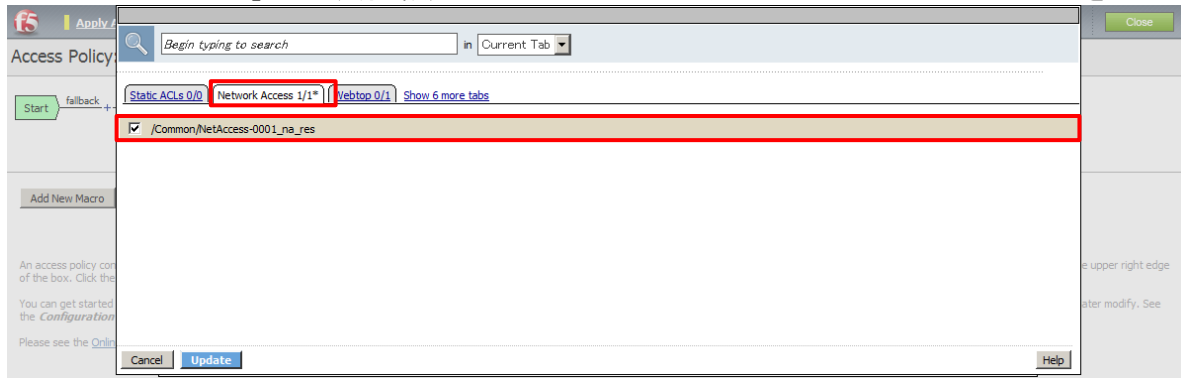
(12)その後、以下の画面が現れます。

「Add new entry」ボタンを押して、Expression を 1 つ追加します。その下の「Add/Delete」をクリックします。



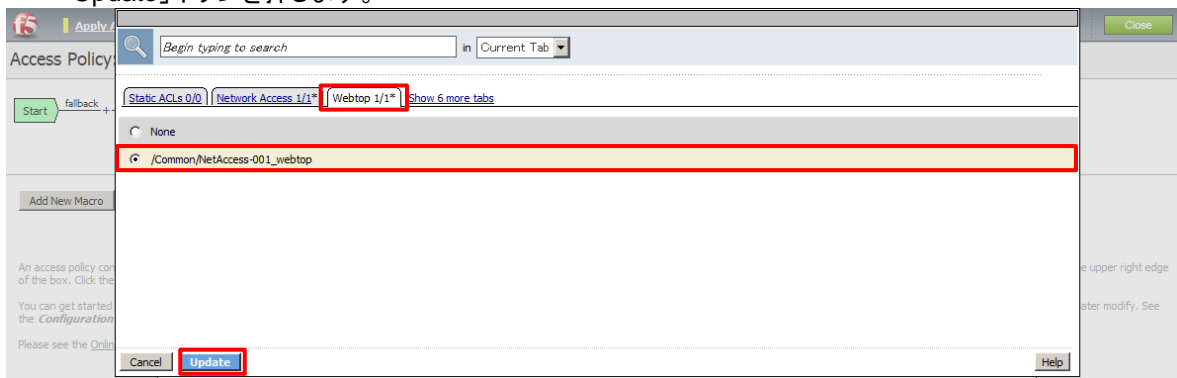
(13)その後、以下の画面が現れます。

「Network Access」タブで、既に設定した Network Access リソースのチェックボタンにチェックを入れます。

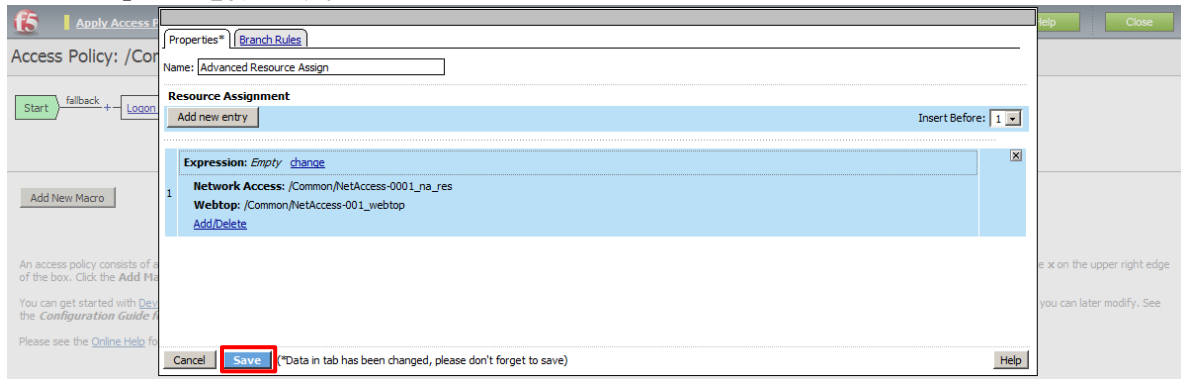


(14)「Webtop」タブで、既に設定した Network Access 用 Webtop のチェックボタンにチェックを入れます。

「Update」ボタンを押します。

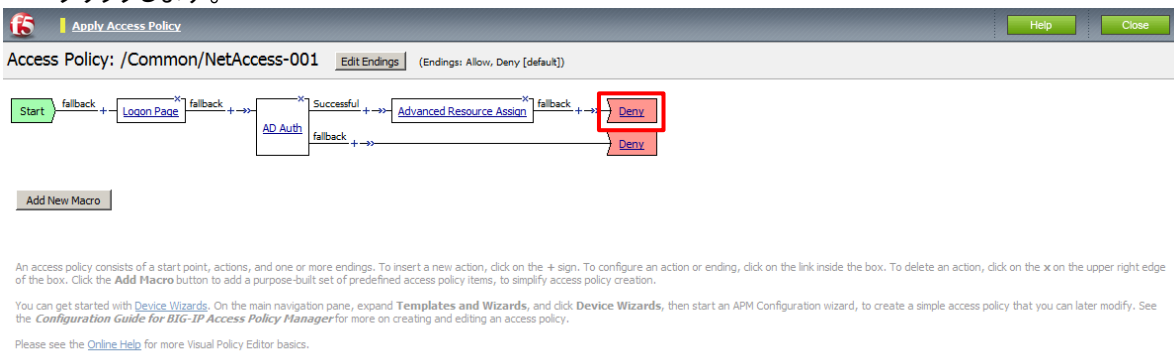


(15)その後、以下のような状態になります。
「Save」ボタンを押します。

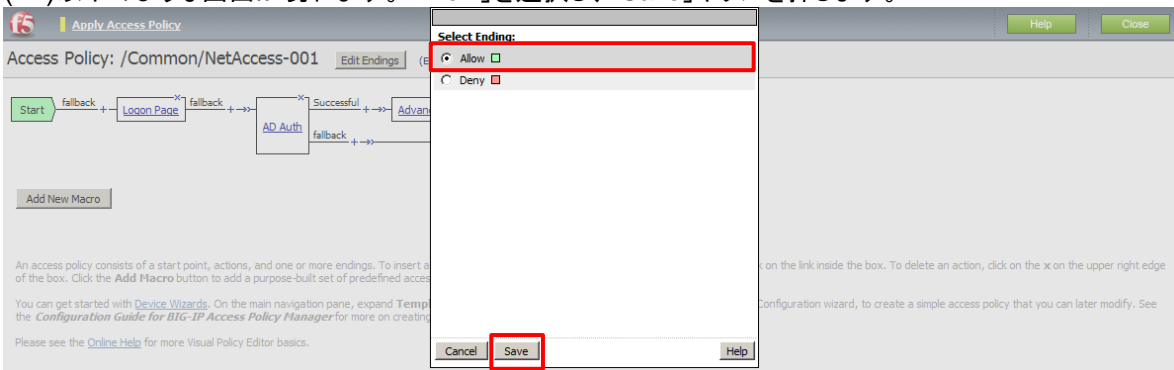


(16)以下のような状態になります。

最後に「Advance Resource Assign」の後ろにある「Deny」を「Allow」に変更する必要がありますので、その「Deny」をクリックします。

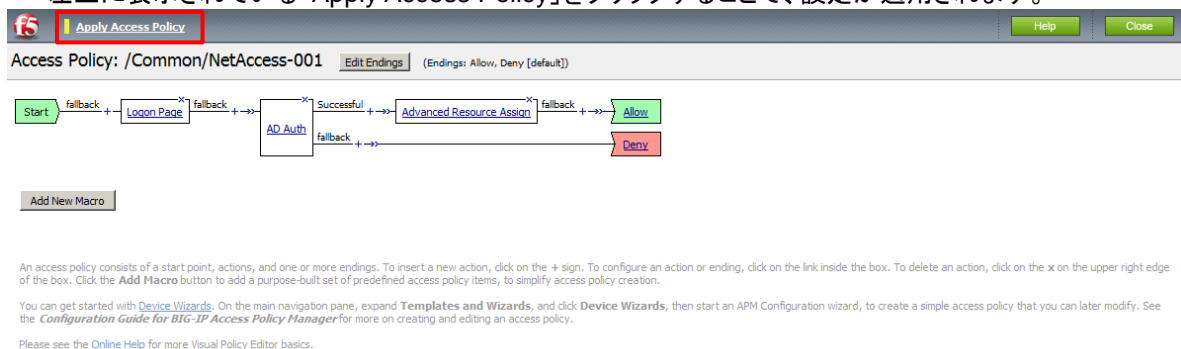


(17)以下のような画面が現れます。「Allow」を選択し、「Save」ボタンを押します。



(18)VPE の設定は以上ですが、まだ設定した値は適用されていません。

左上に表示されている「Apply Access Policy」をクリックすることで、設定が適用されます。



6.1.2.8. APM 用 Virtual Server の設定

「Main」メニュー → 「Local Traffic」 → 「Virtual Servers」 を選択します。
右上の「Create」ボタンを押すと、以下の画面が現れます。 以下のように設定します。

Hostname: big208.f5p.local Date: Dec 6, 2013 User: admin
IP Address: 172.28.15.208 Time: 5:06 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

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

Statistics
iApp
Wizards
Local Traffic
 Network Map
 Virtual Servers
 Policies
 Profiles
 iRules
 Pools
 Nodes
 Monitors
 Traffic Class
 Address Translation
 DNS Express Zones
 DNS Caches
Acceleration
 Access Policy
 Device Management
 Network
 System

General Properties

Name: NetAccess-001_vs *任意の名称を入力。*

Description:
Type: Standard
Source:
Destination: Type: Host Network Address: 10.99.1.101 *Type で Host を選択。 VS の IP アドレスを入力し、サービスポート(443)を選択。*

Service Port: 443 HTTPS
State: Enabled

Configuration: Basic

Protocol: TCP *HTTP Profile を選択。*

HTTP Profile: http
FTP Profile: None
RTSP Profile: None

SSL Profile (Client): Selected: /Common/clientsssl Available: /Common/clientsssl-insecure-compatible, wom-default-clientsssl *clientsssl を選択。*

SSL Profile (Server): Selected: Available: /Common/apm-default-serverssl, serverssl, serverssl-insecure-compatible, wom-default-serverssl

VLAN and Tunnel Traffic: All VLANs and Tunnels
Source Address Translation: None

Content Rewrite

Rewrite Profile: None
HTML Profile: None

Access Policy

Access Profile: NetAccess-001 *設定した Access Profile と Connectivity Profile を選択。*

Connectivity Profile: NetAccess-001_cp
MAM ID Bridge: Enabled
VDI & Java Support: Enabled
OAM Support: Enabled

Acceleration

Rate Class: None
OneConnect Profile: None
NTLM Conn Pool: None
HTTP Compression Profile: None
Web Acceleration Profile: None
SPDY Profile: None

Resources

iRules: Enabled Available: /Common/_sys_APM_ExchangeSupport_OA_BasicAuth, _sys_APM_ExchangeSupport_OA_NtmAuth, _sys_APM_ExchangeSupport_helper, _sys_APM_ExchangeSupport_main

Policies: Enabled Available: /Common/_sys_CEC_video_policy

Default Pool: None
Default Persistence Profile: None
Fallback Persistence Profile: None

Cancel Repeat **Finished**

6.1.2.9. リダイレクト用 Virtual Server の設定

HTTP(80)でアクセスしても、APM 用 Virtual Server(HTTPS(443))へリダイレクトされるように、リダイレクト用の Virtual Server を新規に設定します。

Hostname: big208 f5jp.local Date: Dec 6, 2013 User: admin
IP Address: 172.28.15.208 Time: 5:11 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Local Traffic >> Virtual Servers > Virtual Server List >> New Virtual Server...

General Properties

Name: NetAccess-001_vs_redirect (任意の名称を入力。)

Description: [Empty]

Type: Standard

Source: [Empty]

Destination: Type: Host Network Address: 10.99.1.101 (Type で Host を選択。 VS の IP アドレスを入力し、サービスポート(80)を選択。)

Service Port: 80 HTTP (サービスポート(80)を選択。)

State: Enabled

Configuration: Basic

Protocol: TCP

HTTP Profile: http (HTTP Profile を選択。)

FTP Profile: None

RTSP Profile: None

SSL Profile (Client): [Empty]

SSL Profile (Server): [Empty]

VLAN and Tunnel Traffic: All VLANs and Tunnels

Source Address Translation: None

Content Rewrite

Rewrite Profile: None

HTML Profile: None

Access Policy

Access Profile: None

Connectivity Profile: None

MAM ID Bridge: [Empty]

VDI & Java Support: [] Enabled

OAM Support: [] Enabled

Acceleration

Rate Class: None

OneConnect Profile: None

NTLM Conn Pool: None

HTTP Compression Profile: None

Web Acceleration Profile: None

SPDY Profile: None

Resources

iRules: _sys_https_redirect (デフォルトで用意されている iRule: _sys_https_redirect を選択。)

Policies: [Empty]

Default Pool: None

Default Persistence Profile: None

Fallback Persistence Profile: None

Cancel Repeat Finished

以上で、ウィザードで設定した内容と同等の状態になります。

6.1.2.10. クライアント PC からのアクセス

クライアント PC から、設定した Virtual Server へのアクセスが完了することを確認します。



6.1.3. SSL サーバ証明書の設定

初級編での設定と同様です。

既述の「[SSL サーバ証明書の設定](#)」を参照してください。

6.2. クライアント証明書認証の設定

クライアント証明書による認証を行う設定方法を記載します。

6.2.1. クライアント証明書の発行

クライアント証明書認証の設定を行うためには、以下 2 つの証明書が必要です。

- ① 認証局の証明書
BIG-IP 側で利用します。
- ② クライアント証明書
クライアント PC 側で利用します。

クライアント証明書の発行には、大きくは以下 2 つの方法があります。

- a) 商用の認証局(Verisign、CyberTrust 等)から発行してもらう
- b) 独自の認証局(例: OpenSSL の利用)を建てて、発行する

本ガイドでは、b)の方法: OpenSSL を使って独自の認証局を建てて、クライアント証明書を発行しました。

クライアント証明書を発行する際、PKCS#12 形式で発行することで、キーと証明書を一つのファイルとしてクライアントに提供することが可能です。

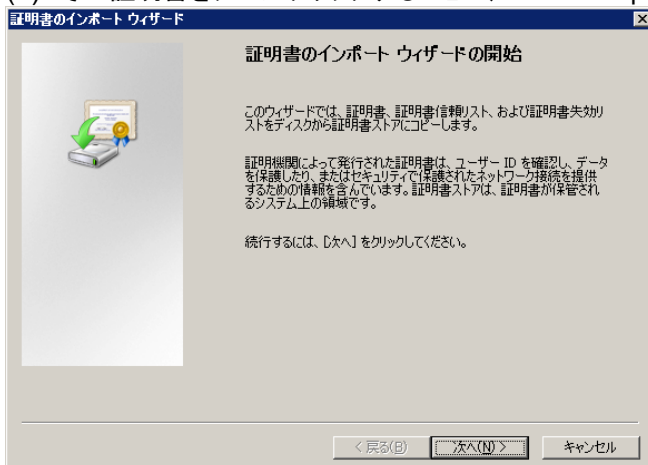
本例では、PKCS#12 形式で、「apmclient001.p12」というファイル名のクライアント証明書を発行しました。

6.2.2. クライアント PC へクライアント証明書をインポート

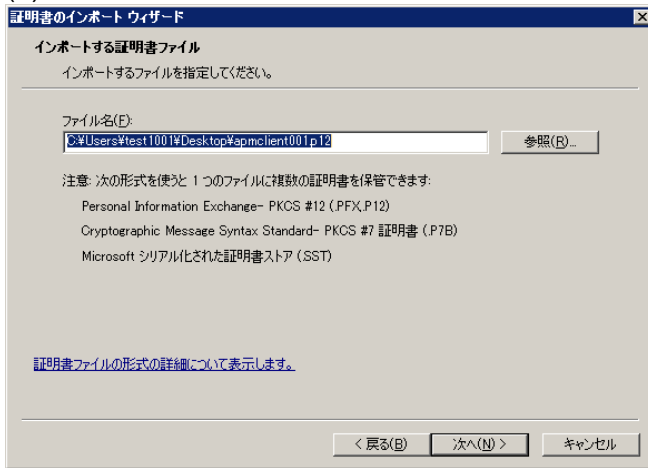
クライアント証明書(PKCS#12)を、クライアント PC へインストールする手順について、参考までに記載します。
本ガイドのクライアント PC は、Windows7 + Internet Explorer 10 を利用しています。

(1) クライアント証明書:「apmclient001.p12」を Windows へコピーします。

(2) その証明書をダブルクリックすることで、Internet Explorer へのインポートが開始されます。



(3) そのまま「次へ」を押します。



証明書のインポート ウィザード

インポートする証明書ファイル
インポートするファイルを指定してください。

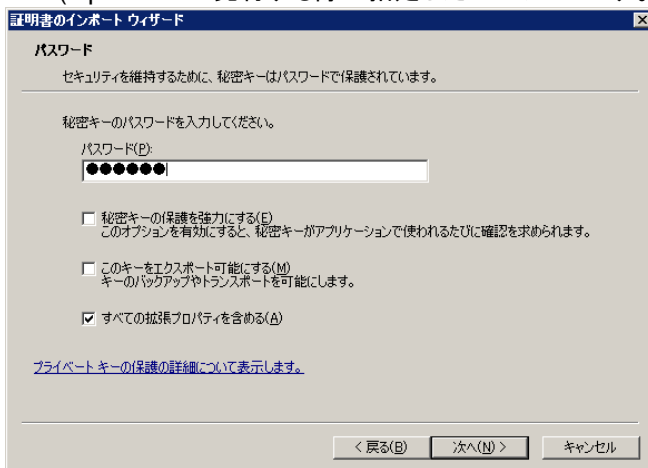
ファイル名(F):
C:\Users\Test11001\Desktop\apmclient001.p12 参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:
Personal Information Exchange- PKCS #12 (PFX,P12)
Cryptographic Message Syntax Standard- PKCS #7 証明書 (P7B)
Microsoft シリアル化された証明書ストア (SST)

[証明書ファイルの形式の詳細について表示します。](#)

< 戻る(B) 次へ(N) > キャンセル

(4) 秘密キーがパスワードで保護されているので、パスワードを入力します。
(OpenSSL で発行する際に指定したパスワードです。)



証明書のインポート ウィザード

パスワード
セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):
●●●●●●

秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

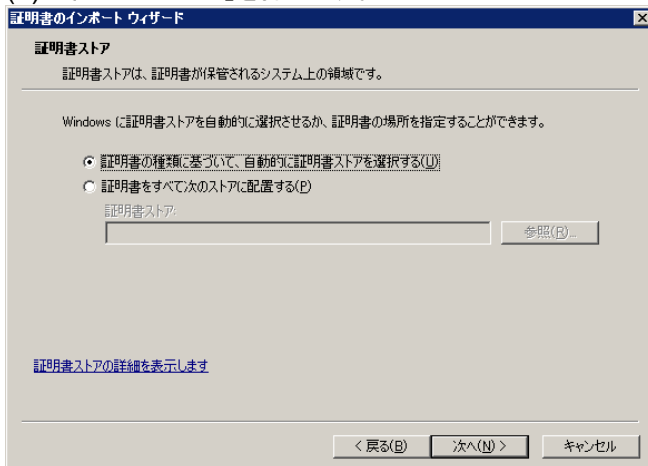
このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

すべての拡張プロパティを含める(A)

[プライベートキーの保護の詳細について表示します。](#)

< 戻る(B) 次へ(N) > キャンセル

(5) そのまま「次へ」を押します。



証明書のインポート ウィザード

証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

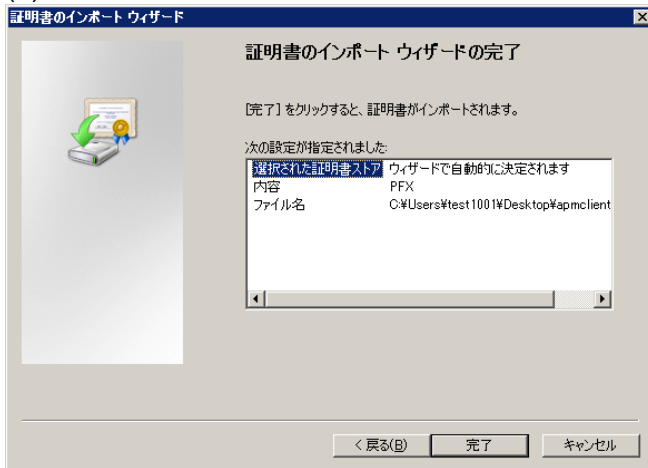
証明書の種類に基づいて、自動的に証明書ストアを選択する(O)
 証明書をすべて次のストアに配置する(P)

証明書ストア:
参照(R)...

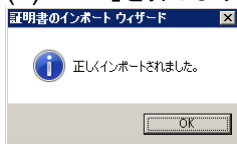
[証明書ストアの詳細を表示します](#)

< 戻る(B) 次へ(N) > キャンセル

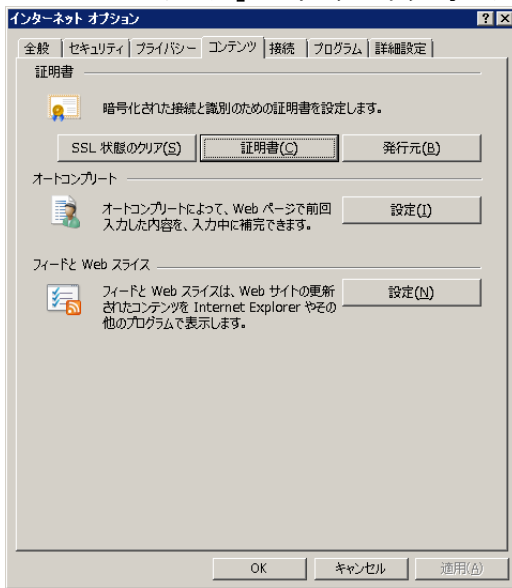
(6) 「完了」を押します。



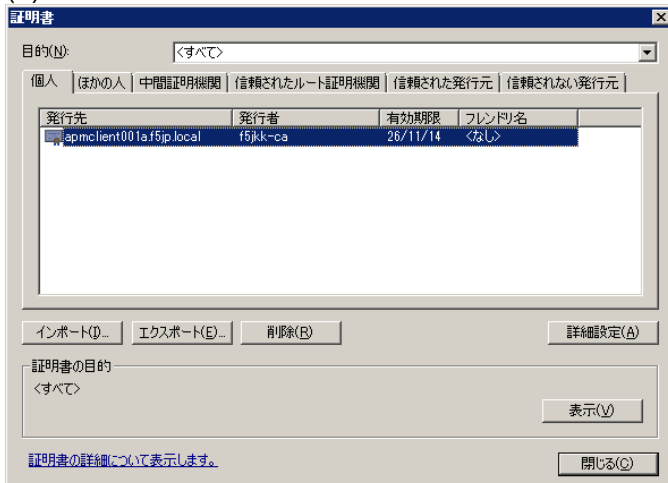
(7) 「OK」を押します。



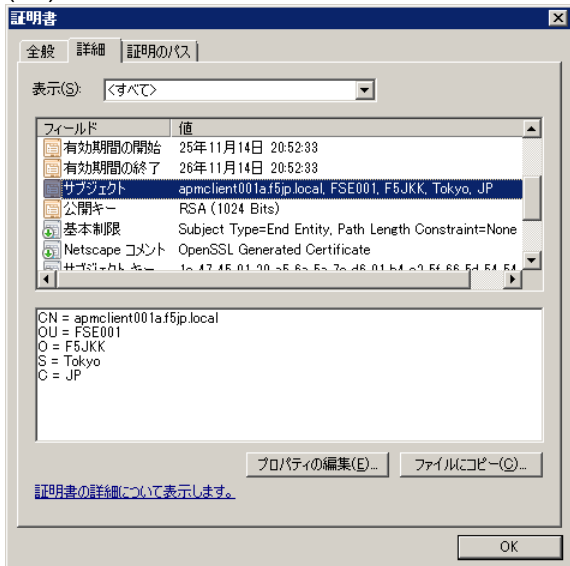
(8) 証明書がインストールされた状態を確認するには、IE10の「ツール」→「インターネットオプション」→「証明書」ボタンを押します。



(9) 「個人」タブで、クライアント証明書がインストールされていることを確認できます。



(10)クライアント証明書をダブルクリックすると、証明書の詳細が確認できます。



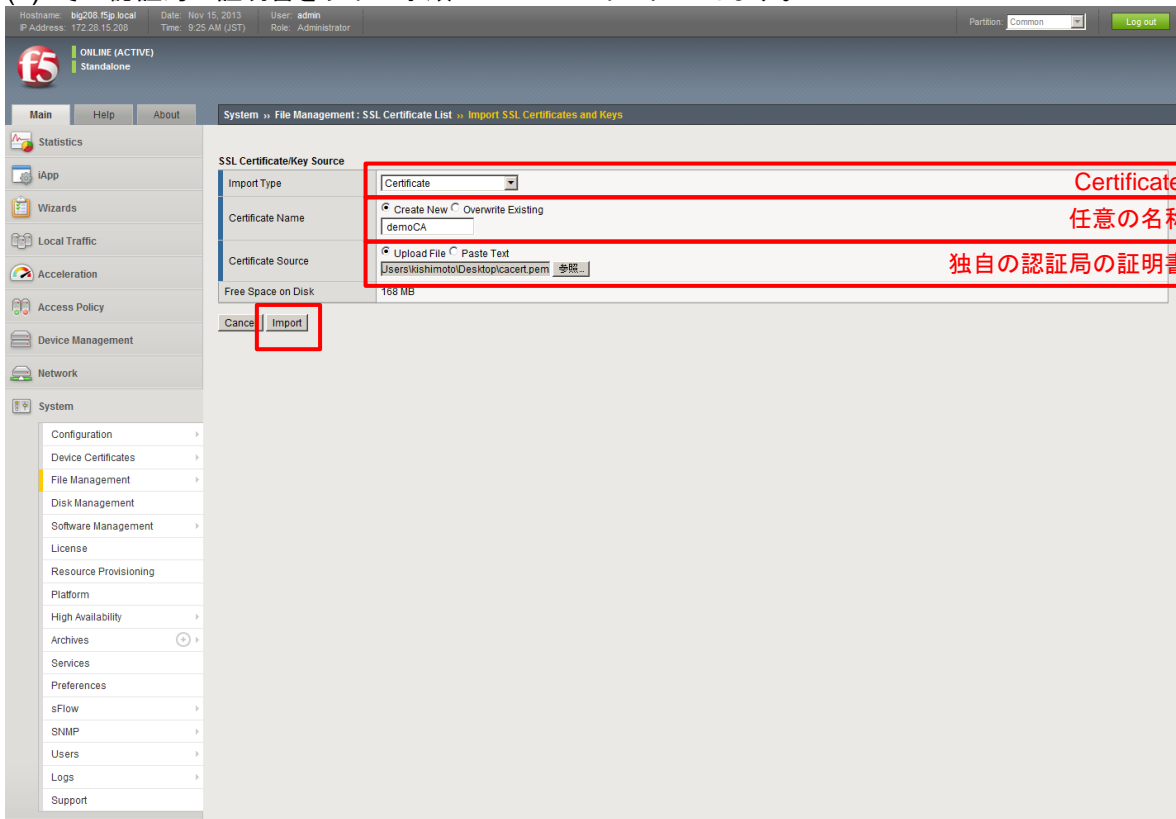
6.2.3. BIG-IP の設定

クライアント証明書認証に必要な BIG-IP の設定を示します。

6.2.3.1. 認証局の証明書のインポート

(1) あらかじめ、認証局の証明書を、BIG-IP の設定用 GUI へアクセスする PC にコピーしておきます。

(2) その認証局の証明書を以下の手順で BIG-IP へインポートします。



(3) 以下の状態になります。

Hostname: big208.f5.jp.local Date: Nov 15, 2013 User: admin
IP Address: 172.20.15.208 Time: 9:26 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

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

Data Group File List File List External Monitor Program File List **SSL Certificate List** Apache Certificate List

Search Import Create

<input type="checkbox"/>	Name	Contents	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>	NetAccess-001_cert	RSA Certificate & Key	apm.f5.jp.local	F5,JKK	Nov 14, 2014	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Aug 13, 2018 - Aug 13, 2018	Common
<input type="checkbox"/>	default	RSA Certificate	localhost.localdomain	MyCompany	May 11, 2023	Common
<input type="checkbox"/>	demoCA	RSA Certificate	f5jkk-ca	F5,JKK	Sep 11, 2022	Common
<input type="checkbox"/>	f5-irule	RSA Certificate	support.f5.com	F5 Networks	Aug 13, 2031	Common

Archive Delete

Configuration >
Device Certificates >
File Management >
Disk Management
Software Management >
License
Resource Provisioning
Platform
High Availability >
Archives >
Services
Preferences
sFlow >
SNMP >
Users >
Logs >
Support

- (4) 「[SSL サーバ証明書の設定](#)」で生成した、Client SSL Profile を編集します。
「Main」メニュー → 「Local Traffic」 → 「Profile」 → 「SSL」 → 「Client」で、該当する Profile をクリックすると、以下の画面が現れます。以下の通り設定します。

The screenshot shows the NetScaler configuration page for 'NetAccess-001-Client-SSL'. The 'Client Authentication' section is expanded, showing the following settings:

- Client Certificate: require (checked)
- Frequency: once
- Retain Certificate: Enabled
- Certificate Chain Traversal Depth: 9
- Trusted Certificate Authorities: demoCA (checked)
- Advertised Certificate Authorities: demoCA (checked)
- Certificate Revocation List (CRL): None

Annotations in red boxes and text:

- Red box around 'require' dropdown: 右のチェックボックスにチェックを入れて、「Require」を選択。
- Red box around 'demoCA' dropdown: 右のチェックボックスにチェックを入れて、インポートした証明書を選択。
- Red box around 'Update' button.

以上で、クライアント証明書認証の設定は完了です。

6.2.4. クライアントからのアクセス

- (1) クライアント PC から、APM VS へアクセスします。
- (2) クライアント証明書の選択画面が出たら、該当する証明書をクリックします。
- (3) APM へのアクセスが完了することを確認します。

6.3. セッション変数について

BIG-IP APM には、セッション変数(Session Variables)という便利な機能が実装されています。

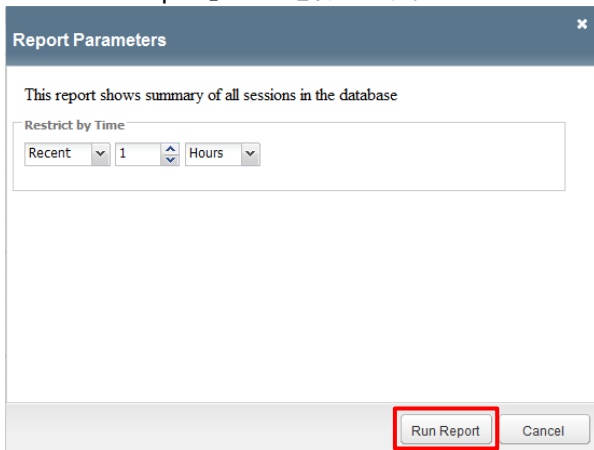
このセッション変数を利用することで、例えば、クライアント端末が持つ情報と、Active Directory で管理している情報を突き合わせて、情報が一致すれば次のアクションを実施する、というようなポリシーを生成することが可能です。

例えば、先のセクションで設定したクライアント証明書認証において、そのクライアント証明書内の値がセッション変数に取り込まれますので、その情報を利用することも可能です。

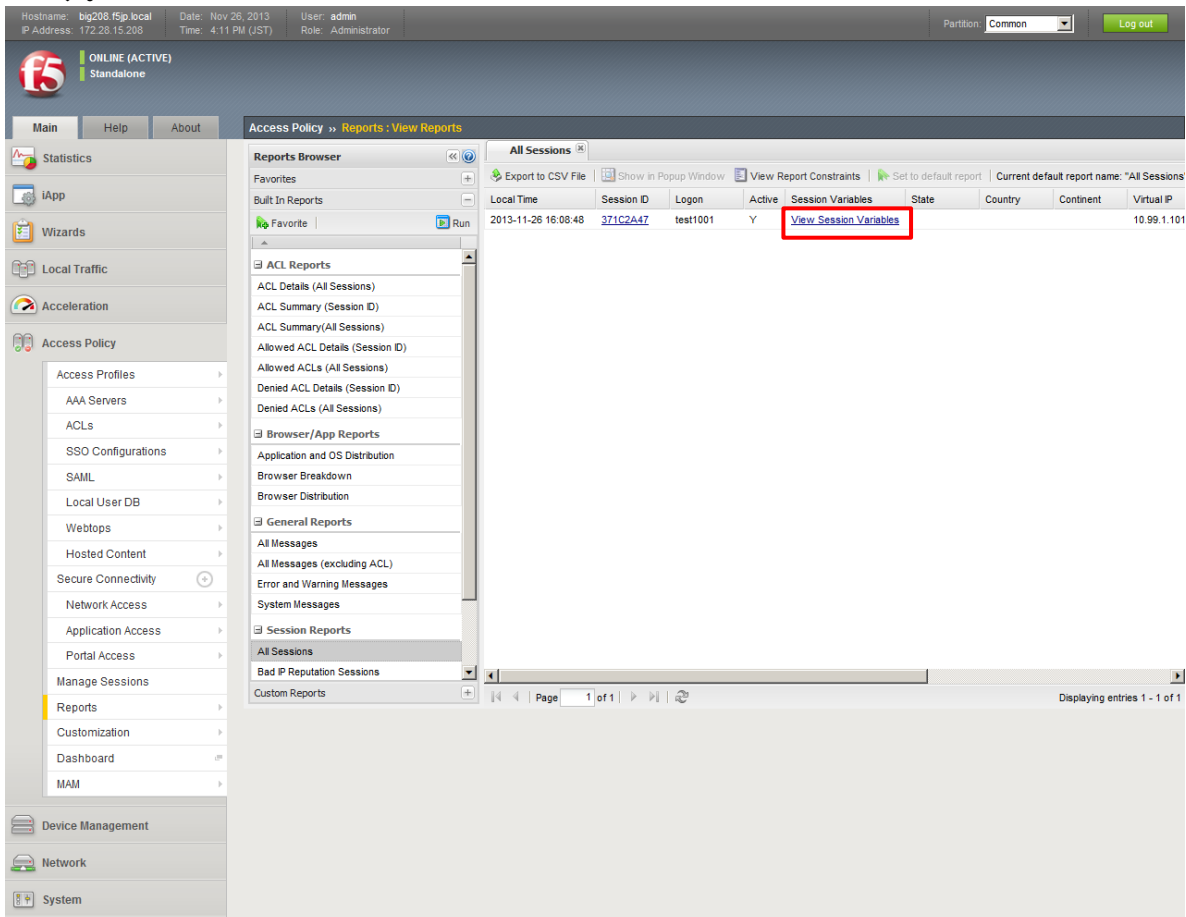
セッション変数の確認方法を以下に示します。

(1) クライアントが APM に接続された状態にします。

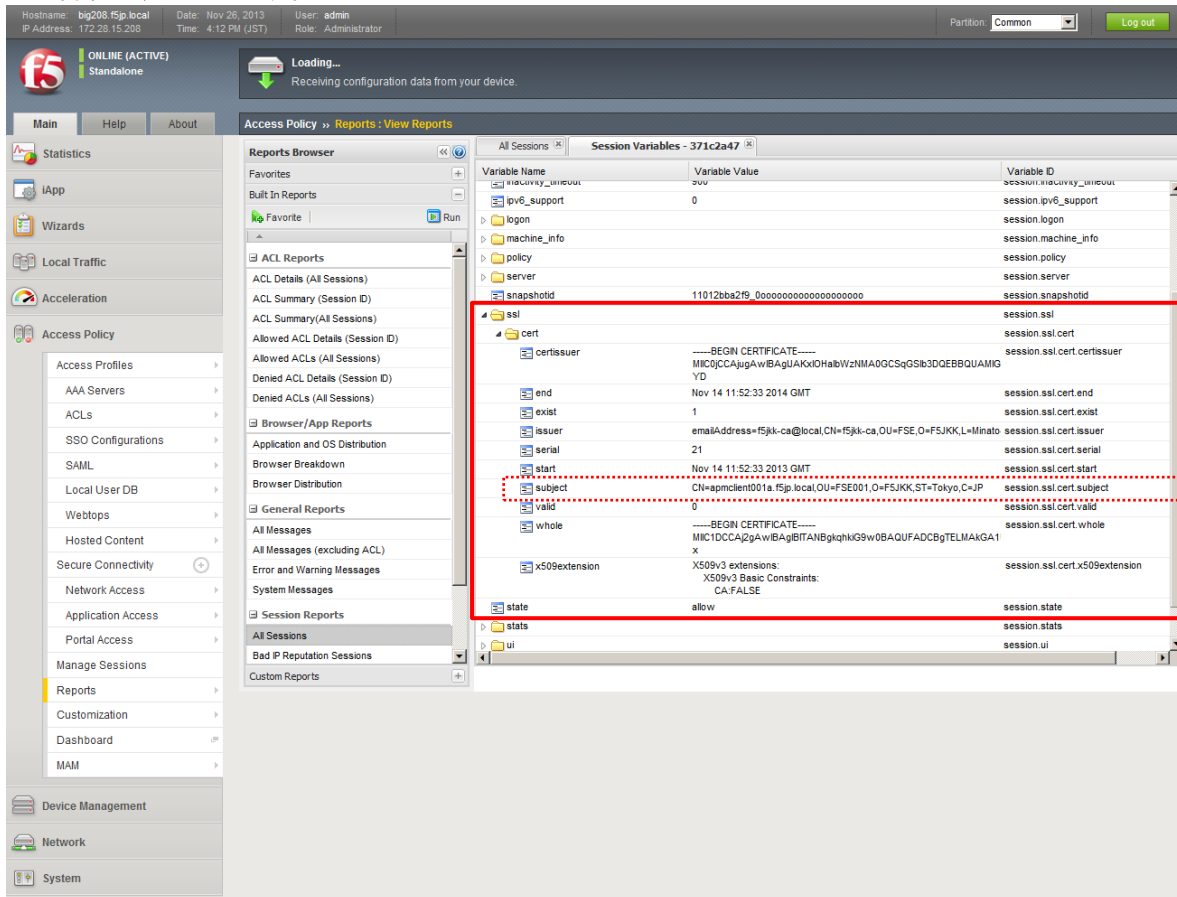
(2) 「Main」メニュー → 「Access Policy」 → 「Reports」を選ぶと、以下の画面が現れます。
「Run Report」ボタンを押します。



(3) アクセスした Logon ユーザ(本例では test1001)の行に表示されている、「View Session Variables」をクリックします。



(4) 表示された画面の Variable Name の中で、「ssl」を捜し、△ボタンをクリックして展開すると、クライアント証明書の詳細が表示されます。



上図の赤点線囲みの部分を例にとりますと、
「session.ssl.cert.subject」がセッション変数であり、
「CN=apmclient001a.f5jp.local,OU=FSE001,O=F5JJKK,ST=Tokyo,C=JP」がその値です。

クライアント証明書情報を APM のセッション変数に取り込む、というのはほんの一例であり、その他にもクライアントが持つ固有の情報(例:Windows であれば、NIC の MAC アドレス、マザーボードの ID 等)を取り込むことが可能です。このセッション変数を利用することで、ユーザ単位にアクセス制御を行うことが可能です。

以降、このセッション変数を利用したポリシーの設定例をいくつか紹介します。

6.4. [VPE サンプル-1] クライアント証明書の OU で ACL を割当て

クライアント証明書の OU 単位 (=組織単位) に、アクセスできるサーバを制限したい=Access Control Listを適用したい、という要件があると仮定します。

本例では、クライアント証明書の Subject に、"OU=FSE001"が含まれている場合に、ある ACL を割当て、という設定を行います。

6.4.1. ACL の作成

サンプルとして、実サーバ: 10.99.2.215 への SSH(Port: 22)アクセスを止める ACL を作成します。

- (1) 「Main」メニュー → 「Access Policy」 → 「ACLs」で表示された画面の右上の「Create」ボタンを押すと、以下の画面が表示されます。以下のように設定します。

The screenshot shows the Cisco F5 configuration interface. The breadcrumb navigation is "Access Policy >> ACLs : User-defined ACLs >> New ACL...". The "General Properties" section is visible, with the "Name" field containing "test1001-ACL". A red box highlights the "Name" field with the text "任意の名称を入力。" (Enter an arbitrary name). The "Type" is set to "Static" and "ACL Order" is set to "Last". The "Configuration" section shows "Match Case For Paths" set to "Yes". At the bottom, the "Create" button is highlighted with a red box.

General Properties	
Name	test1001-ACL
Type	Static
Description	
ACL Order	Last

Configuration	
Match Case For Paths	Yes

- (2) 以下の状態になります。
「Access Control Entries」の横の「Add」ボタンを押します。

The screenshot shows the Mikrotik WinBox interface. The top status bar indicates the user is 'admin' and the role is 'Administrator'. The main menu on the left includes 'Statistics', 'iApp', 'Wizards', 'Local Traffic', 'Acceleration', and 'Access Policy'. The 'Access Policy' section is expanded to show 'Access Profiles', 'AAA Servers', 'ACLs', and 'SSO Configurations'. The 'ACLs' section is selected, showing the configuration for 'test1001-ACL'. The 'General Properties' section includes fields for Name, Type, Partition / Path, Description, and ACL Order. The 'Configuration' section has a 'Match Case For Paths' dropdown set to 'Yes'. The 'Access Control Entries' section is currently empty, with a 'Remove' button and a table header. The 'Add...' button in the top right of this section is highlighted with a red box.

- (3) 送信元は特定せず(=Any)、宛先が 10.99.100.215 の SSH(Port 22)を止める設定を行います。

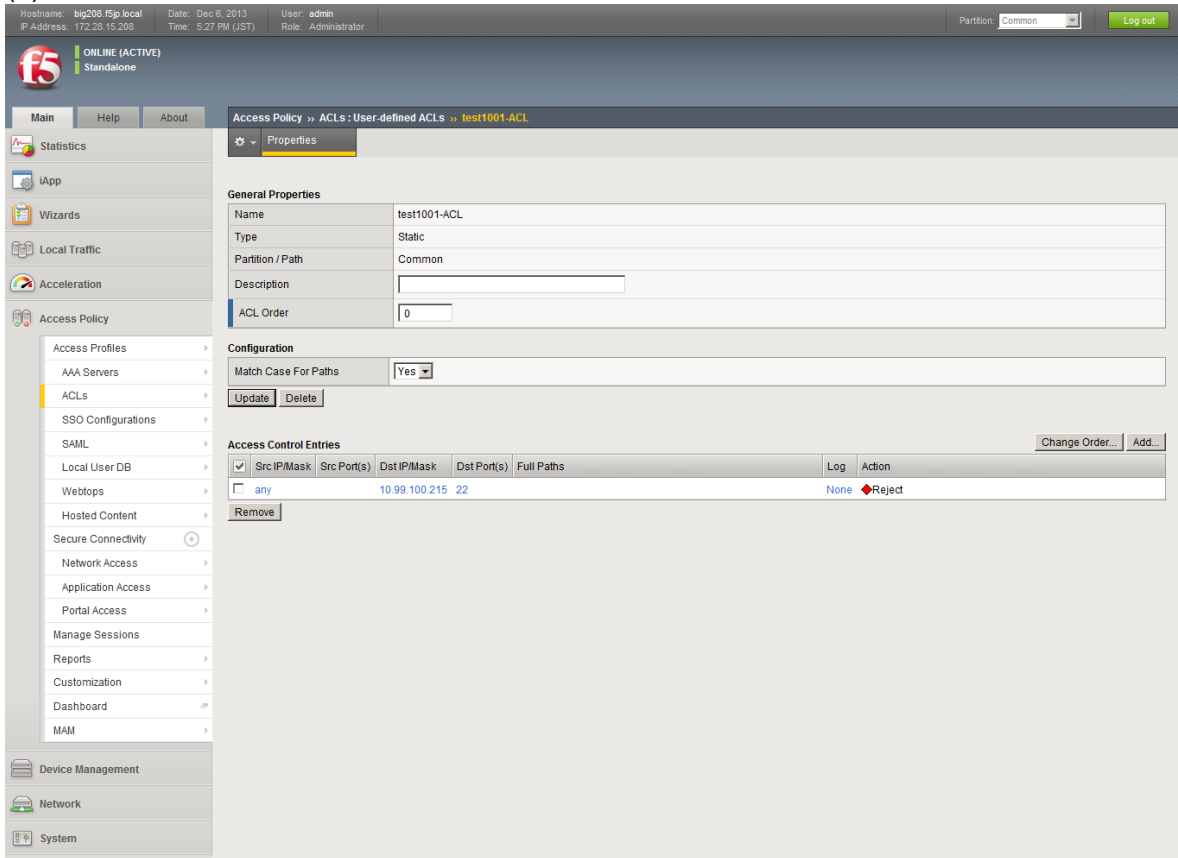
The screenshot shows the 'Access Control Entry Properties' dialog box in Mikrotik WinBox. The dialog is configured with the following settings:

- Type: L4 (selected)
- Source IP Address: Type: Any (selected), Host, Network
- Source Port(s): Type: Port, Port Range; Port: * (selected), All Ports
- Destination IP Address: Type: Any (selected), Host, Network; Address: 10.99.100.215
- Destination Port(s): Type: Port (selected), Port Range; Port: 22 (selected), SSH (selected)
- Protocol: TCP (selected)
- Action: Reject (selected)
- Log: None (selected)

 Red boxes and text annotations highlight these settings:

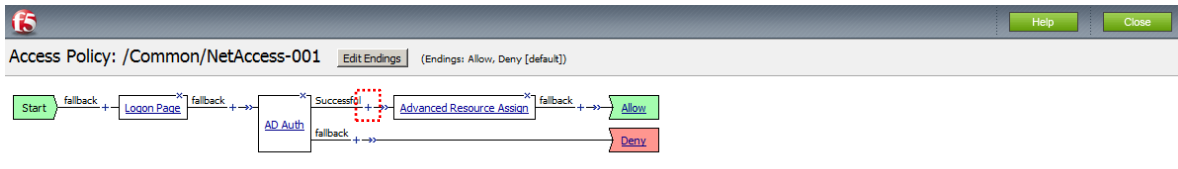
- A red box around the 'Type' dropdown is annotated with '本例では、「L4」を選択。' (In this example, select 'L4').
- A red box around the 'Source IP Address' section is annotated with '送信元は Any を指定。' (Specify Any for the source).
- A red box around the 'Destination IP Address' and 'Destination Port(s)' fields is annotated with '宛先は、10.99.100.215:22 を指定。' (Specify 10.99.100.215:22 for the destination).
- A red box around the 'Protocol' and 'Action' dropdowns is annotated with 'プロトコルは TCP を選択。アクションとして「Reject」を選択。' (Select TCP for the protocol. Select 'Reject' as the action).

(4) この状態になります。



6.4.2. VPE の設定

(1) ここまでの設定では、VPE は以下の状態になっています。
AD Auth の後ろにある「+」をクリックします。



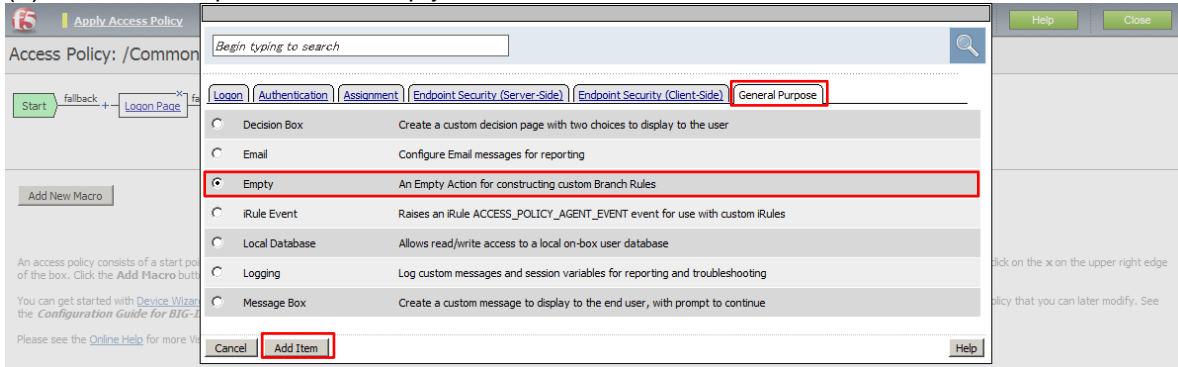
Add New Macro

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the Add Macro button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with Device Wizards. On the main navigation pane, expand Templates and Wizards, and click Device Wizards, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the Configuration Guide for BIG-IP Access Policy Manager for more on creating and editing an access policy.

Please see the Online Help for more Visual Policy Editor basics.

(2) 「General Purpose」タブで「Empty」を選択し、「Add Item」ボタンを押します。



An access policy consists of a start point of the box. Click the Add Macro button

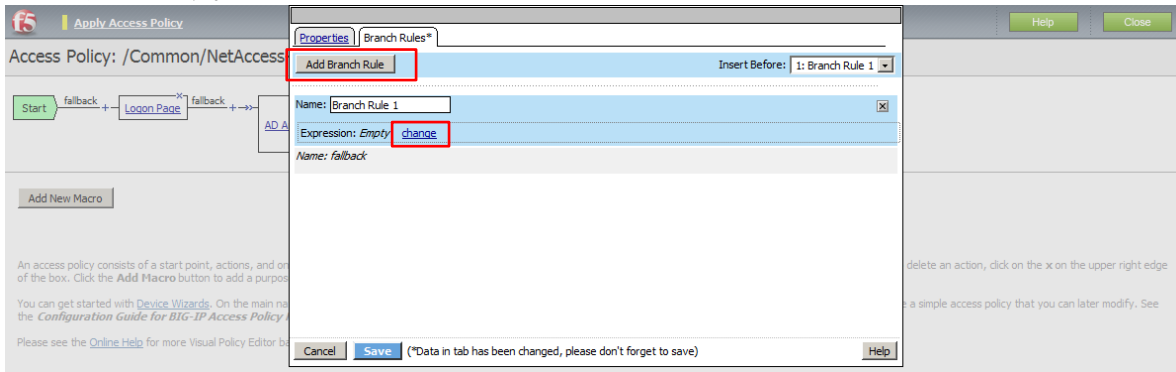
You can get started with Device Wizard the Configuration Guide for BIG-IP

Please see the Online Help for more V

Click on the x on the upper right edge

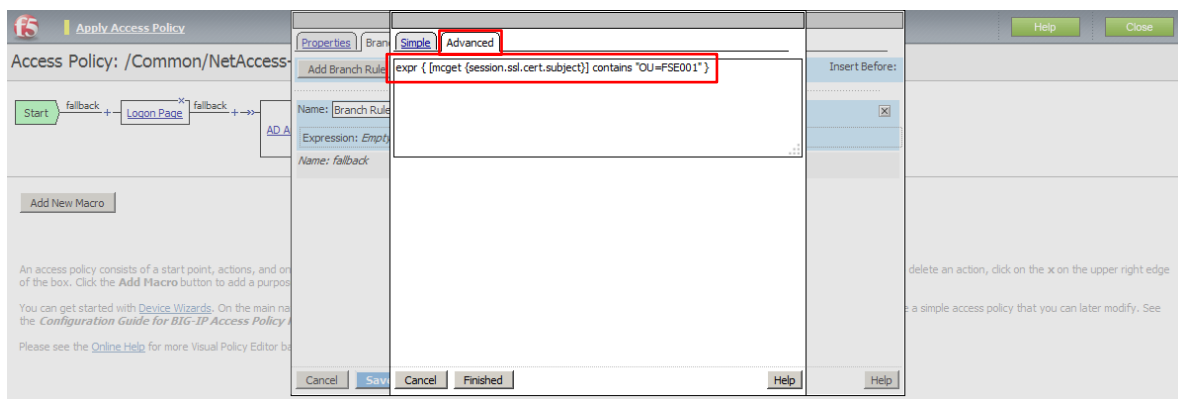
policy that you can later modify. See

- (3) 「Branch Rules」タブを選択します。「Add Branch Rule」ボタンを押して、Expression を 1 つ追加し、「Change」をクリックします。



- (4) 「Advanced」タブを選択し、以下のように TCL 形式で入力します。

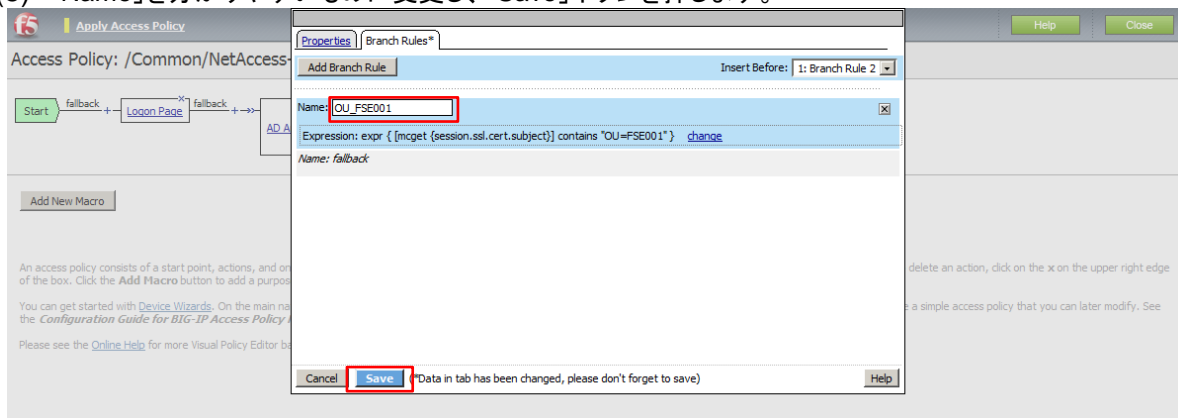
```
expr { [mcget {session.ssl.cert.subject}] contains "OU=FSE001" }
```



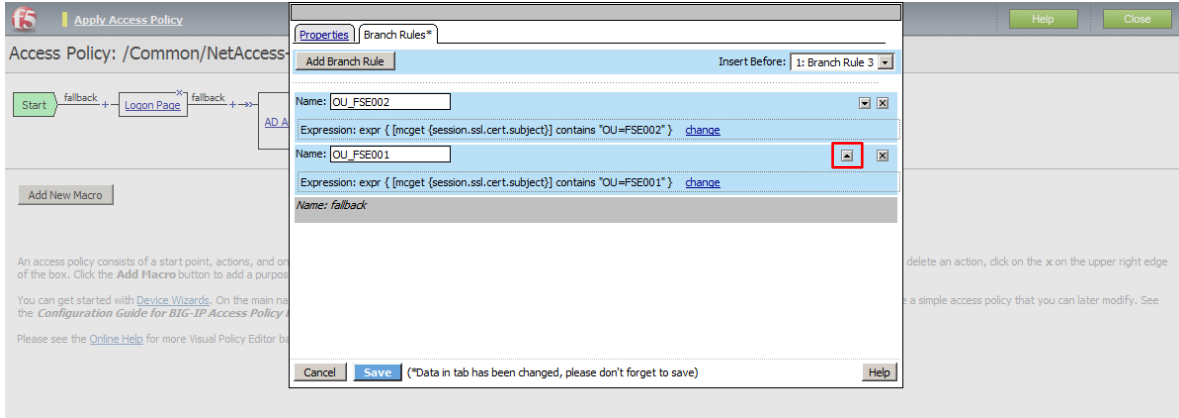
「mcget」コマンド: このコマンドによって、BIG-IP APM のセッション変数(Session Variable)に取り込まれた値を取り出します。

この構文によって、セッション変数: "session.ssl.cert.subject" の値に、"OU=FSE001" が含まれているかどうかを確認します。確認結果が OK であれば、次のボックスへ進みます。

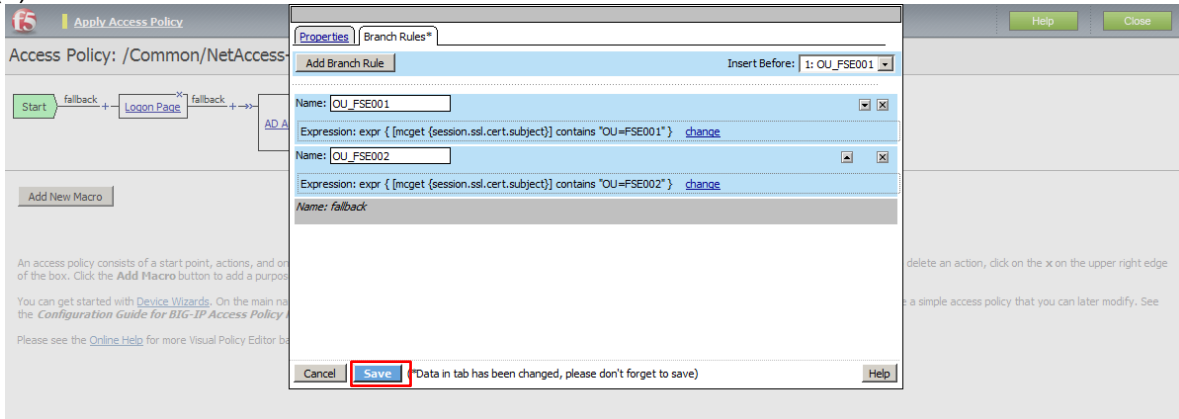
- (5) 「Name」を分かりやすいものに変更し、「Save」ボタンを押します。



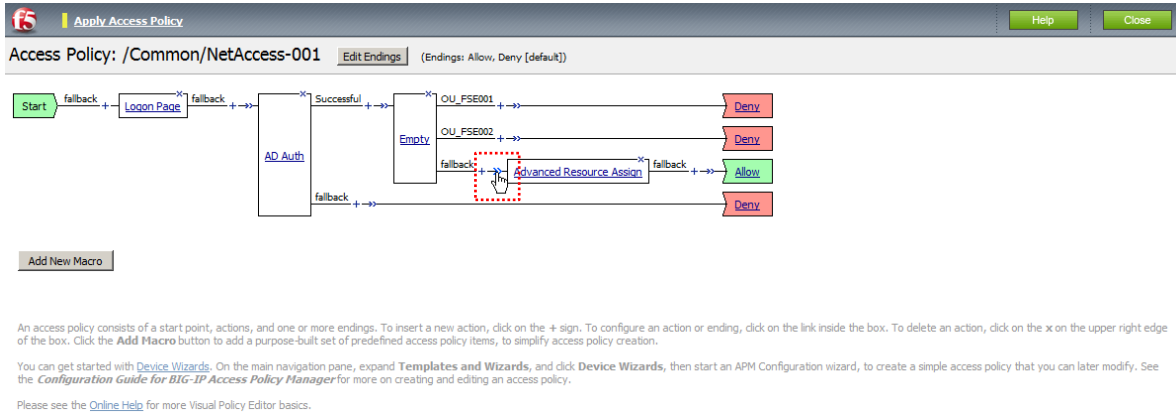
- (6) 同様の方法で、2つ目の分岐(OU=FSE002 の場合)も追加してみた状態です。
VPE の見た目上、FSE001 を一番上にしたい場合、以下の▲ボタンを押します。



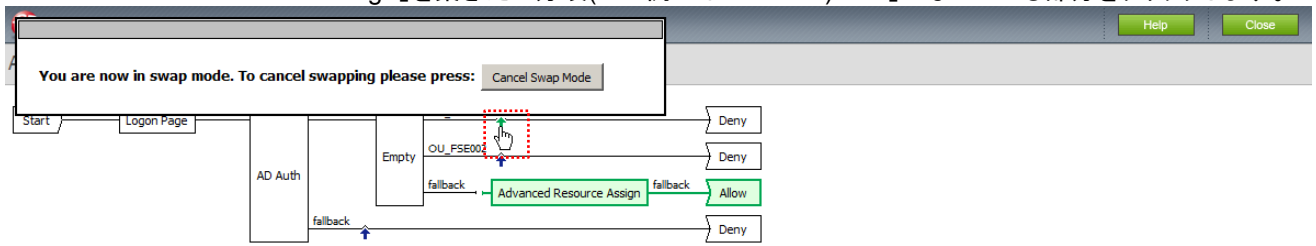
- (7) 以下のように、上下が入れ替わります。「Save」ボタンを押します。



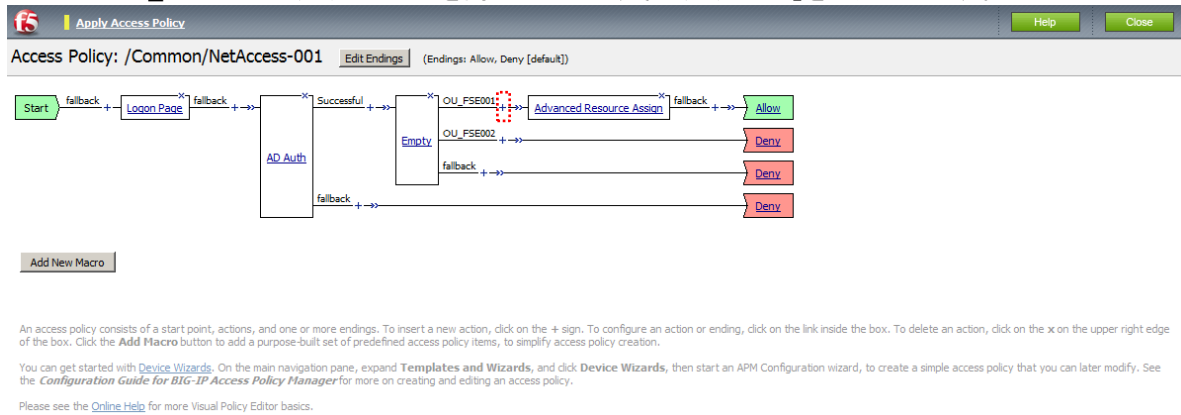
- (8) この例では、以下のように、「Fallback」に「Advanced Resource Assign」がつながっています。
このままだと、OU=FSE001 でも、OU=FSE002 でもないものに対して、リソースがアサインされる状態になっていますので、これを変更します。「Fallback」の後ろにある「>>」のマークをクリックします。



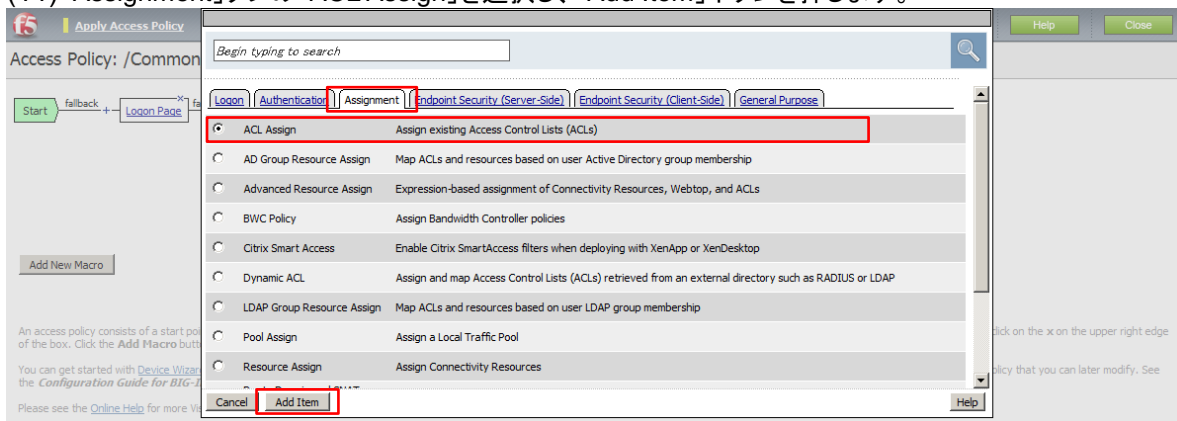
- (9) 以下のような画面に変わります。
「Advanced Resource Assign」を繋ぎたい分岐(この例では FSE001)の「^」になっている部分をクリックします。



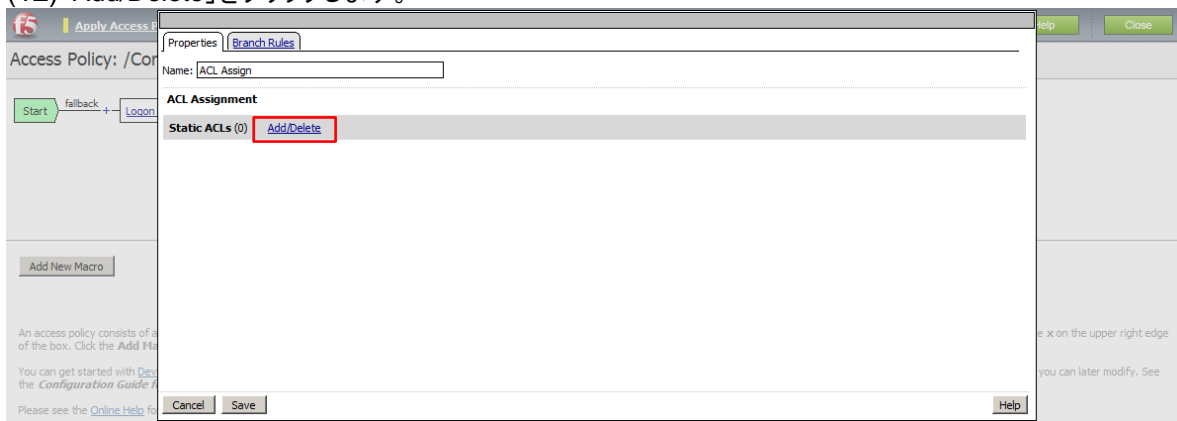
- (10)以下のように、「Advanced Resource Assign」が移動します。
次に"OU_FSE001"の分岐に ACL を割当てるため、その分岐の「+」をクリックします。



- (11)「Assignment」タブの「ACL Assign」を選択し、「Add Item」ボタンを押します。



- (12)「Add/Delete」をクリックします。



- (13)既に作成した ACL(TEST1001-ACL)のチェックボックスにチェックを入れ、「Save」ボタンを押します。



(14)以下の状態になります。「Apply Access Policy」を押して、設定を適用します。



6.4.3. クライアントからのアクセス

- (1) OU=FSE001 のクライアント証明書を持つクライアント PC から、APM の VS へアクセスします。
- (2) アクセス完了後、10.99.2.215 の SSH(Port 22)へのアクセスだけが Reject されることを確認します。

6.5. [VPE サンプル-2] Active Directory の Group で ACL を割当てて

Active Directory のユーザが属する Group 毎に、アクセスできるサーバを制限したい=Access Control List を適用したい、という要件があると仮定します。

本例では、"CorpA-Group"に属するユーザ:"test1001"に対して ACL を適用し、"CorpB-Group"に属するユーザ:"test1002"には ACL を適用しない、という設定を行います。

6.5.1. ACL の作成

"[VPE サンプル-1]"で作成した ACL:Test1001-ACL を利用しますので、設定例は省略します。

6.5.2. Active Directory ユーザ:test1001

(1) 全般

ダイヤルイン	環境	セッション	リモート制御	リモート デスクトップ サービスのプロファイル
個人用仮想デスクトップ	COM+	UNIX 属性	プラグナ	
全般	住所	アカウント	プロファイル	電話
所属されている組織	所属するグループ			

test1001

姓(L): test

名(E): 1001 イニシャル(I):

表示名(S): test1001

説明(D):

事業所(O):

電話番号(T): その他(O)...

電子メール(M): test1001@corp.f5.jp.local

Web ページ(W): その他(W)...

OK キャンセル 適用(A) ヘルプ

(2) 所属するグループ

test1001 は、CorpA-Group に属しています。この CorpA-Group に対して、ACL を割当てて設定を行います。

ダイヤルイン	環境	セッション	リモート制御	リモート デスクトップ サービスのプロファイル
個人用仮想デスクトップ	COM+	UNIX 属性	プラグナ	
全般	住所	アカウント	プロファイル	電話
所属されている組織	所属するグループ			

所属するグループ(M):

名前	Active Directory ドメイン サービス フォルダ
CorpA-Group	corp.f5.jp.local/Users
CSAdministrator	corp.f5.jp.local/Users
Domain Users	corp.f5.jp.local/Users
ExchangeGroup	corp.f5.jp.local/Users

追加(A)... 削除(R)

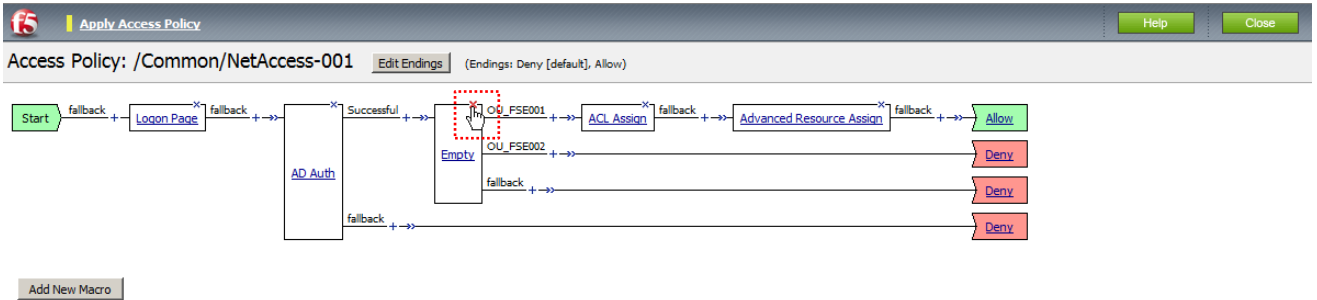
プライマリ グループ: Domain Users

プライマリ グループの設定(S) Macintosh クライアントまたは POSIX 対応のアプリケーションがない場合は、プライマリ グループを変更する必要はありません。

OK キャンセル 適用(A) ヘルプ

6.5.3. VPE の設定

- (1) ここまでの設定では、VPE は以下のようになっています。
一旦、Empty 以降をすべて削除します。
ボックスの右上の「×」をクリックします。

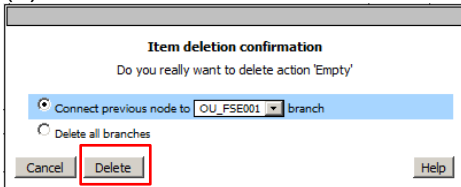


An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

- (2) 以下のような画面が現れます。そのまま、「Delete」を押します。



- (3) 同様の手順で、「ACL Assign」も「Advanced Resource Assign」も削除し、以下の状態にします。
「AD Auth」の Successful 分岐上の「+」をクリックします。

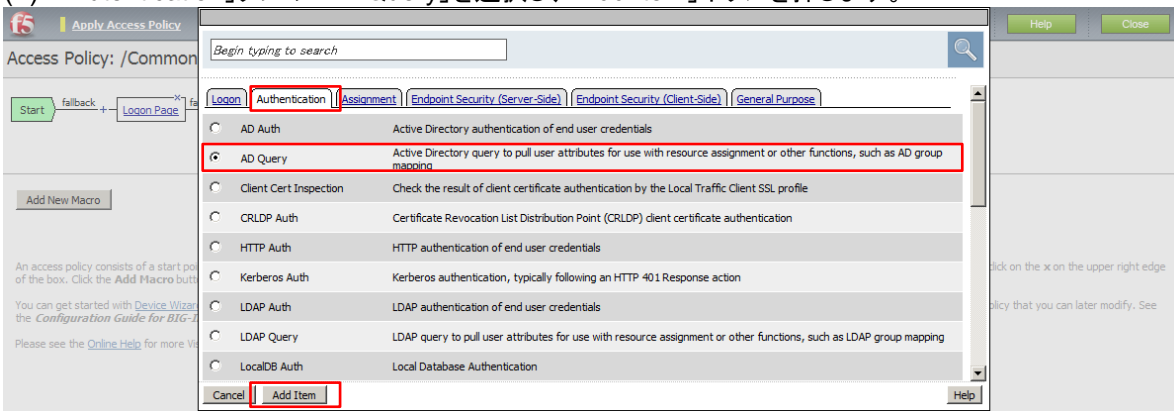


An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

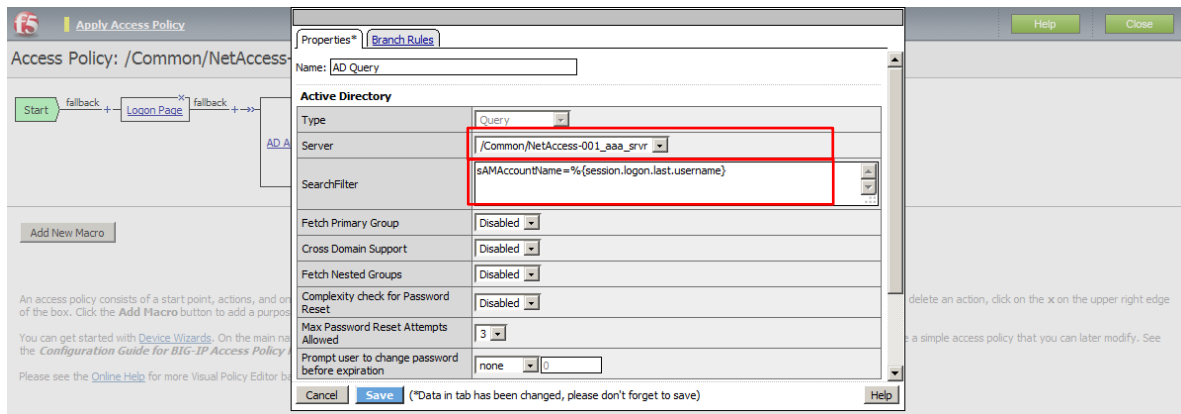
- (4) 「Authentication」タブの「AD Query」を選択し、「Add Item」ボタンを押します。



(5) 「Server」として、既に設定した Active Directory 設定(NetAccess-001_aaa_srvr)を選択します。

「SerchFilter」には、以下を入力します。

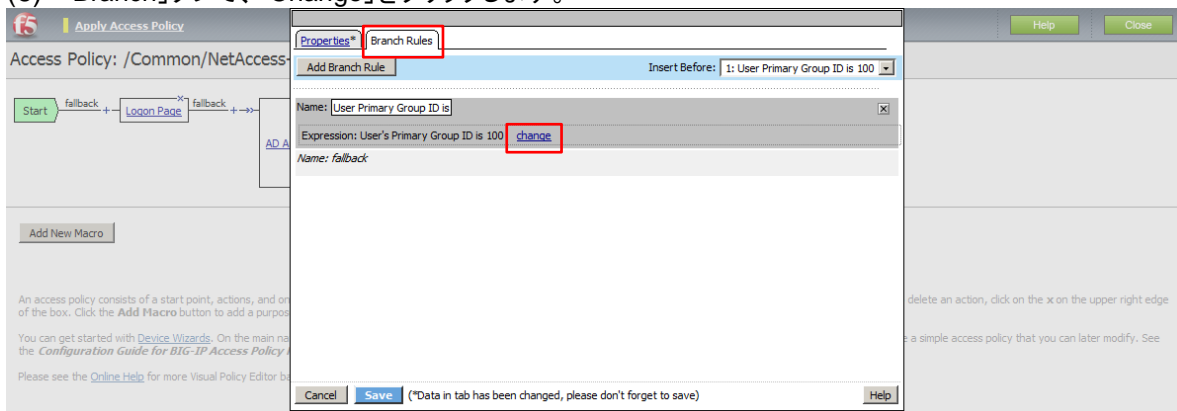
sAMAccountName=%{session.logon.last.username}



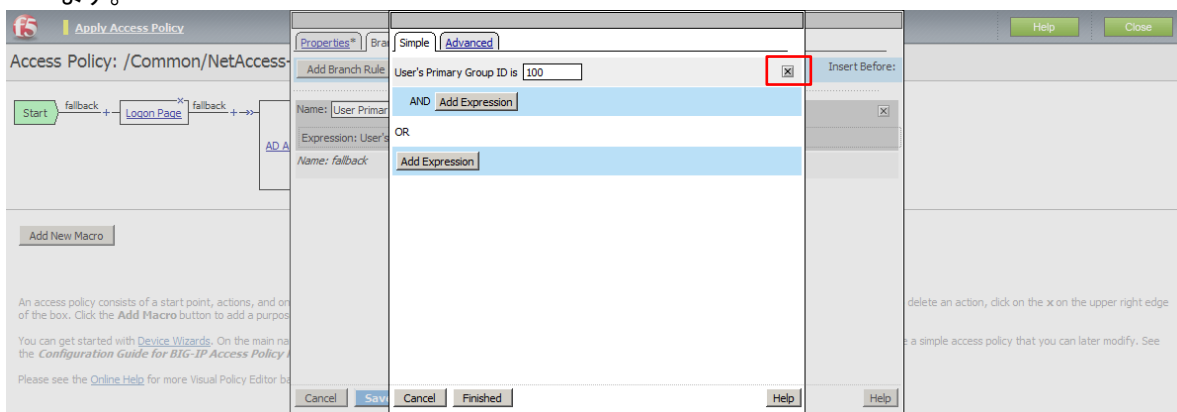
SearchFilter に入力した「sAMAccountName」は、Active Directory で定義されている、ユーザ名の変数です。この変数に、APM にログインしたときのユーザ名(例: test1001)を代入して、AD Query を実施する、という定義です。

APM にログインしたときのユーザ名は、セッション変数:「session.logon.last.username」の値として格納されていますので、「=%{session.logon.last.username}」で代入を行います。

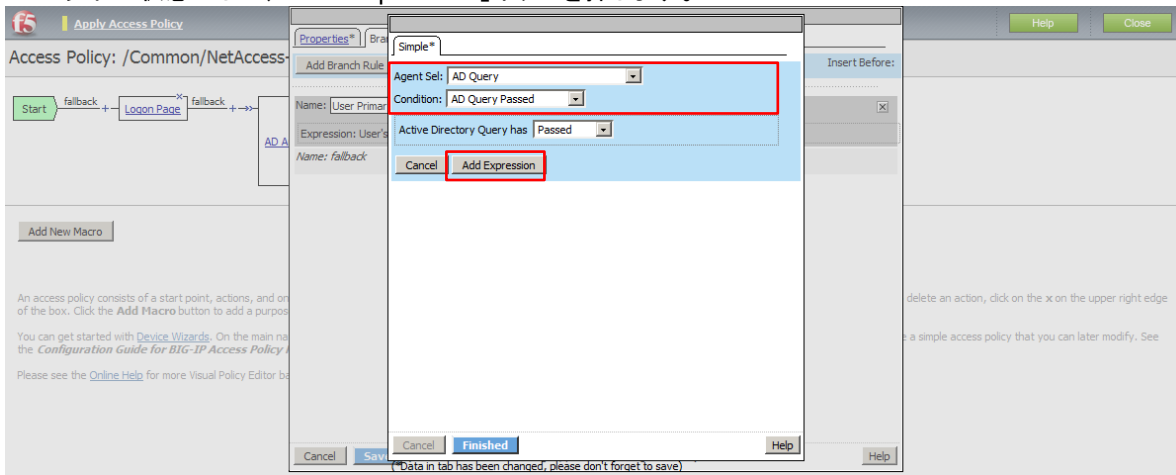
(6) 「Branch」タブで、「Change」をクリックします。



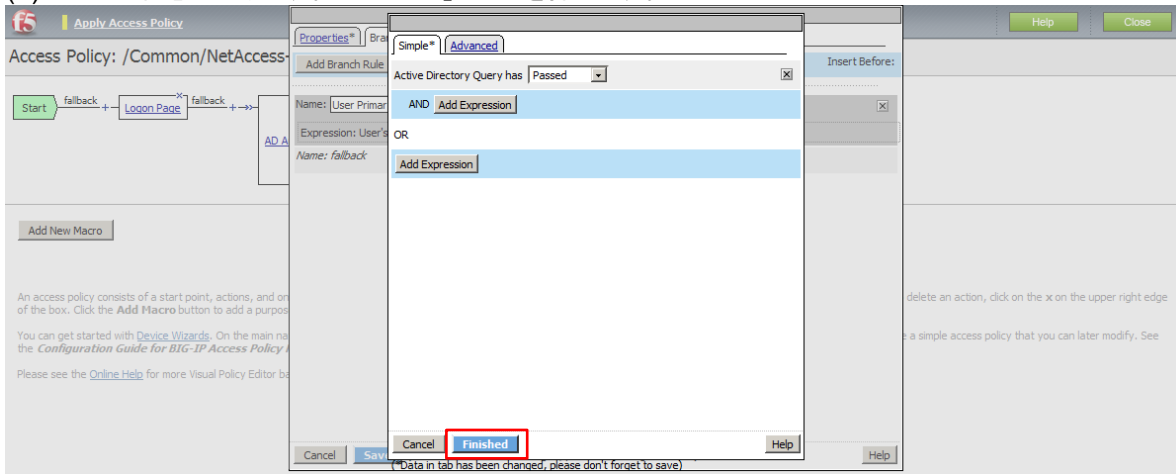
(7) 「Simple」タブ上で、デフォルトで設定されている「User's Primary Group ID is 100」を、「×」ボタンを押して削除します。



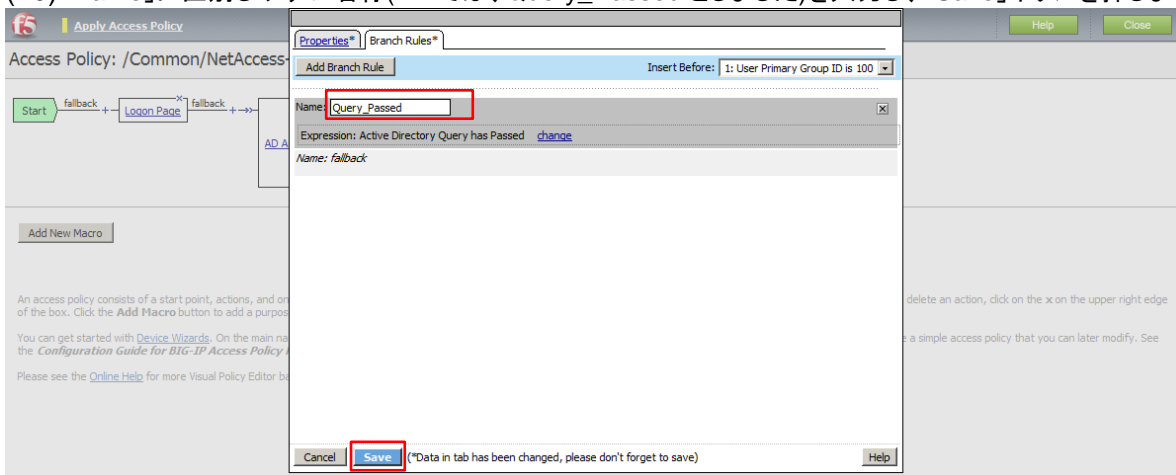
- (8) 「Add Expression」ボタンをクリックすると、以下の画面が現れます。
ここでは、単純に、AD Query が成功したら、次の BOX に移動する定義にしています。
以下の状態にして、「Add Expression」ボタンを押します。



- (9) 以下の状態になります。「Finished」ボタンを押します。

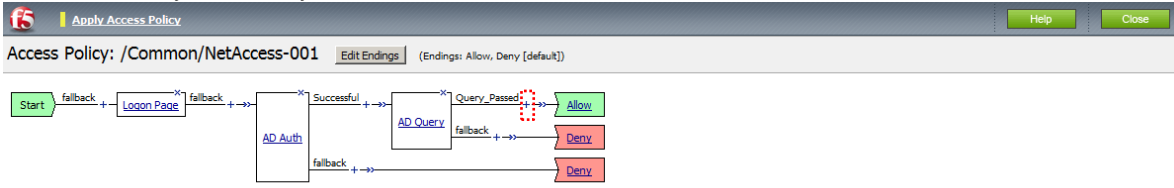


- (10) 「Name」に区別しやすい名称(ここでは、Query_Passed としました)を入力し、「Save」ボタンを押します。



(11)以下の状態になります。

「AD Query」の「Query_Passed」分岐上にある「+」をクリックします。



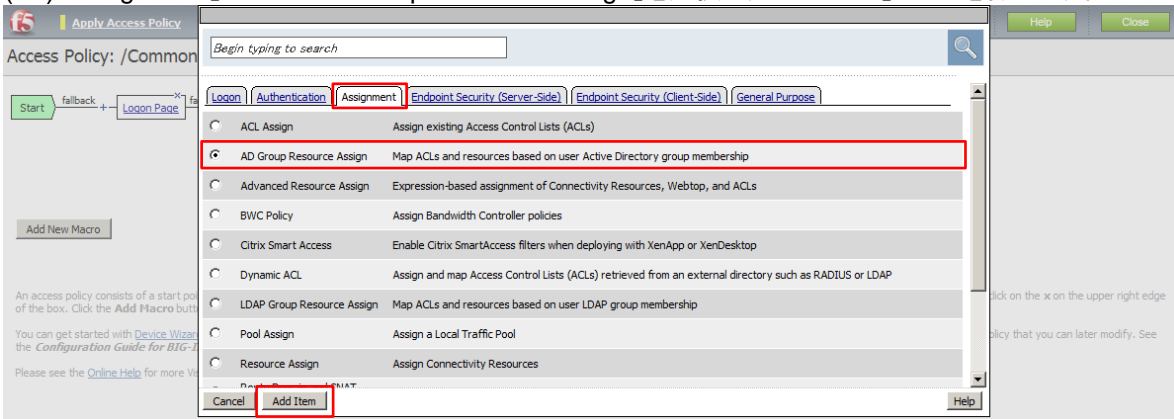
Add New Macro

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

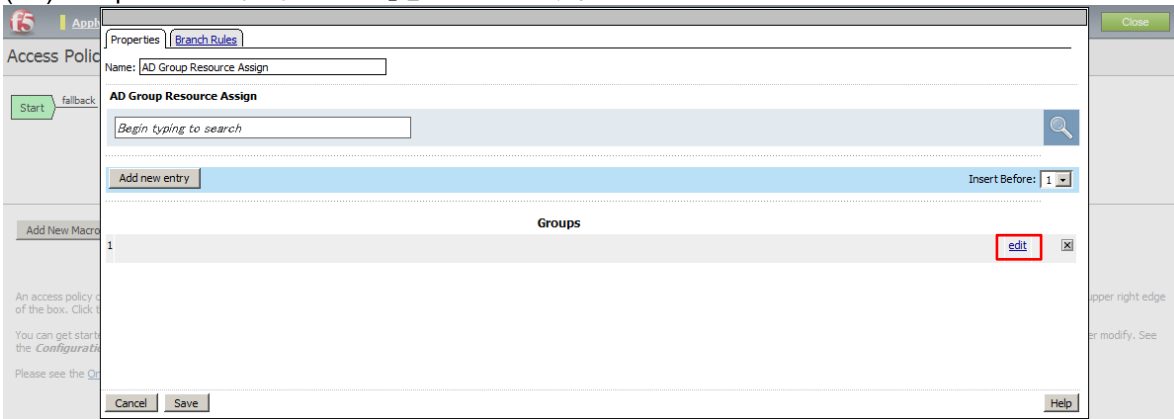
You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

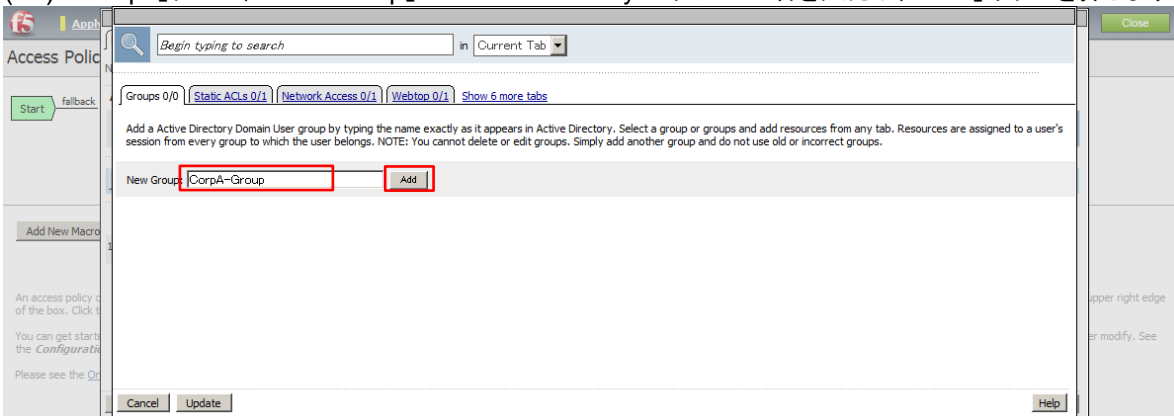
(12)「Assignment」タブの「AD Group Resource Assign」を選択し、「Add Item」ボタンを押します。



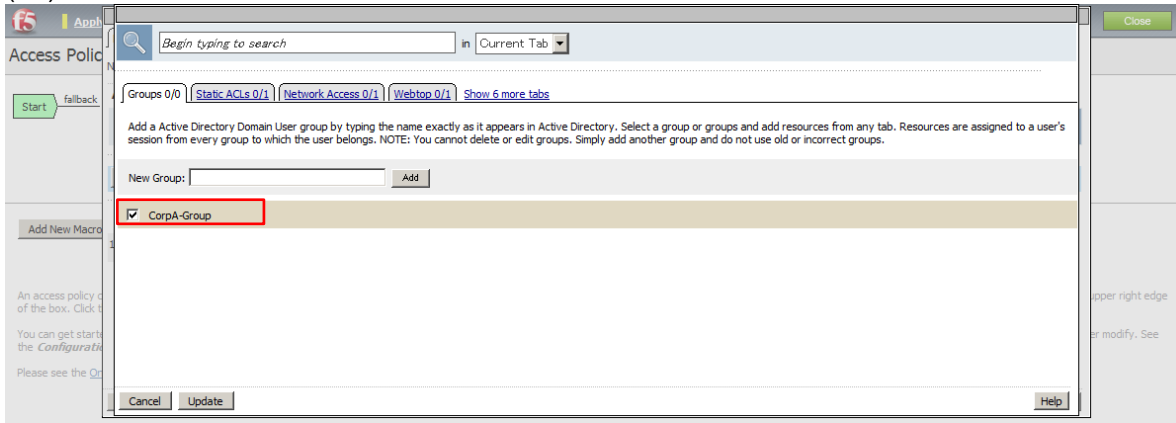
(13)Groups の下にある行の「edit」をクリックします。



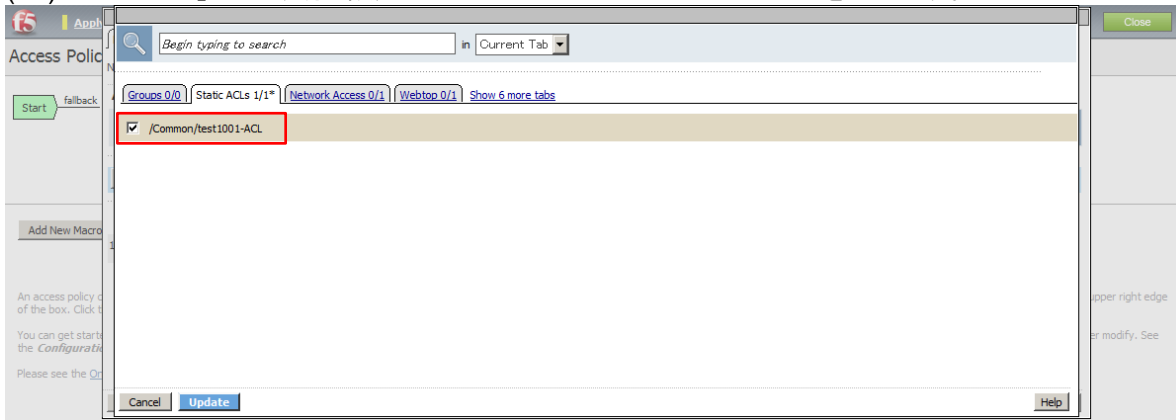
(14)「Groups」タブで、「New Group」に Active Directory のグループ名を入力し、「Add」ボタンを押します。



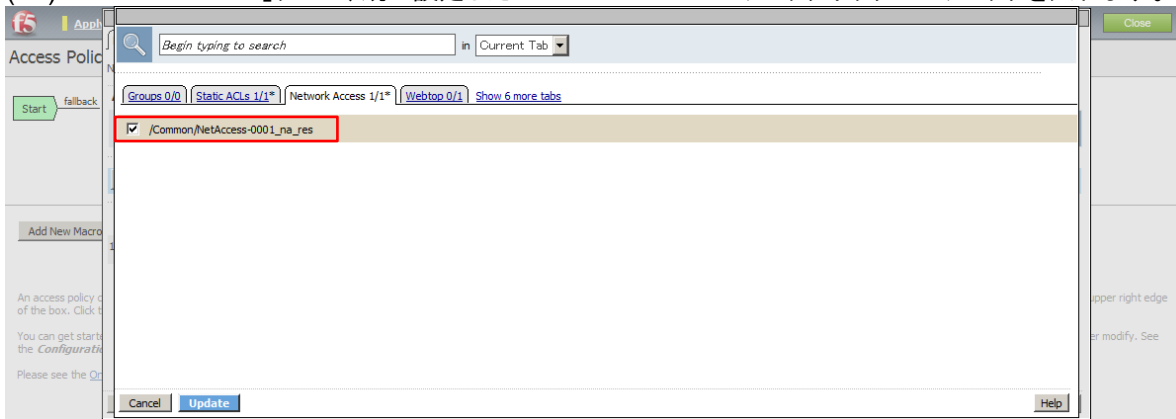
(15)以下の状態になります。



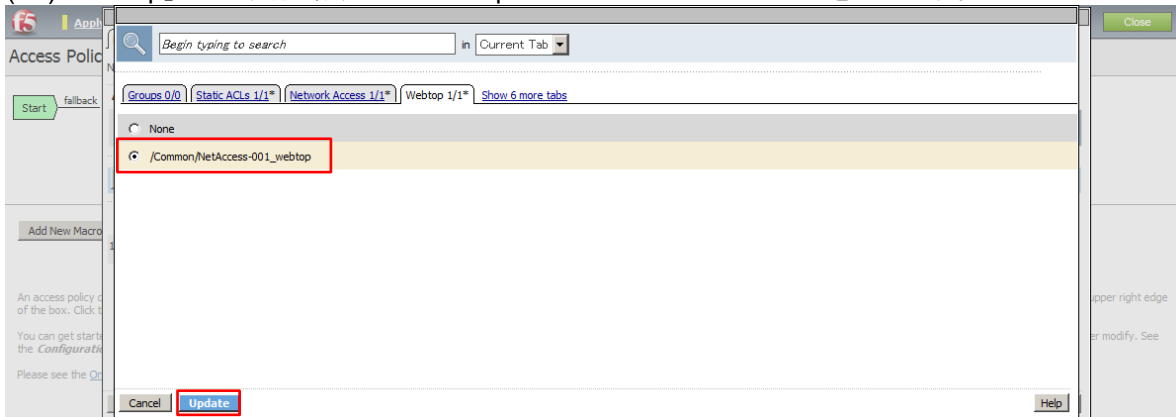
(16)「Static ACL」タブで、既に設定した ACL のチェックボックスにチェックを入れます。



(17)「Network Access」タブで、既に設定した Network Access のチェックボックスにチェックを入れます。

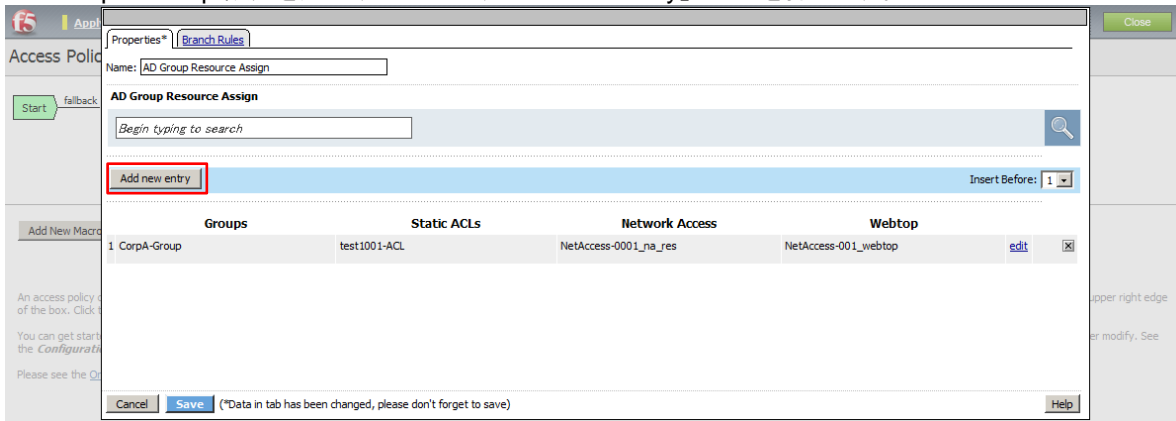


(18)「Webtop」タブで、既に設定した Webtop のチェックボックスにチェックを入れます。



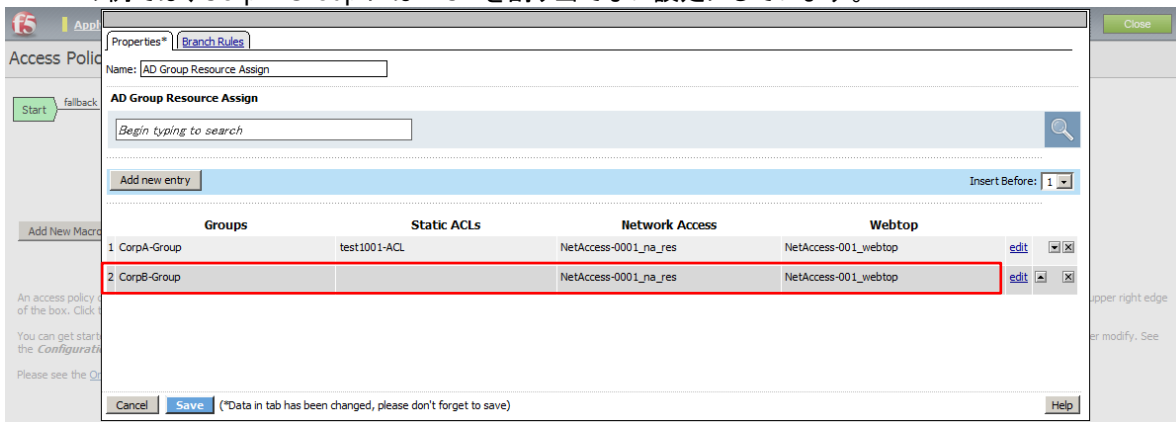
(19)以下の状態になります。

CorpB-Group 設定を追加するために、「Add new entry」ボタンを押します。

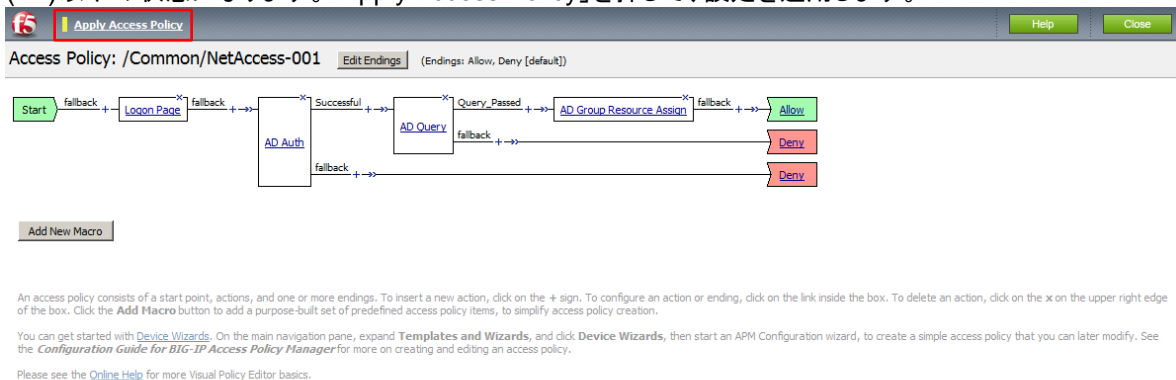


(20)同様の手順で CorpB-Group の設定を行います。

この例では、CorpB-Group には ACL を割り当てない設定にしています。



(21)以下の状態になります。「Apply Access Policy」を押して、設定を適用します。



6.5.4. クライアントからのアクセス

- (1) クライアント PC から、CorpA-Group に属するユーザ:"test1001"で、APM の VS へアクセスします。
- (2) アクセス完了後、10.99.2.215 の SSH(Port 22)へのアクセスだけが Reject されることを確認します。
- (3) クライアント PC から、CorpB-Group に属するユーザ:"test1002"で、APM の VS へアクセスします。
- (4) CorpB-Group には ACL が割り当てられていないので、すべてのアクセスが通過する (なにもRejectされない) ことを確認します。

6.5.5. AD Query がうまく行かない場合:AAA 設定の変更

Active Directory 設定またはそのユーザ設定によっては、Administrator 権限が必要となる場合があります。その場合には、以下の部分を追加してみてください。

「Main」メニュー → 「Access Policy」 → 「AAA Servers」 → 「Active Directory」 → 設定済みの AAA サーバをクリックすることで、以下の画面が現れます。以下の赤囲み部分を追加してみてください。

The screenshot shows the configuration page for an Active Directory AAA server. The interface includes a top status bar with system information, a left sidebar with navigation menus, and a main content area with a breadcrumb trail: Access Policy > AAA Servers > NetAccess-001_aaa_srvr. The 'Properties' tab is active, displaying 'General Properties' and 'Configuration' sections. The 'Configuration' section contains several fields: Domain Name (corp.f5.jp.local), Server Connection (Use Pool / Direct), Domain Controller (10.99.2.218), Admin Name (Administrator), Admin Password (masked with dots), Verify Admin Password (masked with dots), Kerberos Preauthentication Encryption Type (None), and Timeout (15 seconds). A red rectangular box highlights the 'Admin Name', 'Admin Password', and 'Verify Admin Password' fields. At the bottom of the configuration section are 'Update' and 'Delete' buttons.

General Properties	
Name	NetAccess-001_aaa_srvr
Partition / Path	Common
Type	Active Directory

Configuration	
Domain Name	corp.f5.jp.local
Server Connection	<input type="radio"/> Use Pool <input checked="" type="radio"/> Direct
Domain Controller	10.99.2.218
Admin Name	Administrator
Admin Password	*****
Verify Admin Password	*****
Kerberos Preauthentication Encryption Type	None
Timeout	15 seconds

6.6. [VPE サンプル-3] アクセスできるクライアント端末を限定する

Active Directory のユーザが利用する端末を限定したい、という要件があると仮定します。

本例では、"test1001"が使うことができる端末は、その端末のマザーボードシリアル番号が Active Directory に登録されているものだけにする、という設定を行います。

6.6.1. クライアント端末固有の情報の取得

クライアント端末のマザーボードシリアル番号情報が入手できない場合、APM で調べる事も可能です。以下、クライアント PC のマザーボードのシリアル番号を取得するためのステップです。

- (1) ここまでの設定では、以下の状態になっています。
「Logon Page」の前の「+」をクリックします。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with **Device Wizards**. On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the **Configuration Guide for BIG-IP Access Policy Manager** for more on creating and editing an access policy.

Please see the **Online Help** for more Visual Policy Editor basics.

- (2) 「Endpoint Security (Client-Side)」タブで、「Machine Info」を選択し、「Add Item」ボタンを押します。

Item	Description
<input type="radio"/> Anti-Spyware	Anti-spyware Software Check for Windows and Mac
<input type="radio"/> Antivirus	Antivirus Software Check for Windows, Mac and Linux
<input type="radio"/> Firewall	Firewall Software Check for Windows, Mac and Linux
<input type="radio"/> Hard Disk Encryption	Hard Disk Encryption Software Check for Windows and Mac
<input type="radio"/> Linux File	Determine if particular Linux file exists
<input type="radio"/> Linux Process	Determine if particular Linux process exists
<input type="radio"/> Mac File	Determine if particular Macintosh file exists
<input type="radio"/> Mac Process	Determine if particular Macintosh process exists
<input type="radio"/> Machine Cert Auth	Determine if a machine certificate is installed and is valid
<input checked="" type="radio"/> Machine Info	Collects machine information from the client system, such as CPU, BIOS, network adapter, and hard disk details
<input type="radio"/> Patch Management	Patch Management Software Check for Windows, Mac and Linux

- (3) そのまま、「Save」ボタンを押します。

Machine Info

Name: Machine Info

Cancel Save Help

(4) 以下の状態になります。一旦、「Apply Access Policy」をクリックして設定を適用します。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(5) クライアント PC から APM Virtual Server へアクセスします。

(6) 「Main」メニュー → 「Access Policy」 → 「Reports」を選ぶと、以下の画面が現れます。「Run Report」ボタンを押します。

(7) アクセスした Logon ユーザ (本例では test1001) の行に表示されている、「View Session Variables」をクリックします。

Local Time	Session ID	Logon	Active	Session Variables	State	Country	Continent	Virtual IP
2013-11-26 16:08:48	371C2A47	test1001	Y	View Session Variables				10.99.1.101

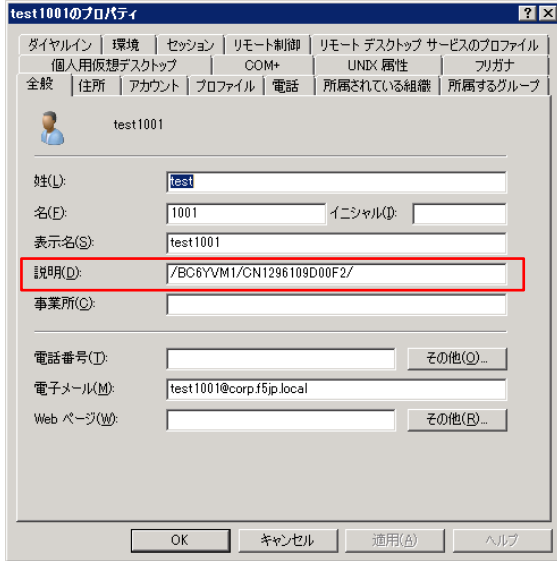
- (8) 「Variable Name」の「Machine_info」の△をクリックして展開します。
 その中に、「Motherboard」ディレクトリがあるので、△をクリックして展開します。
 「Variable ID」が、「session.machine_info.last.motherboard.sn」の値がマザーボードのシリアル番号です。

Variable Name	Variable Value	Variable ID
machine_info		session.machine_info
/Common/NetAccess-001_act_machine_info_ag		session.machine_info/Common/NetAccess-001_act_machine_info_ag
last		session.machine_info.last
bios		session.machine_info.last.bios
manufacturer	Dell Inc.	session.machine_info.last.bios.manufacturer
sn	BC6VVM1	session.machine_info.last.bios.sn
version	DELL - 6222004	session.machine_info.last.bios.version
cpu		session.machine_info.last.cpu
description	Intel®4 Family 6 Model 37 Stepping 5	session.machine_info.last.cpu.description
max_clock	2534	session.machine_info.last.cpu.max_clock
name	Intel(R) Core(TM) i5 CPU M 540 @ 2.53GHz	session.machine_info.last.cpu.name
vendor	GenuineIntel	session.machine_info.last.cpu.vendor
hdd		session.machine_info.last.hdd
count	2	session.machine_info.last.hdd.count
list		session.machine_info.last.hdd.list
[0]		session.machine_info.last.hdd.list.[0]
model	SAMSUNG SSD PM1800 2.5" 128GB ATA Device	session.machine_info.last.hdd.list.[0].model
sn	S0DTNEAZA02312	session.machine_info.last.hdd.list.[0].sn
[1]		session.machine_info.last.hdd.list.[1]
model	BUFFALO HD-PCTU2 USB Device	session.machine_info.last.hdd.list.[1].model
sn	00J05B0P724100000000	session.machine_info.last.hdd.list.[1].sn
motherboard		session.machine_info.last.motherboard
manufacturer	Dell Inc.	session.machine_info.last.motherboard.manufacturer
product	012JJ4	session.machine_info.last.motherboard.product
sn	/BC6VVM1/CN1298109D00F2/	session.machine_info.last.motherboard.sn
net_adapter		session.machine_info.last.net_adapter
count	2	session.machine_info.last.net_adapter.count
list		session.machine_info.last.net_adapter.list
[0]		session.machine_info.last.net_adapter.list.[0]
mac_address	00:24:D7:36:3A:AC	session.machine_info.last.net_adapter.list.[0].mac_address
name	Intel(R) Centrino(R) Ultimate-N 6300 AGN	session.machine_info.last.net_adapter.list.[0].name
[1]		session.machine_info.last.net_adapter.list.[1]
mac_address	5C:26:0A:09:06:47	session.machine_info.last.net_adapter.list.[1].mac_address
name	Intel(R) 82577LM Gigabit Network Controller	session.machine_info.last.net_adapter.list.[1].name

マザーボードシリアル番号がチェックできたら(またはコピーできたら)、一旦、ネットワークアクセスを切断します。

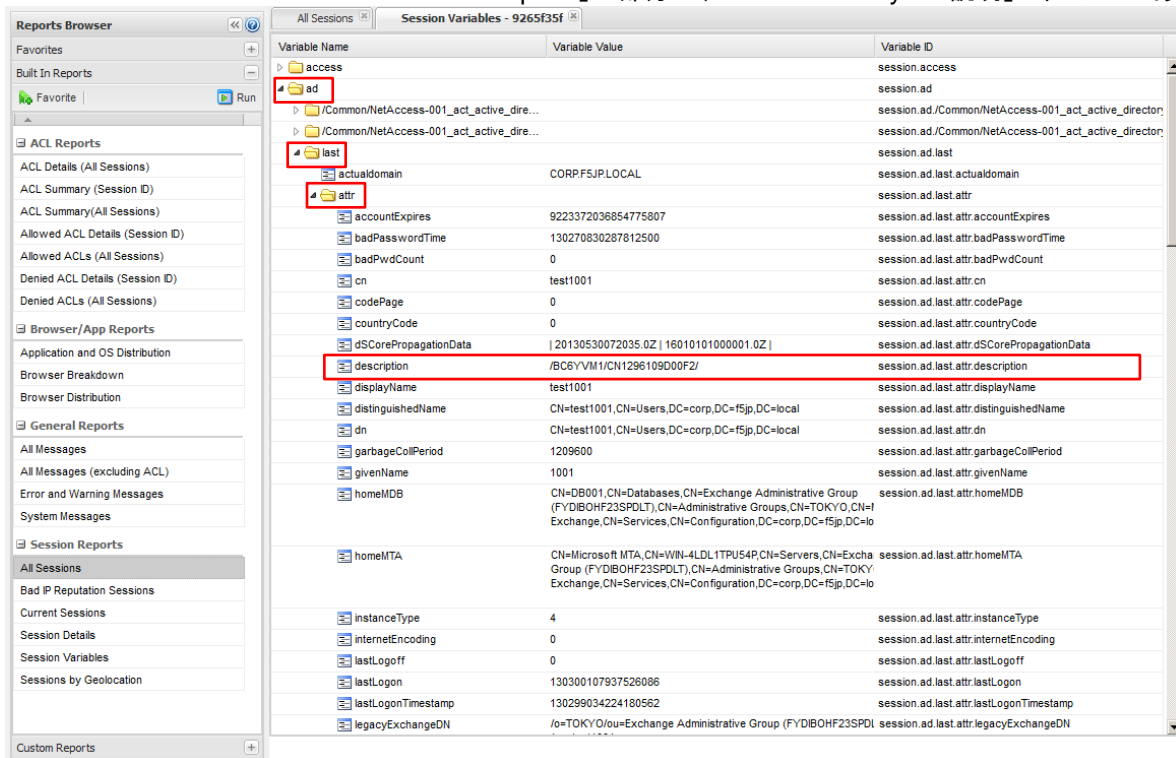
6.6.2. Active Directory の設定

- (1) Active Directory 上の "test1001" 設定を開きます。本例では、「説明」フィールドを使うことにします。ここに、クライアント PC のマザーボードシリアル番号を入力します。



The screenshot shows the 'test1001のプロパティ' dialog box. The '説明(D):' field is highlighted with a red box and contains the value '/BC6YVM1/CN1296109D00F2/'. Other fields include '姓(L): test', '名(E): 1001', '表示名(S): test1001', '電子メール(M): test1001@corp.f5jp.local', and 'Web ページ(W):'.

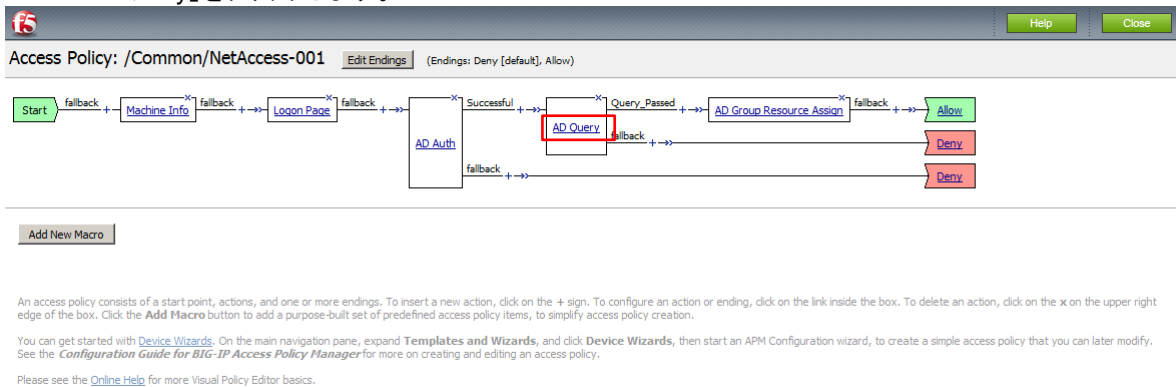
- (2) 今一度、クライアント PC から、APM の Virtual Server へアクセスします。
- (3) もう一度、「Main」メニュー → 「Access Policy」 → 「Reports」で、test1001 の Session Variable を確認します。「ad」 → 「last」 → 「attr」を展開します。Variable ID: 「session.ad.last.attr.description」の部分が、Active Directory の「説明」フィールドにあたります。



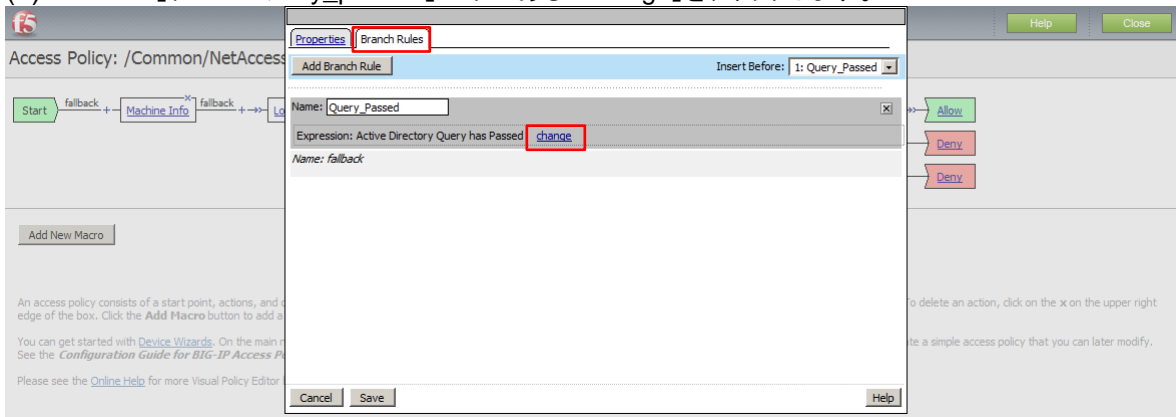
The screenshot shows the 'Session Variables - 9265f35f' window. The 'description' variable is highlighted with a red box, showing its value as '/BC6YVM1/CN1296109D00F2/'. Other variables include 'access', 'ad', 'last', 'attr', 'actualdomain', 'accountExpires', 'badPasswordTime', 'badPwdCount', 'cn', 'codePage', 'countryCode', 'dSCorePropagationData', 'displayName', 'distinguishedName', 'dn', 'garbageCollPeriod', 'givenName', 'homeMDB', 'homeMTA', 'instanceType', 'internetEncoding', 'lastLogoff', 'lastLogon', 'lastLogonTimestamp', and 'legacyExchangeDN'.

Variable Name	Variable Value	Variable ID
access		session.access
ad		session.ad
ad	/Common/NetAccess-001_act_active_dir...	session.ad./Common/NetAccess-001_act_active_dir...
ad	/Common/NetAccess-001_act_active_dir...	session.ad./Common/NetAccess-001_act_active_dir...
last		session.ad.last
last	actualdomain	session.ad.last.actualdomain
last	attr	session.ad.last.attr
last.attr	accountExpires	session.ad.last.attr.accountExpires
last.attr	badPasswordTime	session.ad.last.attr.badPasswordTime
last.attr	badPwdCount	session.ad.last.attr.badPwdCount
last.attr	cn	session.ad.last.attr.cn
last.attr	codePage	session.ad.last.attr.codePage
last.attr	countryCode	session.ad.last.attr.countryCode
last.attr	dSCorePropagationData	session.ad.last.attr.dSCorePropagationData
last.attr	description	session.ad.last.attr.description
last.attr	displayName	session.ad.last.attr.displayName
last.attr	distinguishedName	session.ad.last.attr.distinguishedName
last.attr	dn	session.ad.last.attr.dn
last.attr	garbageCollPeriod	session.ad.last.attr.garbageCollPeriod
last.attr	givenName	session.ad.last.attr.givenName
last.attr	homeMDB	session.ad.last.attr.homeMDB
last.attr	homeMTA	session.ad.last.attr.homeMTA
last.attr	instanceType	session.ad.last.attr.instanceType
last.attr	internetEncoding	session.ad.last.attr.internetEncoding
last.attr	lastLogoff	session.ad.last.attr.lastLogoff
last.attr	lastLogon	session.ad.last.attr.lastLogon
last.attr	lastLogonTimestamp	session.ad.last.attr.lastLogonTimestamp
last.attr	legacyExchangeDN	session.ad.last.attr.legacyExchangeDN

- (4) クライアントPCのマザーボードシリアル番号と、Active Directoryに登録したそのシリアル番号を比較して、同じであれば次のボックスへ進む、という設定を行います。
「AD Query」をクリックします。

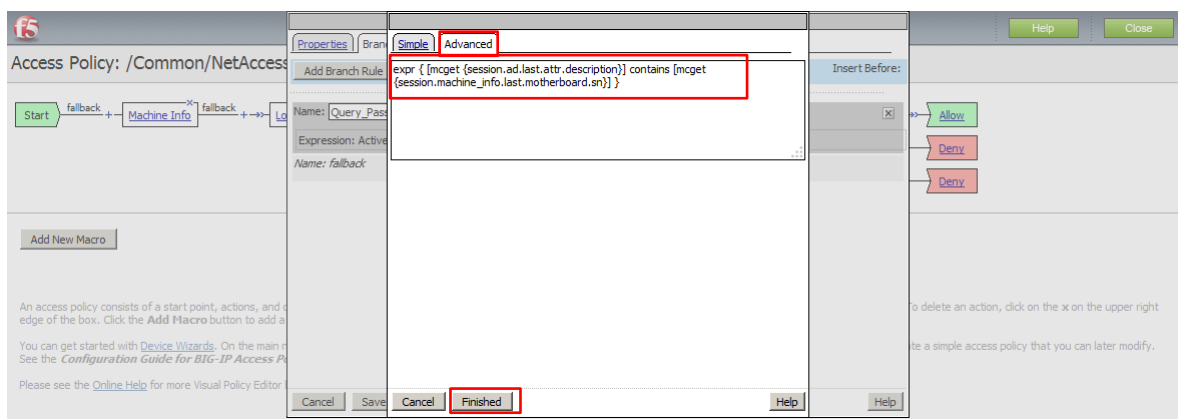


- (5) 「Branch」タブで「Query_passed」の下にある「Change」をクリックします。



- (6) 「Advanced」タブで、以下を入力します。

```
expr { [mcget {session.ad.last.attr.description}] contains [mcget {session.machine_info.last.motherboard.sn}] }
```

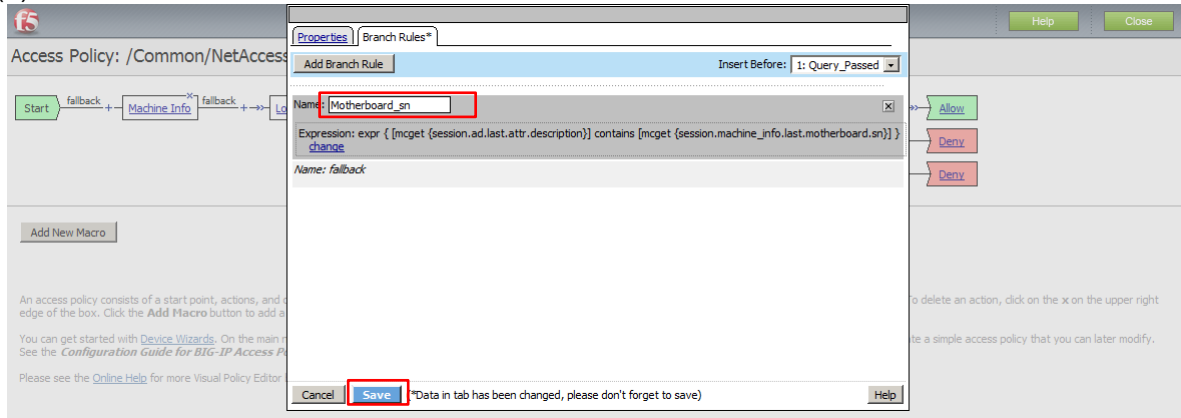


セッション変数:「session.ad.last.attr.description」の値(=Active Directoryの「説明」フィールド値)をmcgetで取得しています。

また、「session.machine_info.last.motherboard.sn」の値(=クライアントPCのマザーボードシリアル番号)もmcgetで取得しています。

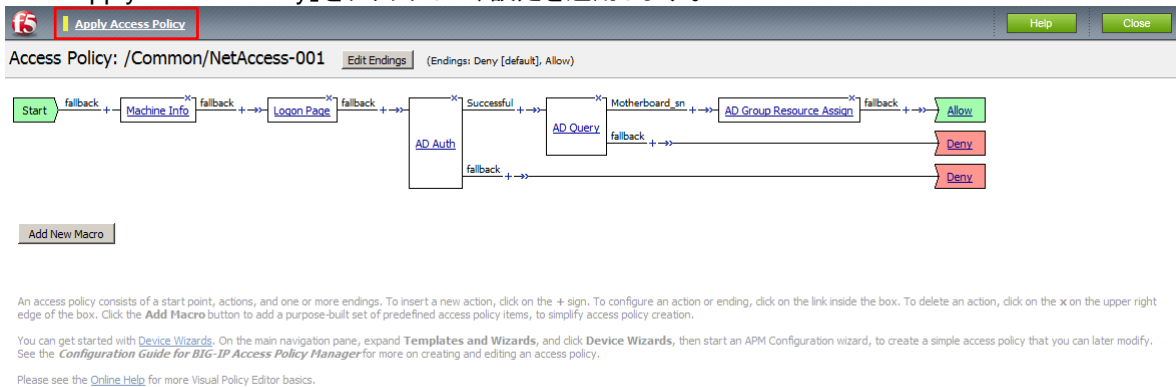
この例では、「session.ad.last.attr.description」の値が「session.machine_info.last.motherboard.sn」の値を含んでいるかどうかをチェックし、含んでいる(=同じである)場合には次のボックスに進む、という設定にしています。

(7) 「Name」を区別しやすいものに変更し、「Save」ボタンを押します。



(8) 以下の状態になります。

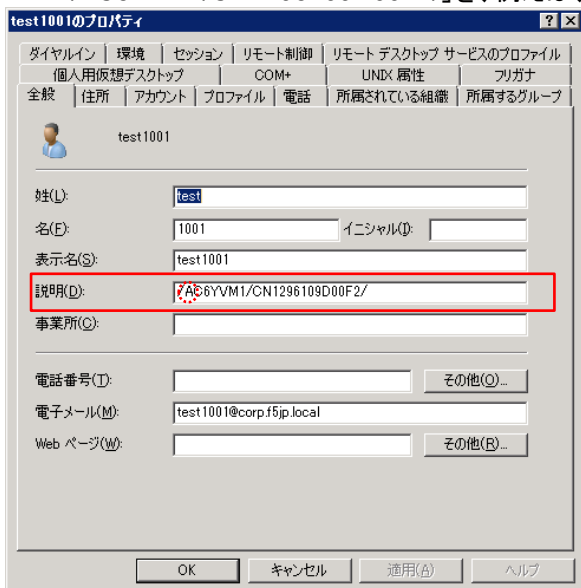
「Apply Access Policy」をクリックして、設定を適用します。



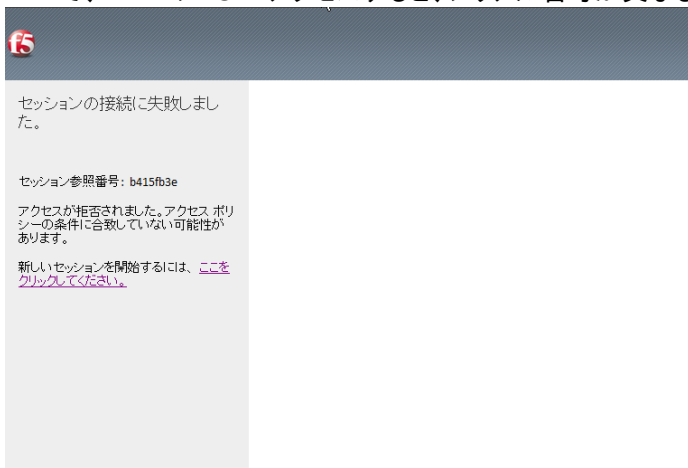
6.6.3. クライアントからのアクセス

(1) マザーボードシリアル番号:「/BC6YVM1/CN1296109D00F2/」を持つクライアント PC から、"test1001"で、APM の VS へアクセスし、アクセスができることを確認します。

(2) Active Directory のユーザ: "test1001"の「説明」フィールドに記載されたマザーボードシリアル番号: 「/BC6YVM1/CN1296109D00F2/」を、例えば、「/AC6YVM1/CN1296109D00F2/」に変更してみます。



- (3) もう一度、マザーボードシリアル番号:「/BC6YVM1/CN1296109D00F2/」を持つクライアント PC から、"test1001" で、APM の VS へアクセスすると、シリアル番号が異なるので、接続ができなくなります。



本製品は、FS Networksからライセンスが付与されています。© 1999-2013 FS Networks. All rights reserved.

6.7. [VPE サンプル-4] クライアント OS の種類に応じてポリシーを変える

クライアント OS 毎にポリシーを変更したい、という要件があると仮定します。

本例では、Windows クライアントには、[VPE サンプル-3]で設定したポリシーを適用し、iOS(Apple iPhone/iPad)にはそれとは異なるポリシーを適用する、という設定を行います。

(1) ここまでの設定では、以下の状態になっています。

「Machine Info」前の「+」をクリックします。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(2) 「Endpoint Security (Server-Side)」タブで、「Client OS」を選択し、「Add Item」ボタンを押します。

Begin typing to search

Logon Authentication Assignment **Endpoint Security (Server-Side)** Endpoint Security (Client-Side) General Purpose

- Client for MS Exchange Check for client for MS Exchange Server, such as MS Outlook, etc. This action requires an Exchange profile
- Client OS** Create branch rules for different operating systems
- Client Type Determine whether the user is connecting via a full or mobile browser, F5 MAM Client, Edge Client, Edge Portal, Citrix Receiver or VMware View client.
- Client-Side Capability Determine if the client is capable of running ActiveX controls or other plug-ins
- Date Time Create branch rules based on day or time
- IP Geolocation Match Determine user's geographic location
- IP Reputation Check Client's IP Reputation
- IP Subnet Match Create policy branch rules based on user's subnet
- Jailbroken or Rooted Device Detection Detect jailbroken or rooted mobile devices

Cancel **Add Item** Help

click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(3) そのまま、「Save」ボタンを押します。

Apply Access Policy

Access Policy: /Common/NetAccess-001

Name: Client OS

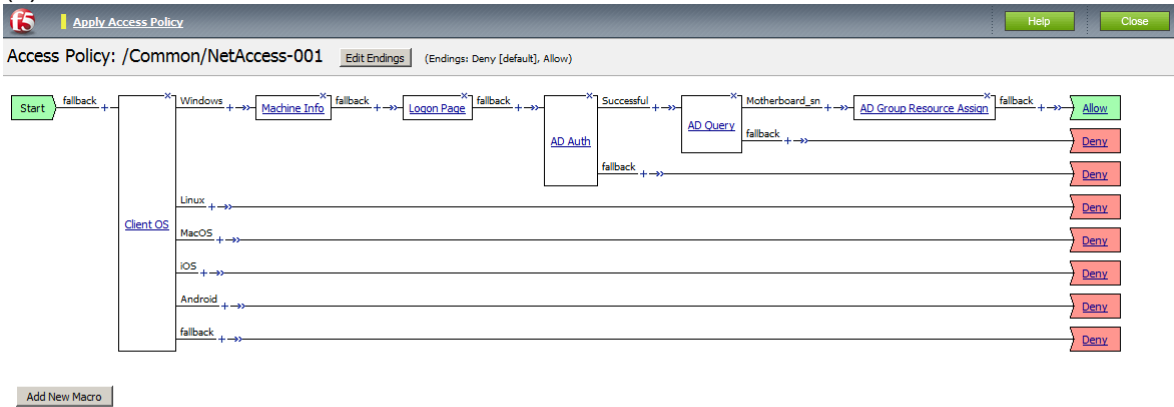
Cancel **Save** Help

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(4) 以下の状態になります。

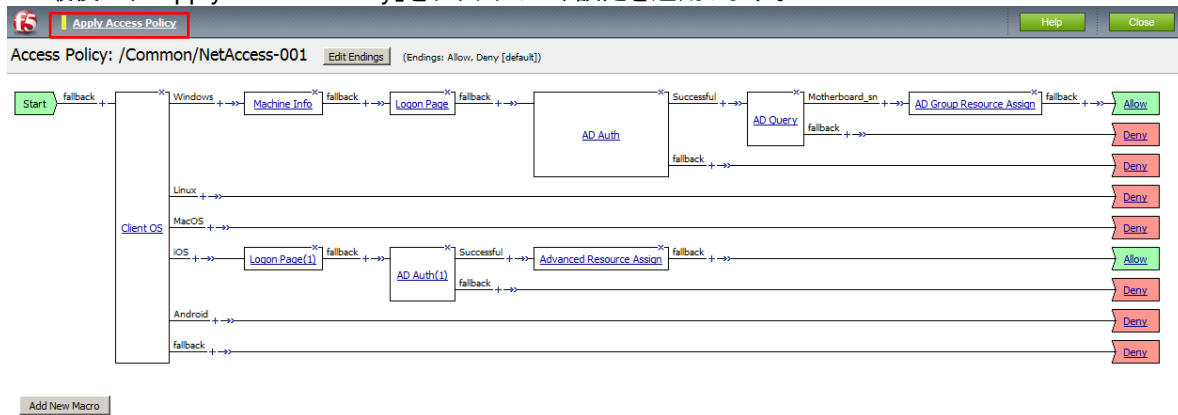


An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(5) iOS 設定には、「Logon Page」、「AD Auth」、「Advanced Resource Assign」のみ追加してみました。最後に、「Apply Access Policy」をクリックして、設定を適用します。



An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

この設定によって、クライアント OS 毎に異なるポリシーを適用することができます。

6.8. [VPE サンプル-5] マクロを使う

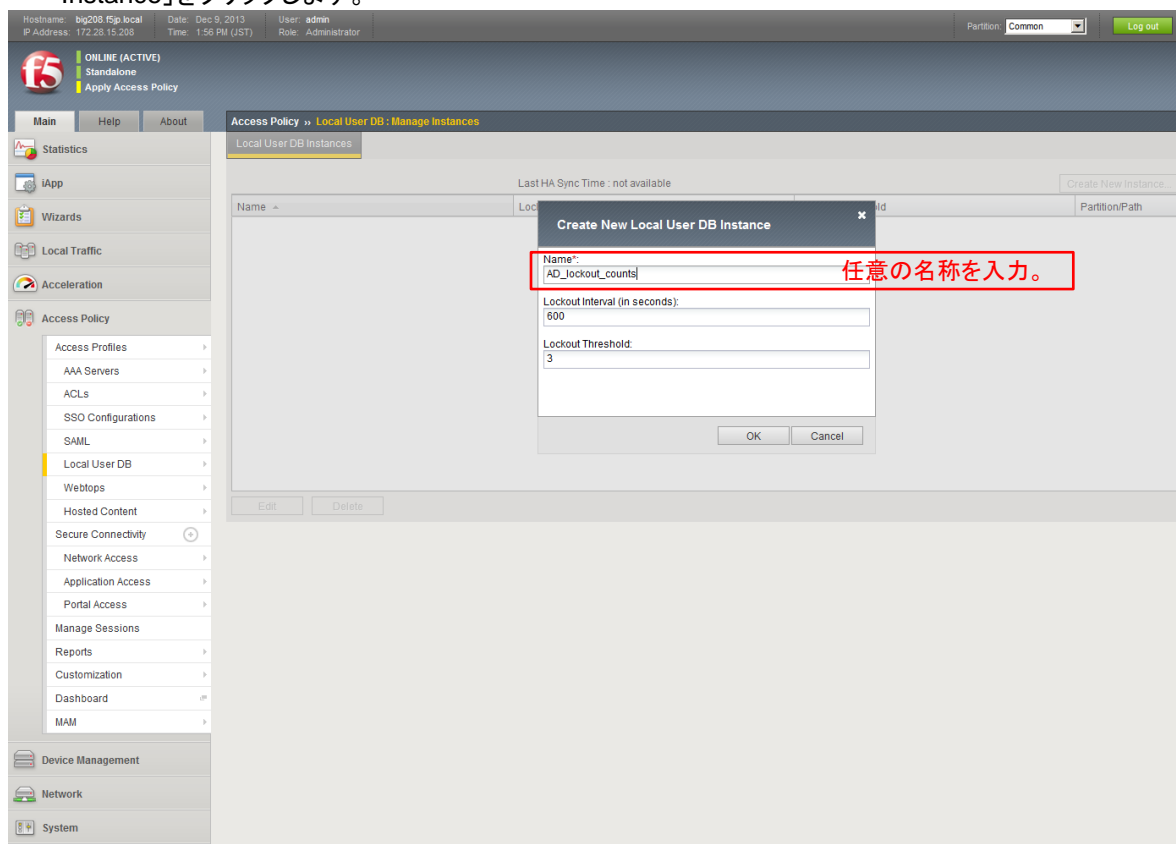
VPE には、マクロ機能があります。繰り返し利用されるポリシーをマクロ化して再利用する、またはデフォルトで用意されている便利なマクロを利用することもできます。

ここでは、以下 2 つの要件に対して、デフォルトで用意されているマクロを利用する例を示します。

- ① Active Directory 認証の誤り回数をカウントしたい。
さらに指定回数を超えたらロックし、ロック解除するまで使えないようにしたい。
- ② Android と iOS は同じ設定なので、一つの設定にまとめたい。

6.8.1. AD 認証の誤り回数カウント

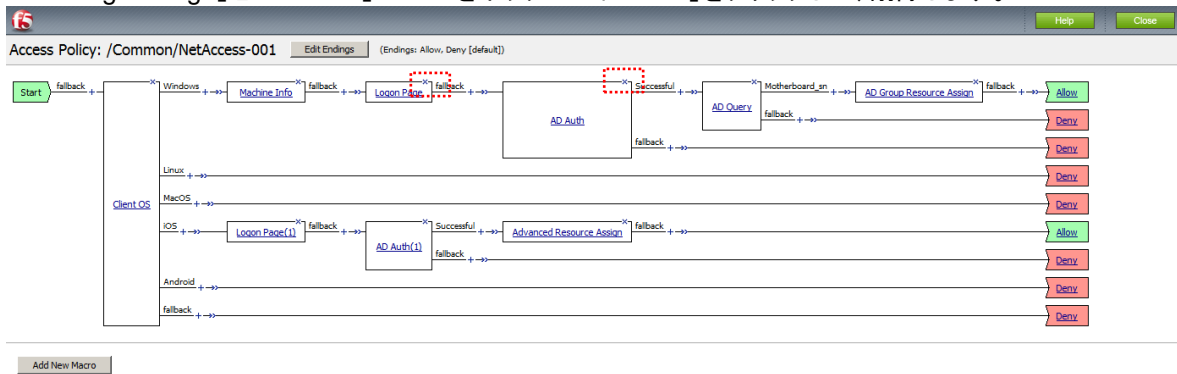
- (1) まず、ユーザエントリの存在しない、空の Local User DB の Instance を作ります。
「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Instances」で、左上の「Create New Instance」をクリックします。



(2) VPE 設定に戻ります。

ここまでの設定では、以下の状態になっています。

「Logon Page」と「AD Auth」の 2 つをボックスの右上「×」をクリックして、削除します。



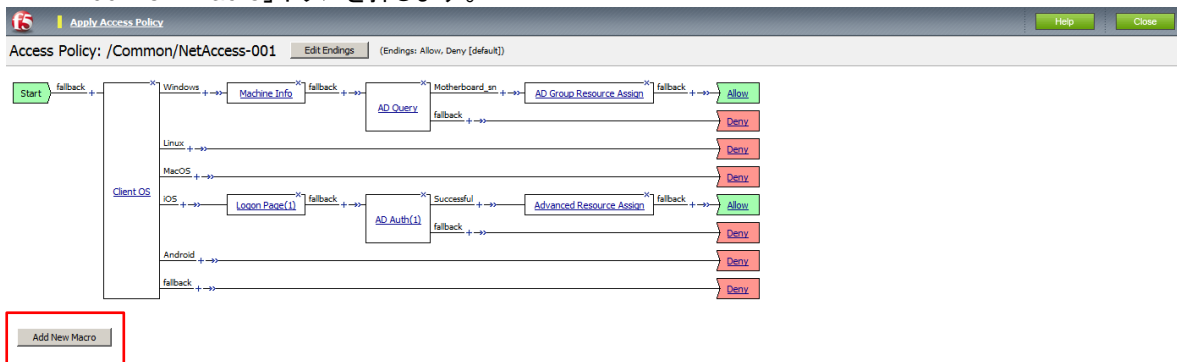
An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(3) 以下の状態になります。

「Add New Macro」ボタンを押します。

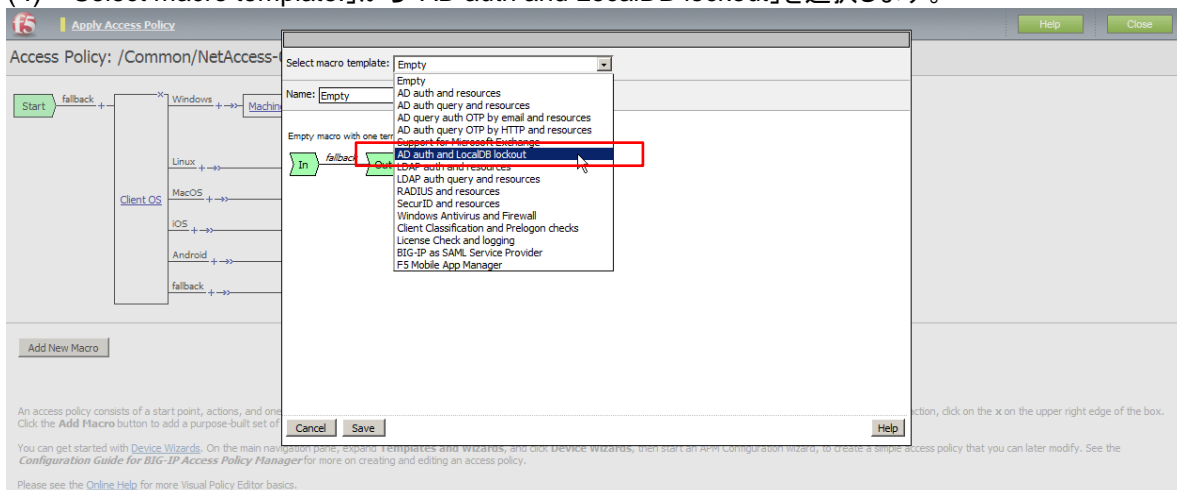


An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(4) 「Select macro template:」から「AD auth and LocalDB lockout」を選択します。



An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(5) 以下の画面が現れますので、「Save」ボタンを押します。

The screenshot shows the 'Visual Policy Editor' interface. A macro template window is open, titled 'AD auth and LocalDB lockout'. The flowchart shows a sequence of actions: 'Logon Page' (with an 'In' terminal), 'LocalDB - Read', 'User Locked Out', 'Logging', 'AD Auth', 'LocalDB - Write (Reset)', and 'LocalDB - Write (Incr)'. The 'Save' button at the bottom of the window is highlighted with a red rectangle. Below the window, there is a 'Cancel' button and a 'Help' button.

(6) 以下の「+」をクリックすると、マクロが展開されます。

The screenshot shows the 'Visual Policy Editor' with the macro 'AD auth and LocalDB lockout' expanded. The flowchart shows the macro's internal logic, including actions like 'Machine Info', 'AD Query', 'Motherboard_sn', 'AD Group Resource Assign', 'Logon Page(1)', 'AD Auth(1)', 'Successful', and 'Advanced Resource Assign'. The '+' icon next to the macro name in the left sidebar is highlighted with a red box.

(7) 「*」部分は、現在、設定が不十分であることを表しています。以降、「*」の部分を設定していきます。

The screenshot shows the 'Visual Policy Editor' with the macro 'AD auth and LocalDB lockout' expanded. The flowchart shows the macro's internal logic, including actions like 'LocalDB - Read', 'AD Auth', 'LocalDB - Write (Reset)', and 'LocalDB - Write (Incr)'. The asterisks (*) next to these actions indicate that they are not fully configured. The 'LocalDB - Read' and 'AD Auth' actions are highlighted with red boxes.

(8) 「LocalDB - Read」をクリックすると、以下の画面が現れます。

設定した DB インスタンス: AD_lockout_counts を選択し、「Save」ボタンを押します。

The screenshot shows the 'Apply Access Policy' window with the 'LocalDB - Read' macro selected. The 'Local Database' section is expanded, showing the following configuration:

LocalDB Instance	User Name	Allow User Creation
/Common/AD_lockout_counts	session.logon.last.username	No

The 'Action' table is as follows:

Action	Destination	Source
1 Read	Session Variable: session.localdb.locked_out	DB Property: locked_out

The 'Save' button is highlighted with a red box. A message at the bottom of the window reads: "Data in tab has been changed, please don't forget to save".

(9) 「AD Auth」をクリックすると、以下の画面が現れます。

設定済みの Active Directory 設定を選択し、「Save」ボタンを押します。

The screenshot shows the 'Apply Access Policy' window with the 'AD Auth' macro selected. The 'Active Directory' section is expanded, showing the following configuration:

Type	Server	Cross Domain Support	Complexity check for Password Reset	Show Extended Error	Max Logon Attempts Allowed	Max Password Reset Attempts Allowed
Authentication	/Common/NetAccess-001_aaa_srvr	Disabled	Disabled	Disabled	1	3

The 'Save' button is highlighted with a red box. A message at the bottom of the window reads: "Data in tab has been changed, please don't forget to save".

(10) 「LocalDB - Write (Reset)」をクリックすると、以下の画面が現れます。

設定した DB インスタンス: AD_lockout_counts を選択し、「Save」ボタンを押します。

Properties* Branch Rules
Access Policy: /Common
Name: LocalDB - Write (Reset)

Local Database
LocalDB Instance: /Common/AD_lockout_counts
User Name: session.logon.last.username
Allow User Creation: Yes

Add new entry Insert Before: 1

Action	Destination	Source
1 Write	DB Property: login_failures	Expression: expr ("0")

Cancel Save *Data in tab has been changed, please don't forget to save Help

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an **APM Configuration wizard**, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(11) 「LocalDB - Write (Incr)」をクリックすると、以下の画面が現れます。

設定した DB インスタンス: AD_lockout_counts を選択し、「Save」ボタンを押します。

Properties* Branch Rules
Access Policy: /Common
Name: LocalDB - Write (Incr)

Local Database
LocalDB Instance: /Common/AD_lockout_counts
User Name: session.logon.last.username
Allow User Creation: Yes

Add new entry Insert Before: 1

Action	Destination	Source
1 Read	Session Variable: session.localdb.login_failures	DB Property: login_failures
2 Write	DB Property: login_failures	Expression: expr ([mcget (session.localdb.login_failures)])

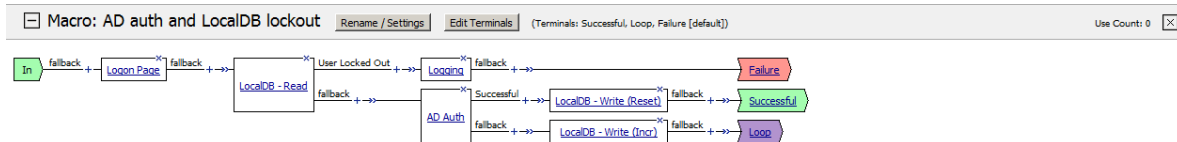
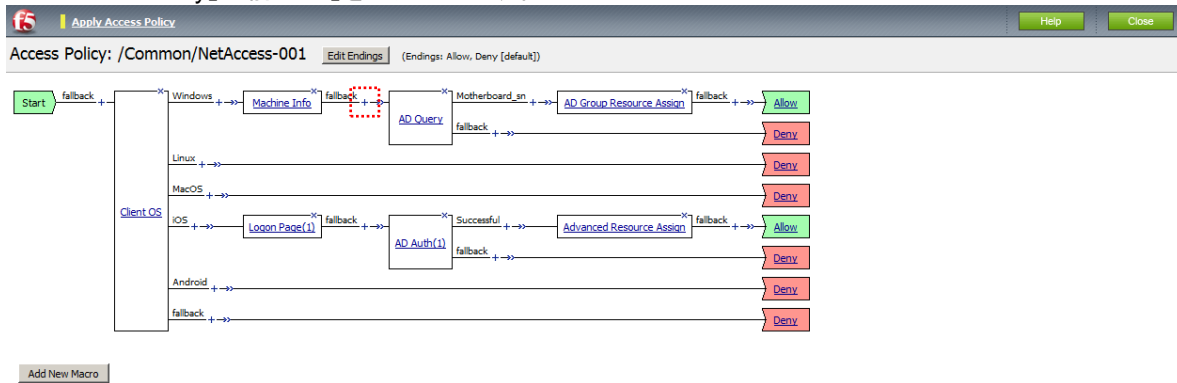
Cancel Save *Data in tab has been changed, please don't forget to save Help

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an **APM Configuration wizard**, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(12) 本サンプルでは、「AD Query」の前に、マクロを入れることにします。
「AD Query」の前の「+」をクリックします。



An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

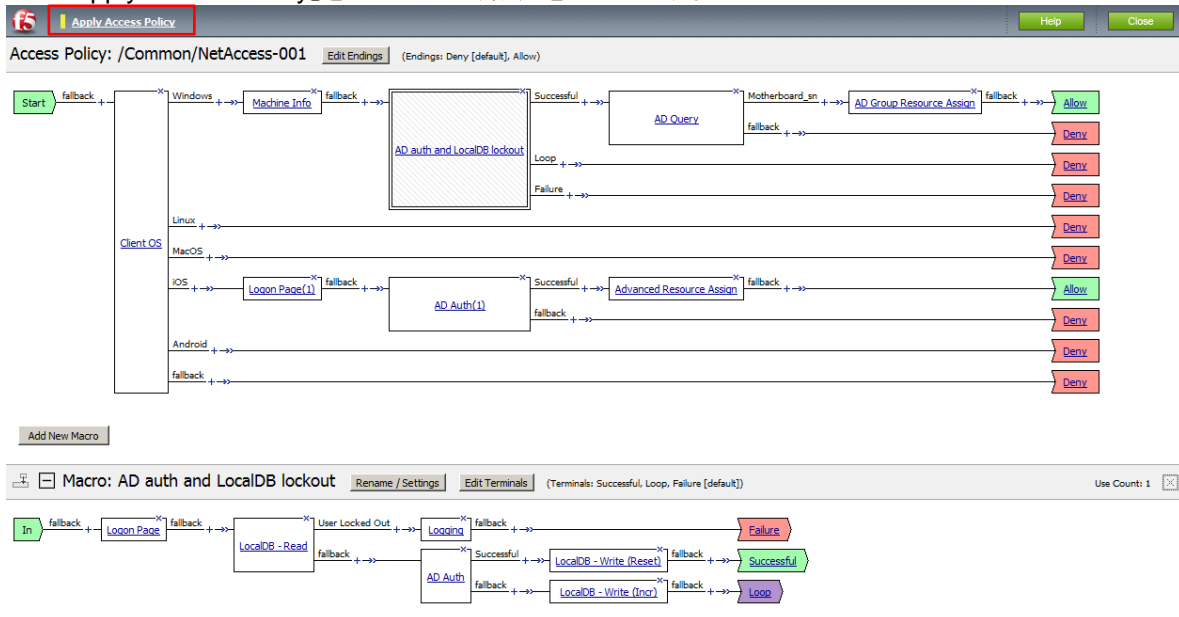
(13) 「Macrocalls」タブで、設定した「Ad auth and LocalDB locout」を選択し、「Add Item」ボタンを押します。

An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

(14) 以下の状態になります。
「Apply Access Policy」をクリックして、設定を適用します。



An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

6.8.1.1. クライアントからのアクセス

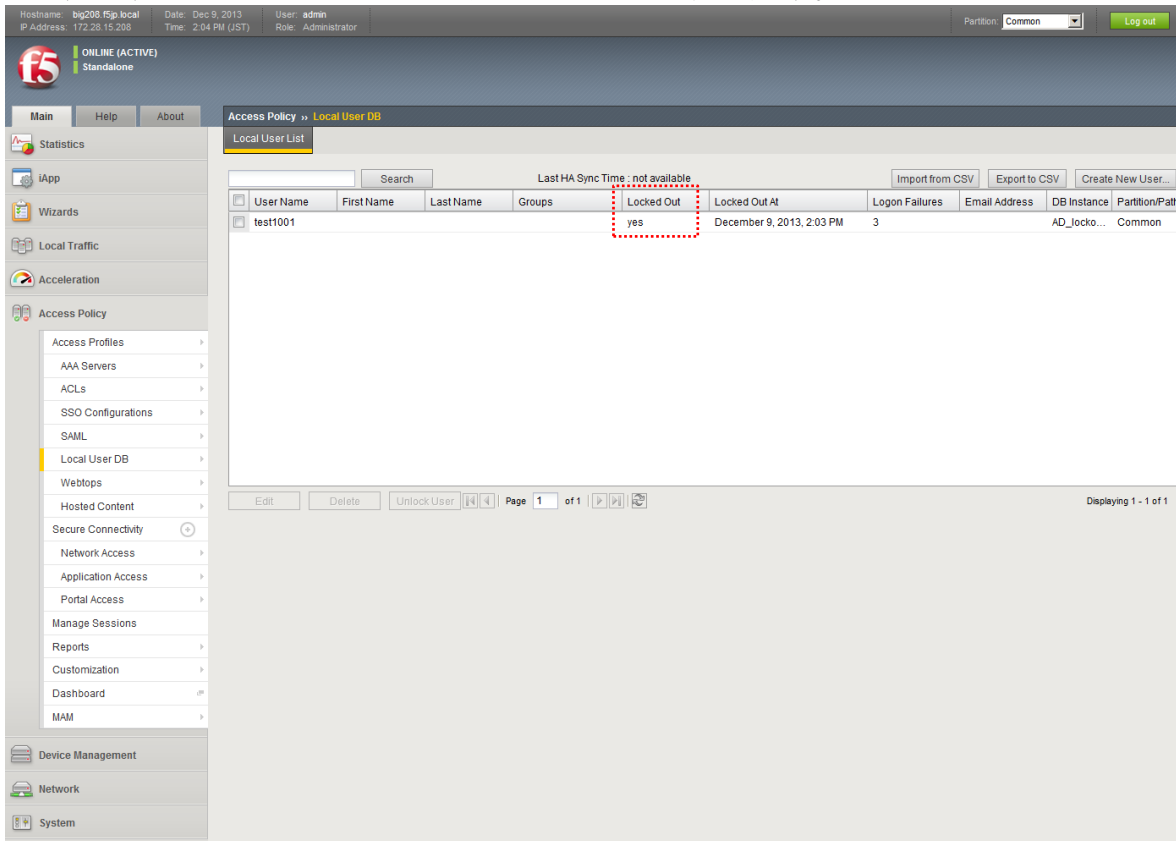
(1) まずは、クライアント PC から正しい ID とパスワード(test1001/test1001)でアクセスしてみます。
「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Users」を確認します。
すると、ユーザ: test1001 がエントリされていることが分かります。

User Name	First Name	Last Name	Groups	Locked Out	Locked Out At	Logon Failures	Email Add	DB Instance	Partition/Path
test1001			no	N/A		0		AD_lockout_counts	Common

- (2) 今度は、誤ったパスワードで、3 回程度アクセスしてみます。
 以下のように、アクセスが拒否されたメッセージが表示されます。



- (3) 「Main」メニュー → 「Access Policy」 → 「Local User DB」 → 「Manage Users」を確認します。
 すると、ユーザ: test1001 がロックアウトされていることが分かります。



- (4) ロックされたユーザのロック解除

V11.4.1(HF1 含む)では、GUI からのロック解除ができず、コマンドラインで実施する必要があります。

(詳細は以下 SOL を参照ください)

<http://support.f5.com/kb/en-us/solutions/public/14000/700/sol14746.html>

- ① SSH で BIG-IP へログイン(デフォルト ID/Pass: root/default)
- ② 以下のコマンドを実行。(赤文字部分のみ変更してご利用ください。)

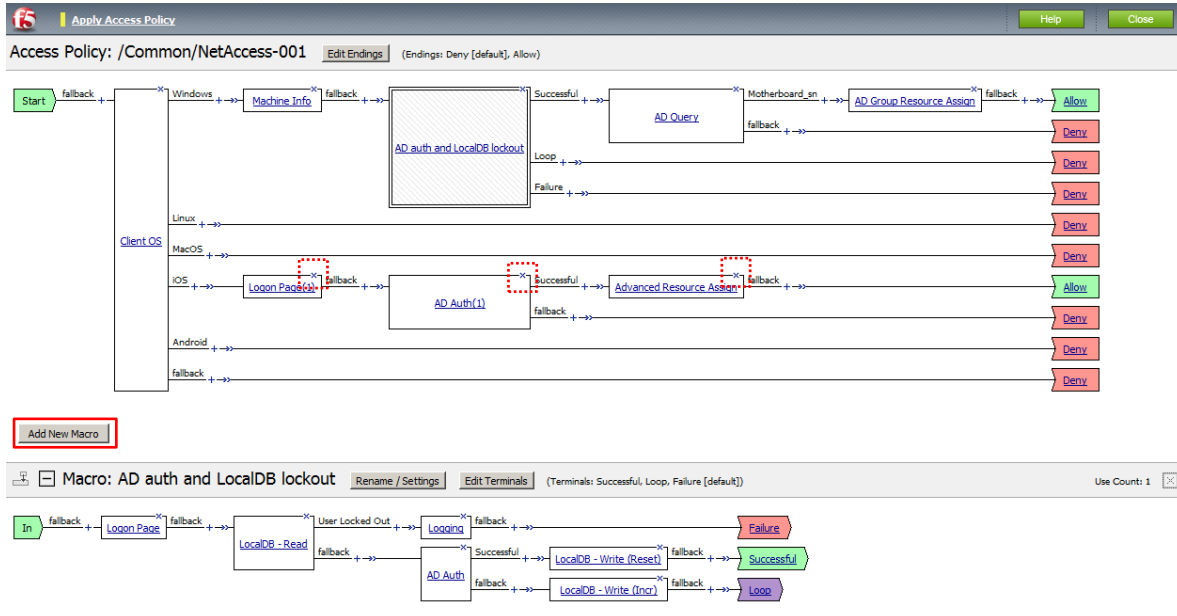
```
[root@big208:Active:Standalone] config # ldbutil --update --uname=test1001
--instance=/Common/AD_lockout_counts --locked_out=0 --lockout_start=0 --login_failures=0
```

6.8.2. 同じ設定をまとめる

ご要件として、iOS と Android は同じ設定を行う、と仮定します。

iOS と Android それぞれに同じ設定を追加しても全く問題はないのですが、見た目上、少し煩雑になります。そこで、ここではサンプルとして、共通のマクロを生成して、それを再利用する、という設定を行ってみます。

- (1) ここでは一旦、iOS の分岐上にあるボックス全てを削除します。
その後、「Add New Macro」ボタンをクリックします。

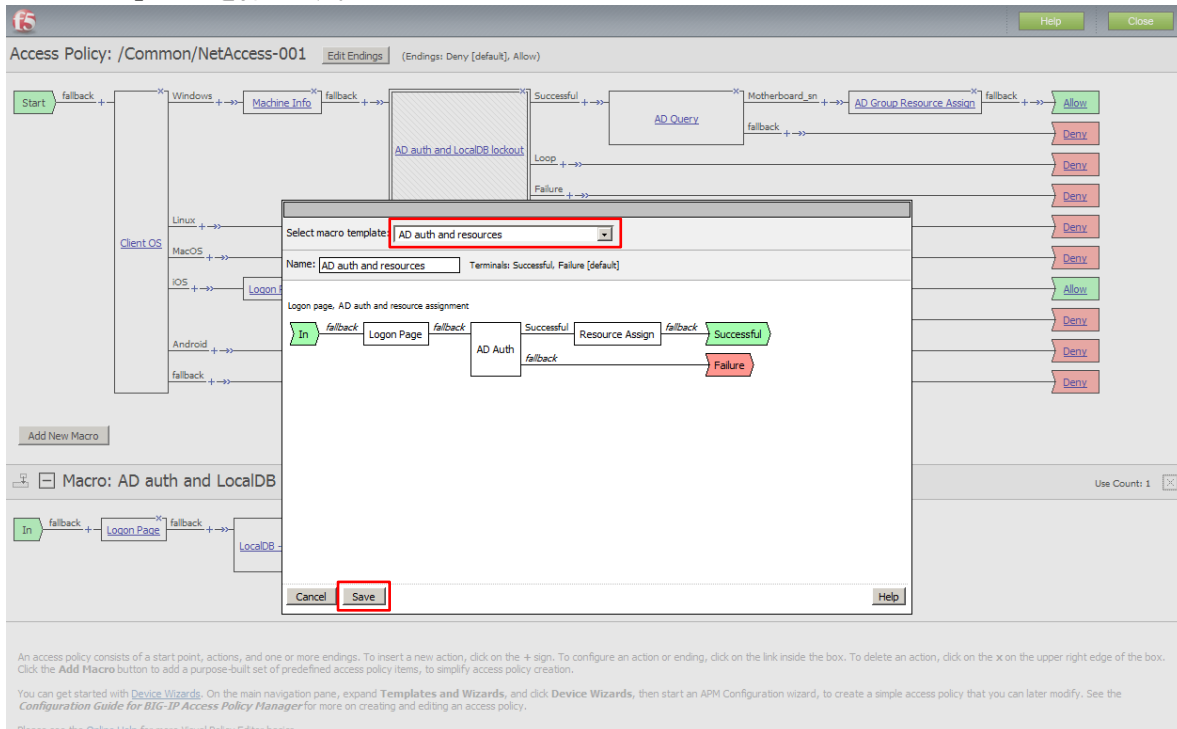


An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the Add Macro button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

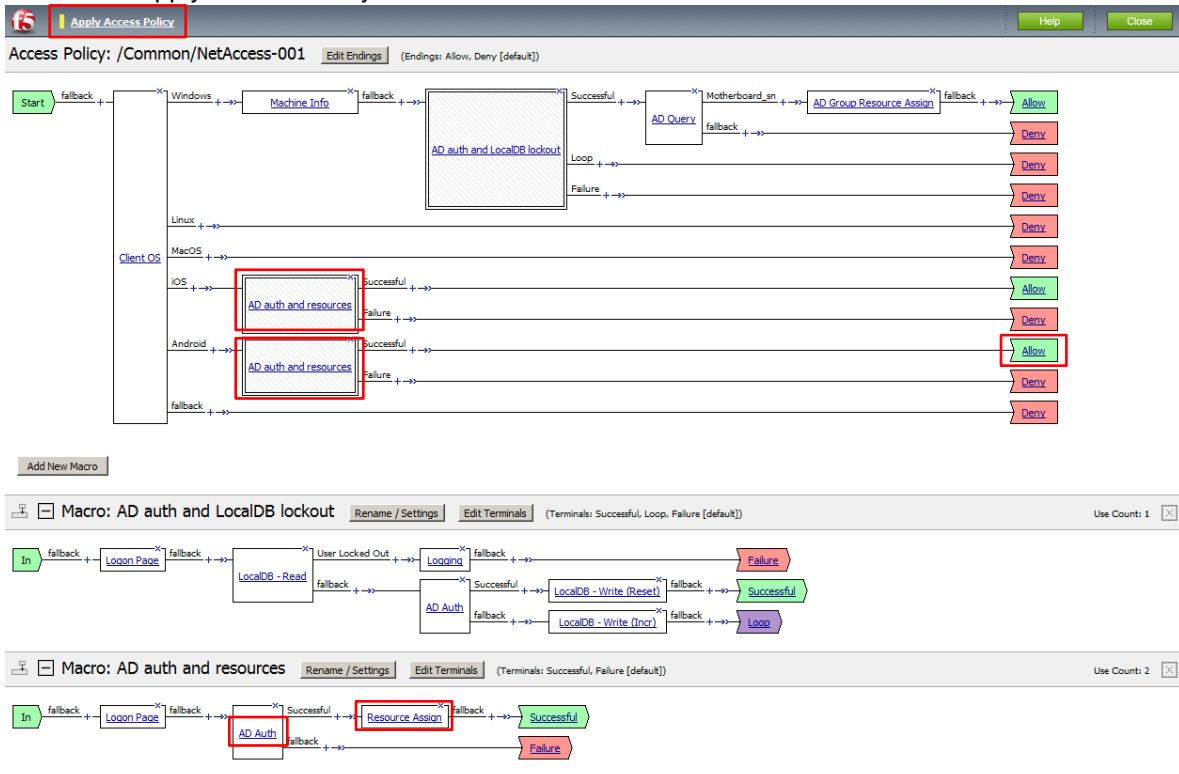
Please see the [Online Help](#) for more Visual Policy Editor basics.

- (2) ここでは、サンプルとして、「AD auth and resources」を選択してみました。
「Save」ボタンを押します。



- (3) 追加したマクロ:「AD Auth and resources」の「*」マークの付いたボックス:「AD Auth」と「Resource Assign」をそれぞれ設定します。
その後、iOS と Android の分岐の「+」をクリックして、そのマクロを追加します。

AndroidはEndingが「Deny」になっているので、「Allow」に変更します。
最後に「Apply Access Policy」をクリックして、設定を適用します。



An access policy consists of a start point, actions, and one or more endings. To insert a new action, click on the + sign. To configure an action or ending, click on the link inside the box. To delete an action, click on the x on the upper right edge of the box. Click the **Add Macro** button to add a purpose-built set of predefined access policy items, to simplify access policy creation.

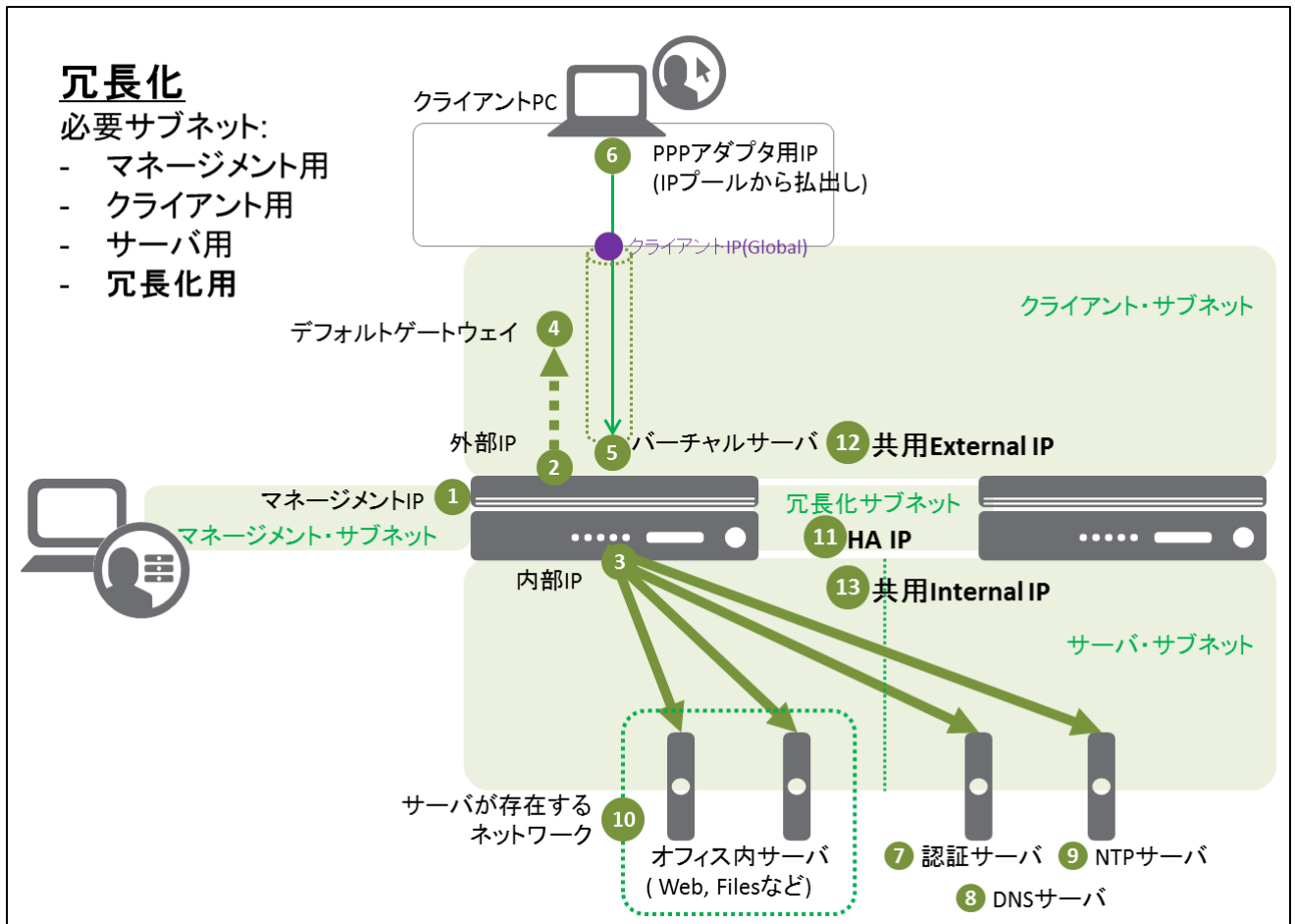
You can get started with [Device Wizards](#). On the main navigation pane, expand **Templates and Wizards**, and click **Device Wizards**, then start an APM Configuration wizard, to create a simple access policy that you can later modify. See the [Configuration Guide for BIG-IP Access Policy Manager](#) for more on creating and editing an access policy.

Please see the [Online Help](#) for more Visual Policy Editor basics.

以上で設定は完了です。

7. 冗長化

7.1. 冗長化イメージ

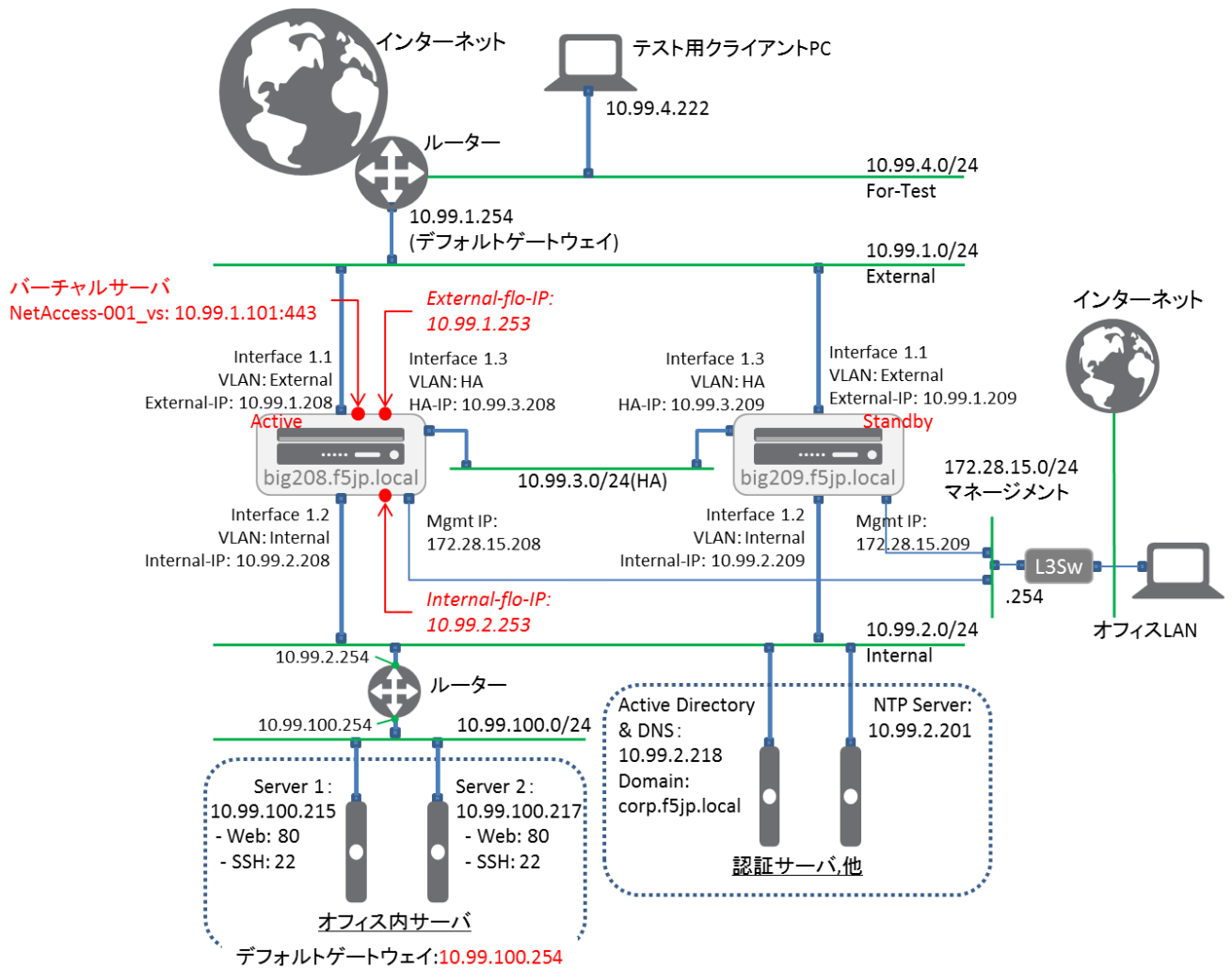


スタンドアロン構成に加え、冗長化用サブネットが必要になります。また、2台で共有し、どちらかがActiveに動作する共有IPアドレスを設定し、サーバのデフォルトGWとして指定します。

項目	名前	値	名前	値
		1号機	2号機	
-	ホスト名	big208.f5jp.local		big209.f5jp.local
①	管理IP	---	---	172.28.15.209/24
②	External インタフェース	external	external	10.99.1.209/24
③	Internal インタフェース	internal	internal	10.99.2.209/24
④	デフォルトゲートウェイ	default-GW		⇒ 設定同期によりコピー
⑤	仮想サーバアドレス	NetAccess-001_vs		⇒ 設定同期によりコピー
⑥	PPP アダプタ用 IP プール	NetAccess-001_ip		⇒ 設定同期によりコピー
⑦	認証サーバ(Active Directory)	NetAccess-001_aaa_srvr		⇒ 設定同期によりコピー
⑧	DNSサーバ(Active Directory)	---		⇒ 設定同期によりコピー
⑨	NTPサーバ	---		⇒ 設定同期によりコピー
⑩	サーバが存在するネットワーク	---		⇒ 設定同期によりコピー
⑪	HA インタフェース	HA	HA	10.99.3.209/24
⑫	共有 External	External-flo-ip		⇒ 設定同期によりコピー
⑬	共有 Internal	Internal-flo-ip		⇒ 設定同期によりコピー

7.2. 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。



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。

7.3. Active 機(big208.f5jp.local)の設定

(1) HA VLAN の設定

「Main」メニュー →「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: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 2:34 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE) Standalone

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

General Properties

Name: HA 名前(任意)を指定。
Description:
Tag:
Resources

Untagged	Available	Tagged
1.3	1.1 1.2	

Interfaces

Configuration: Basic

Source Check:
MTU: 1500

sFlow

Polling Interval: Default Default Value: 10 seconds
Sampling Rate: Default Default Value: 2048 seconds

Cancel Repeat Finished

Network

- Interfaces
- Routes
- Self IPs
- Packet Filters
- Trunks
- Tunnels
- Route Domains
- VLANs**
- ARP
- IPsec
- WCCP

(2) HA VLAN の IP 設定

「Main」メニュー →「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: big208.f5jp.local Date: Jul 23, 2013 User: admin
IP Address: 172.28.15.208 Time: 7:54 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE) Standalone

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

Configuration

Name: HA-ip 名前(任意)、IP アドレス、サブネットマスク、VLAN を設定。
IP Address: 10.99.3.208
Netmask: 255.255.255.0
VLAN / Tunnel: HA
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: Inherit traffic group from current partition / path
traffic-group-local-only (non-floating)

Cancel Repeat Finished

Network

- Interfaces
- Routes
- Self IPs
- Packet Filters
- Trunks
- Tunnels
- Route Domains
- VLANs
- ARP
- IPsec
- WCCP

(3) 一覧は以下のような状態になります。

Hostname: big208.f5jp.local Date: Jul 23, 2013 User: admin
 IP Address: 172.28.15.208 Time: 9:09 PM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Network >> Self IPs

Self IP List Create...

<input type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	HA-ip		10.99.3.208	255.255.255.0	HA	traffic-group-local-only	Common
<input type="checkbox"/>	external-ip		10.99.1.208	255.255.255.0	external	traffic-group-local-only	Common
<input type="checkbox"/>	internal-ip		10.99.2.208	255.255.255.0	internal	traffic-group-local-only	Common

Delete...

(4) 次に、「Main」メニュー →「Device Management」→「Devices」で、自分自身 :big208.f5jp.local(self)を選択します。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
 IP Address: 172.28.15.208 Time: 3:01 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management >> Devices

Device List

Search

Status	Name	Address	Hostname	Version
	big208.f5jp.local (Self)	172.28.15.208	big208.f5jp.local	BIG-IP v11.4.0 (Build 142.0)

Overview Devices Device Groups Device Trust Traffic Groups

- (5) 「Device Connectivity」プルダウンメニューから「ConfigSync」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: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:01 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management » Devices » big208.f5jp.local

Statistics iApp Local Traffic Acceleration Device Management Overview Devices Device Groups Device Trust Traffic Groups Network System

Device Connectivity

ConfigSync Configuration

Local Address 10.99.3.208 (HA) HA VLAN に設定した IP アドレスを選択。

Update

- (6) 「Device Connectivity」プルダウンメニューから「Failover」を選択し、「Add」ボタンを押します。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:04 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management » Devices » big208.f5jp.local

Statistics iApp Local Traffic Acceleration Device Management Overview Devices Device Groups Device Trust Traffic Groups Network System

Device Connectivity

Failover Unicast Configuration

Local Address Add...

No records to display.

Delete

Failover Multicast Configuration

Use Failover Multicast Address Enabled

Update

(7) HA VLAN に設定した IP アドレスを選択します。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:04 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management » Devices » big208.f5jp.local

Statistics
iApp
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Network
System

New Failover Unicast Address

Address: 10.99.3.208 (HA) HA VLAN に設定した IP アドレスを選択。
Port: 1026

Cancel Repeat Finished

(8) 「Device Connectivity」プルダウンメニューから「Mirroring」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。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:04 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management » Devices » big208.f5jp.local

Properties Device Connectivity

Mirroring Configuration

Primary Local Mirror Address: 10.99.3.208 (HA) Primary には HA VLAN に設定した IP アドレスを選択。
Secondary Local Mirror Address: 10.99.2.208 (Internal) Secondary は任意(ここでは Internal VLAN を選択)。

Update

7.4. Standby 機(big209.f5jp.local)の設定

(1) Active 機での VLAN, Self IP, Devices の設定と同様の設定を Standby 機に対しても行います。

(2) Standby 機に設定された VLAN は以下のようになります。

The screenshot shows the F5 configuration interface for the Standby machine (big209.f5jp.local). The 'VLANs : VLAN List' page is displayed, showing a table of configured VLANs. A red box highlights the table content.

<input checked="" 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

(3) Standby 機に設定された Self IP アドレスは以下のようになります。

The screenshot shows the F5 configuration interface for the Standby machine (big209.f5jp.local). The 'Self IP List' page is displayed, showing a table of configured Self IP addresses. A red box highlights the table content.

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	HA-ip		10.99.3.209	255.255.255.0	HA	traffic-group-local-only	Common
<input type="checkbox"/>	external-ip		10.99.1.209	255.255.255.0	external	traffic-group-local-only	Common
<input type="checkbox"/>	internal-ip		10.99.2.209	255.255.255.0	internal	traffic-group-local-only	Common

- (4) 次に、「Main」メニュー →「Device Management」→「Devices」で、自分自身: big209.f5jp.local(self)を選択し、Active 機同様に、Device Connectivity の設定を行います。
以下は ConfigSync 設定。

The screenshot shows the F5 configuration interface. At the top, it displays system information: Hostname: big209.f5jp.local, Date: May 14, 2013, Time: 3:08 AM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation bar includes Main, Help, About, and Device Management >> Devices >> big209.f5jp.local. The left sidebar contains various menu items like Statistics, iApp, Local Traffic, Acceleration, Device Management (Overview, Devices, Device Groups, Device Trust, Traffic Groups), Network, and System. The main content area is titled 'ConfigSync Configuration' and has a 'Device Connectivity' dropdown menu. Below this, there is a 'Local Address' dropdown menu with '10.99.3.209 (HA)' selected. A red box highlights this dropdown, with a red text label 'HA VLAN の IP アドレスを選択。' (Select HA VLAN IP address). An 'Update' button is located below the dropdown.

- (5) Failover 設定。

The screenshot shows the F5 configuration interface for Failover settings. At the top, it displays system information: Hostname: big209.f5jp.local, Date: May 14, 2013, Time: 3:08 AM (JST), User: admin, Role: Administrator, Partition: Common, and a Log out button. The main navigation bar includes Main, Help, About, and Device Management >> Devices >> big209.f5jp.local. The left sidebar contains various menu items like Statistics, iApp, Local Traffic, Acceleration, Device Management (Overview, Devices, Device Groups, Device Trust, Traffic Groups), Network, and System. The main content area is titled 'New Failover Unicast Address'. It has an 'Address:' dropdown menu with '10.99.3.209 (HA)' selected, and a 'Port:' text input field with '1026' entered. A red box highlights the 'Address:' dropdown, with a red text label 'HA VLAN の IP アドレスを選択。' (Select HA VLAN IP address). Below the form are 'Cancel', 'Repeat', and 'Finished' buttons.

(6) Mirroring 設定。

Hostname: big209.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.209 Time: 3:08 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management >> Devices >> big209.f5jp.local

Statistics
iApp
Local Traffic
Acceleration
Device Management
 Overview
 Devices
 Device Groups
 Device Trust
 Traffic Groups
Network
System

Properties Device Connectivity

Mirroring Configuration

Primary Local Mirror Address	10.99.3.209 (HA)
Secondary Local Mirror Address	10.99.2.209 (internal)

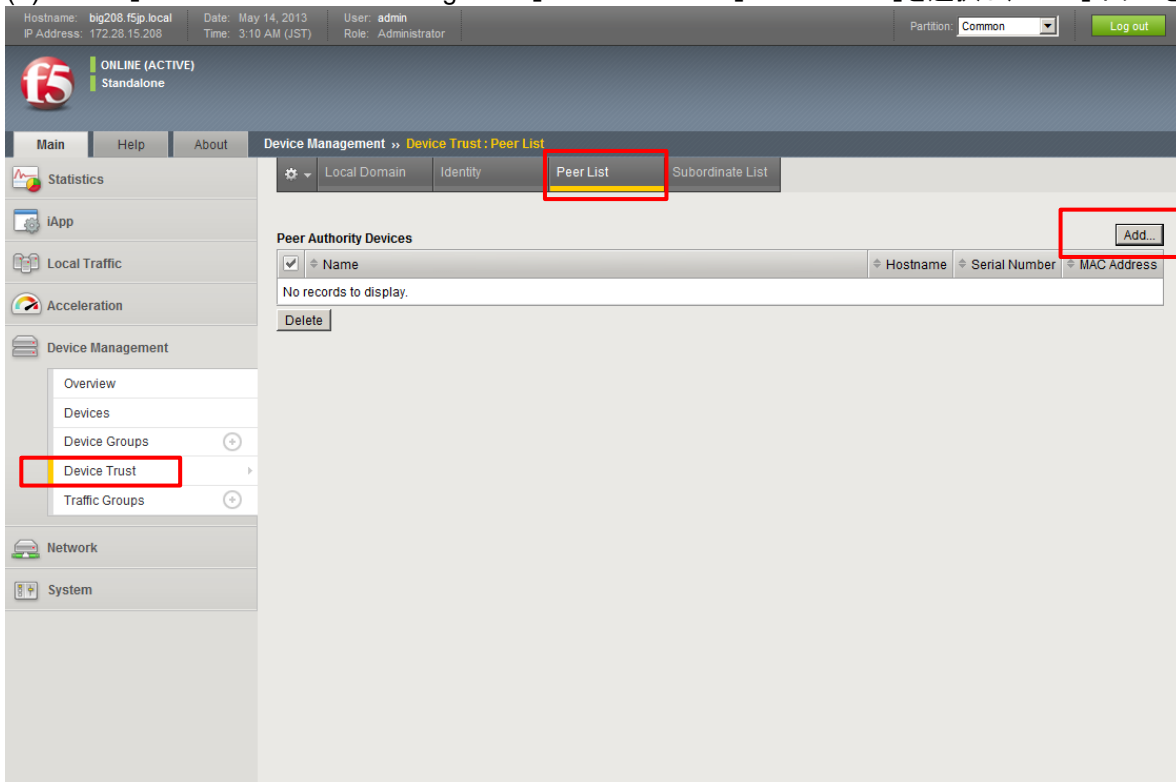
Update

Primary には HA VLAN に設定した IP アドレスを選択。
Secondary は任意(ここでは Internal VLAN を選択)。

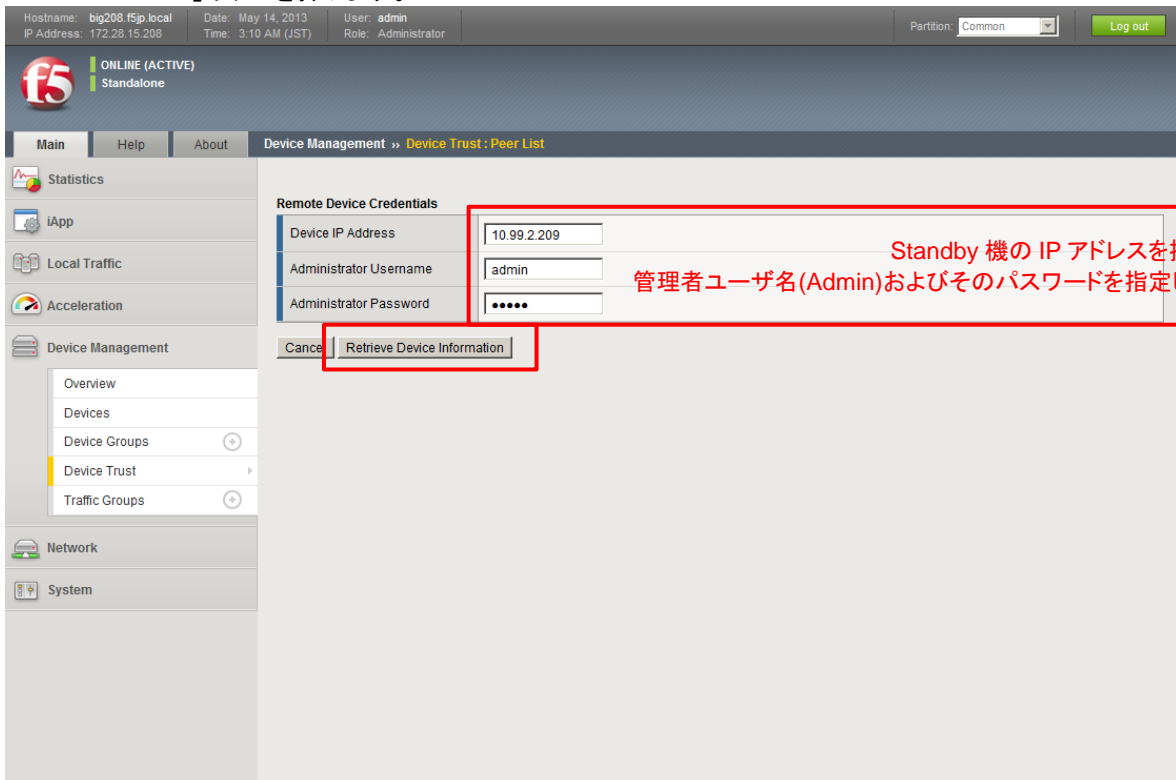
7.5. デバイストラスト設定 (Active 機:big208.f5jp.local 側から実施)

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:big208.f5jp.local からのみ、設定します。

(1) 「Main」メニュー → 「Device Management」→ 「Device Trust」→ 「Peer List」を選択し、「Add」ボタンを押します。



(2) Standby 機:big209.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。



(3) Standby 機 big209.f5jp.local の証明書情報が表示されます。「Finished」ボタンを押して終了します。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:26 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
Standalone

Main Help About Device Management » Device Trust : Peer List

Statistics
iApp
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Network
System

Remote Device Credentials

Device IP Address	10.99.2.209
Administrator Username	admin
Administrator Password	*****

Device Certificate

Subject	/C=-- /ST=WAL=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	10.99.2.209
Expiration	Sun May 11 15:32:09 JST 2023
Serial Number	fe80b0d2c536a703
Signed	Yes
SHA-1	0fb44f89ba05a199268af3ab97bb2c399afb577b
MD5	2e801a16c1fb1a34767d68422c155ff4

Device Properties

Name	big209.f5jp.local
------	-------------------

Cancel Finished

(4) 承認されたデバイスとして登録された状態です。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:27 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (ACTIVE)
In Sync

Main Help About Device Management » Device Trust : Peer List

Local Domain Identity Peer List Subordinate List

Peer Authority Devices Add...

<input checked="" type="checkbox"/>	Name	Hostname	Serial Number	MAC Address
<input type="checkbox"/>	big209.f5jp.local	big209.f5jp.local	564d7ba2-82c6-15b9-9c688cbeb1a1	0:c:29:be:b1:a1

Delete

- (5) 「Device Management」→「Devices」で見ると、(self)に加え、Standby 機:big209.f5jp.local も表示されます。
(ここは確認のみです。)

The screenshot shows the F5 BIG-IP web interface. At the top, the status is 'ONLINE (ACTIVE) In Sync'. The user is 'admin' with the role of 'Administrator'. The interface is divided into a left sidebar and a main content area. The sidebar contains navigation menus for Statistics, iApp, Local Traffic, Acceleration, Device Management, Network, and System. The 'Device Management' menu is expanded, showing 'Overview', 'Devices', 'Device Groups', 'Device Trust', and 'Traffic Groups'. The 'Devices' menu item is selected, and the 'Device List' tab is active in the main content area. A search bar is present above a table listing the devices.

Status	Name	Address	Hostname	Version
	big208.f5jp.local (Self)	172.28.15.208	big208.f5jp.local	BIG-IP v11.4.0 (Build 142.0)
	big209.f5jp.local	172.28.15.209	big209.f5jp.local	BIG-IP v11.4.0 (Build 142.0)

7.6. 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、という組み合わ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) 「Main」メニュー → 「Device Management」→ 「Device Groups」から、デバイスグループを作成します。

名前(任意)を設定。
「Sync-Failover」を選択。

冗長化を行うデバイス(自分自身を含む)を選択。

ネットワークフェイルオーバーを行うので、チェック。

(2) デバイスグループが作られた状態です。

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

7.7. 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。

「Main」メニュー →「Device Management」→「Traffic Groups」を確認します。

- (1) 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。

The screenshot shows the F5 management console interface. At the top, it displays system information: Hostname: big208.f5jp.local, Date: May 14, 2013, Time: 3:29 AM (JST), User: admin, Role: Administrator, and Partition: Common. The main navigation menu includes Main, Help, About, and Device Management. Under Device Management, the 'Traffic Groups' option is selected and highlighted with a red box. The 'Traffic Group List' table is also highlighted with a red box. The table contains one entry: 'traffic-group-1'. A red annotation points to this entry with the text 'デフォルトのトラフィックグループ。' (Default traffic group).

Name	Current Device	Next Active Device	Failover Objects	HA Load Factor	Partition / Path
traffic-group-1	big209.f5jp.local	big208.f5jp.local (Self)	3	1	Common

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

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。

「Main」メニュー →「Network」→「Self IPs」から設定します。

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。

Hostname: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:31 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

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

Configuration

Name	internal-flo-ip	名前(任意)を設定。
IP Address	10.99.2.253	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。

Cancel Repeat Finished

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

Hostname: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:30 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

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

Configuration

Name	external-flo-ip	名前(任意)を設定。
IP Address	10.99.1.253	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。

Cancel Repeat Finished

- (4) 「Main」メニュー→「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: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:32 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

Main Help About Local Traffic » Virtual Servers : Virtual Address List » 10.99.111.101

Statistics iApp Local Traffic
 Network Map
Virtual Servers
 Policies
 Profiles
 iRules
 Pools
 Nodes
 Monitors
 Traffic Class
 Address Translation
 DNS Express Zones
 DNS Caches

Acceleration Device Management Network System

General Properties

Name	10.99.111.101
Partition / Path	Common
Address	10.99.111.101
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)
Availability	<input checked="" type="checkbox"/>
State	Enabled
Auto Delete	<input checked="" type="checkbox"/>

Configuration

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

Update Delete

- (5) 「Main」メニュー→「Device Management」→「Traffic Groups」の Traffic-group-1 をクリック→「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: big208.f5.jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:32 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

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

Statistics iApp Local Traffic Acceleration Device Management
 Overview
 Devices
 Device Groups
 Device Trust
Traffic Groups
 Network System

Properties Failover Objects

Search

Name	Address	Type	Partition / Path
10.99.111.101	10.99.111.101	Virtual Address	Common
external-flo-ip	10.99.1.253	Self IP	Common
internal-flo-ip	10.99.2.253	Self IP	Common

7.8. ConfigSync

Active 機:big208.f5jp.local にのみ行った設定を、Standby 機:big209.f5jp.local に同期するために、ConfigSync を行します。

(1) 「Main」メニュー→「Device Management」→「Overview」を選択します。

Active 機(Big208.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。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:32 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

Main Help About Device Management >> Overview

Statistics
iApp
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Network
System

Device Groups

Name	Sync Status	Number of Devices	Device Group Type	Sync Type
Device-Group-001	Changes Pending	2	Sync-Failover	Manual

Sync Summary

Status	Changes Pending
Summary	Changes pending
Details	Recommended action: Synchronize big208.f5jp.local to group Device-Group-001

Devices

HA Status	Name	Sync Status	Configuration Time
Self	big208.f5jp.local (Self)	Awaiting initial Sync with Changes Pending	5/13/2013 11:31:13
	big209.f5jp.local	Awaiting Initial Sync	no value set

Sync Options

Sync Device to Group
 Sync Group to Device

Overwrite Configuration

Sync

クリック。

(2) 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ます。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
IP Address: 172.28.15.208 Time: 3:33 AM (JST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
In Sync

Main Help About Device Management >> Overview

Statistics
iApp
Local Traffic
Acceleration
Device Management
Overview
Devices
Device Groups
Device Trust
Traffic Groups
Network
System

Device Groups

Name	Sync Status	Number of Devices	Device Group Type	Sync Type
Device-Group-001	In Sync	2	Sync-Failover	Manual

Sync Summary

Status	In Sync
Summary	All devices in the device group are in sync
Details	

Devices

HA Status	Name	Sync Status	Configuration Time
Self	big208.f5jp.local (Self)	In Sync	5/13/2013 11:31:13
	big209.f5jp.local	In Sync	5/13/2013 11:31:13

Sync Options

Sync Device to Group
 Sync Group to Device

Overwrite Configuration

Sync

7.9. Traffic-group-1 の優先度設定

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。したがって、本構成では、Standby にしたい機器 : big209.f5jp.local がこの Traffic-group-1 の Active となっています。

以降、Active 機にしたい機器 : big208.f5jp.local が Traffic-group-1 の Active になるように設定します。

- (1) big209.f5jp.local へ移動し、「Main」メニュー→「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 web interface. At the top, the status is 'ONLINE (ACTIVE) In Sync'. The breadcrumb navigation is 'Device Management >> Traffic Groups >> traffic-group-1'. The 'Properties' tab is selected. The 'General Properties' section contains the following fields:

Name	traffic-group-1				
Partition	Common				
Description					
Current Device	big209.f5jp.local (Self)				
Next Active Device	big208.f5jp.local				
HA Load Factor	1				
MAC Masquerade Address					
Auto Failback	<input type="checkbox"/> Enabled				
Failover Order	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td>/Common big208.f5jp.local big209.f5jp.local</td><td></td></tr></tbody></table>	Enabled	Available	/Common big208.f5jp.local big209.f5jp.local	
Enabled	Available				
/Common big208.f5jp.local big209.f5jp.local					
Floating	Yes				

At the bottom of the configuration area, there are buttons for 'Update', 'Cancel', 'Delete', and 'Force to Standby'. The 'Force to Standby' button is highlighted with a red rectangle.

(2) その結果、big209.f5jp.local が Standby になります。

Hostname: big209.f5jp.local Date: May 14, 2013 User: admin
 IP Address: 172.28.15.209 Time: 3:52 AM (JST) Role: Administrator Partition: Common Log out

f5 ONLINE (STANDBY) In Sync

Main Help About Device Management >> Traffic Groups

Statistics
 iApp
 Local Traffic
 Acceleration
 Device Management
 Overview
 Devices
 Device Groups
 Device Trust
 Traffic Groups
 Network
 System

Traffic Group List

Failover Status

Status	STANDBY
Summary	1/1 standby
Details	

Search Create...

<input checked="" type="checkbox"/>	Name	Current Device	Next Active Device	Failover Objects	HA Load Factor	Partition / Path
<input type="checkbox"/>	traffic-group-1	big208.f5jp.local	big209.f5jp.local (Self)	3	1	Common

Force to Standby... Delete...

(3) big208.f5jp.local は Active になります。

Hostname: big208.f5jp.local Date: May 14, 2013 User: admin
 IP Address: 172.28.15.208 Time: 3:53 AM (JST) Role: Administrator Partition: Common Log out

f5 ONLINE (ACTIVE) In Sync

Main Help About Device Management >> Traffic Groups

Statistics
 iApp
 Local Traffic
 Acceleration
 Device Management
 Overview
 Devices
 Device Groups
 Device Trust
 Traffic Groups
 Network
 System

Traffic Group List

Failover Status

Status	ACTIVE
Summary	1/1 active
Details	active for /Common/traffic-group-1

Search Create...

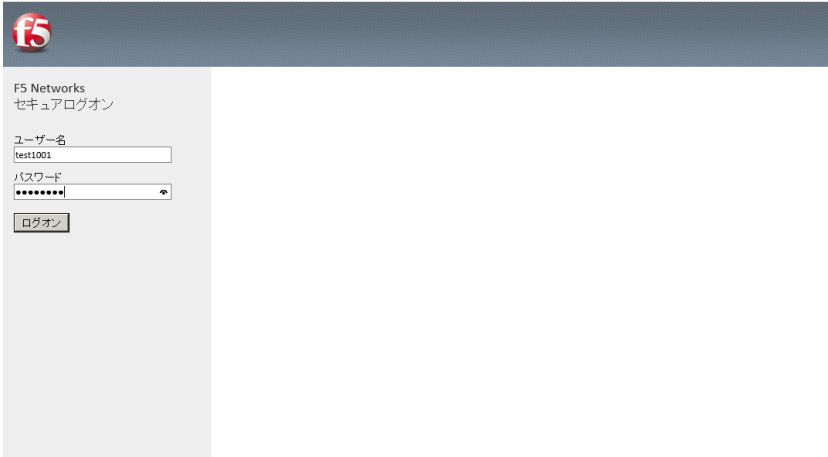
<input checked="" type="checkbox"/>	Name	Current Device	Next Active Device	Failover Objects	HA Load Factor	Partition / Path
<input type="checkbox"/>	traffic-group-1	big208.f5jp.local (Self)	big209.f5jp.local	3	1	Common

Force to Standby... Delete...

以上で冗長化設定は終わりです。

7.10. クライアント PC からのアクセス

クライアント PC から、設定した Virtual Server へのネットワークアクセスが完了することを確認します。



F5 Networks
セキュアログイン

ユーザー名
test1001

パスワード

ログオン

本製品は、F5 Networksからライセンスが付与されています。© 1999-2013 F5 Networks. All rights reserved.

8. おわりに

基本的な APM セットアップに関しては以上で終了となります。

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、サーバ負荷分散はもちろんのこと、広域負荷分散やネットワークファイアウォール機能、Web アプリケーションファイアウォール機能など、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。

詳細は各種 WEB サイトにてご確認いただくか、購入元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

<http://www.f5networks.co.jp/>

F5 Tech Depot: エンジニア向け製品関連情報サイト

<http://www.f5networks.co.jp/depot/>

AskF5: ナレッジベース総合サイト(英語)

<http://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/>

以上