



Starfield SSL Install Manual
for
Multi-Domain & Wildcard
on
Big- IP/F5

ジェイサート株式会社

CSRファイル作成手順

CSRをBIG-IP上で作成する場合は、以下の手順にて行います。

他のシステムにて作成されたサーバ秘密鍵(key), 証明書(Certificate)をインポートする場合はこの項目の手順は不要です。

CSRファイル作成手順(1)

The screenshot shows the BIG-IP WebGUI interface. The browser address bar displays `https://172.28.4.207/xui/`. The page title is "Local Traffic >> SSL Certificates". The "Local Traffic" menu in the left sidebar is highlighted with a red dashed circle and a circled "1". The "Create..." button in the top right corner is also circled with a red dashed circle and a circled "2".

<input checked="" type="checkbox"/>	Name	Contents	Common Name	Organization	Expiration
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Nov 28, 2008 - Nov 21, 2037
<input type="checkbox"/>	default	Certificate & Key	localhost.localdomain	MyCompany	Sep 2, 2019

1. BIG-IP WebGUIにて、Local Traffic → SSL Certificateの画面を開き
2. [Create]ボタンを押します。

CSRファイル作成手順(2)

Local Traffic » SSL Certificates » New SSL Certificate...

General Properties

Name	<input type="text" value="multi-domain-test"/>
------	--

Certificate Properties

Issuer	<input type="text" value="Certificate Authority"/>
Common Name	<input type="text" value="www.sample-a.jp"/>
Division	<input type="text" value="Sample Division"/>
Organization	<input type="text" value="Sample Organization"/>
Locality	<input type="text" value="Minato-ku"/>
State Or Province	<input type="text" value="Tokyo"/>
Country	<input type="text" value="Japan"/> <input type="text" value="JP"/>
E-mail Address	<input type="text" value="admin@sample-a.jp"/>
Challenge Password	<input type="text" value="*****"/>
Confirm Password	<input type="text" value="*****"/>

Key Properties

Size	<input type="text" value="2048"/> bits
------	--

次の画面で適宜値を入力します。

“Name”

BIG-IP上で作成されるファイルおよびCSR
およびKeyにつけられる名前です。

“Common Name”

サーバ証明書の証明対象となるサーバ
名 (FQDN) です。

“Challenge Password”

認証局に署名を依頼する際、およびBIG-
IP上で当該の証明書を利用する際に必要
となるパスワードです。

“Key Properties”

要件に応じて鍵長を設定してください。


最後に[Finished]を押します。

CSRファイル作成手順(3)

Local Traffic » SSL Certificates » Certificate Signing Request

Certificate Signing Request

Request Text	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIDIjCCAgwCAQAwgagExCzAJBgNVBAYTAjE A1UEBxMFVVG9reW8xHDAaBgNVBAoTE1Nhbj BAsTD1NhbXBsZSBEaXZpc2lvdjEYMBYGA. HgYJKoZIhvcNAQkBFhFhZGlpbkBsZWlwb BQADggEPADCCAQoCggEBAOI3ZUwCH7Zboi ZbFaNv80oB02Wj0FeYqlesuHzwYKFAkvLj -----</pre>
Request File	Download multi-domain-test.csr
Certificate Authorities	Digital Signature Trust Company Entrust GlobalSign VeriSign



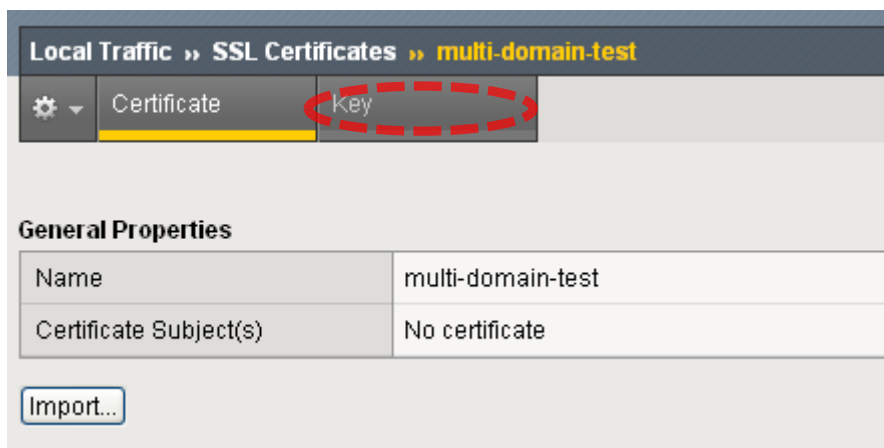
CSRが作成されました。

テキストウィンドウ内のテキストをコピーするが、
[Download xxx.csr]ボタンを押してCSRファイルをダウンロードします。

最後に[Finished]を押します。

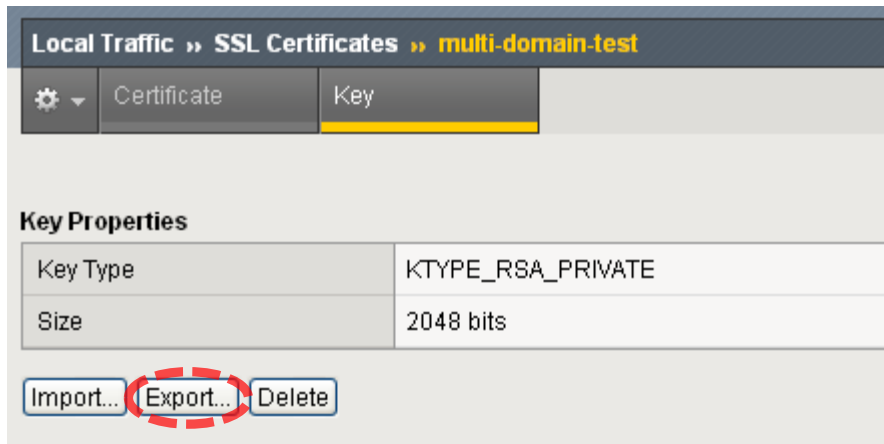
サーバ秘密鍵の保存(バックアップ)

サーバ秘密鍵の保存(1)



作成されたCSRに関する概要が表示されます。

[Key]タブを押します。

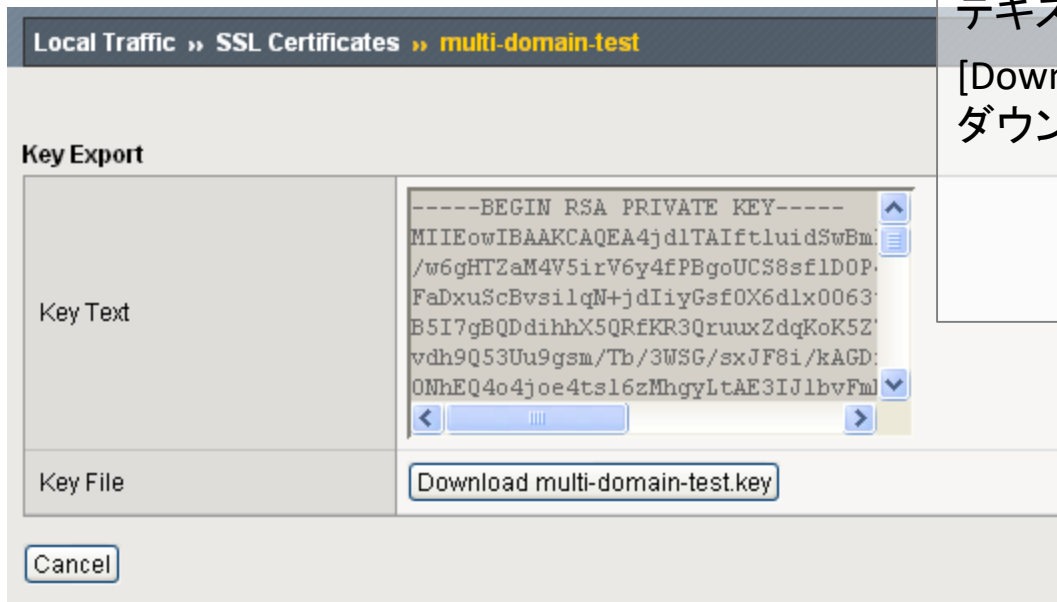


該当するCSRのために生成されたKey(サーバ秘密鍵)に関する概要が表示されます。

他のサーバでの利用やバックアップのためにExportすることができます。

[Export]タブを押します。

サーバ秘密鍵の保存(2)

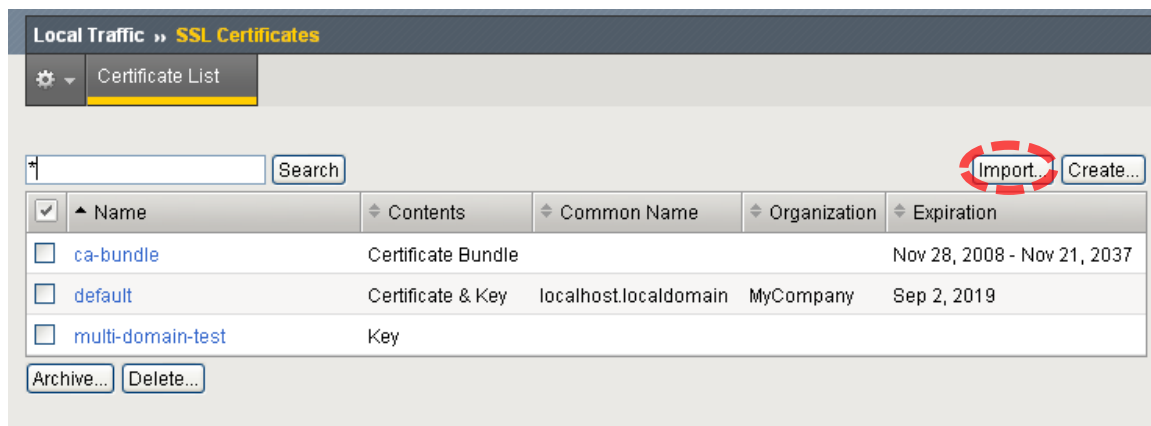


テキストウインドウの中身をコピー、または [Download xxxx.key] ボタンを押してファイルをダウンロードします。

中間証明書インストール手順

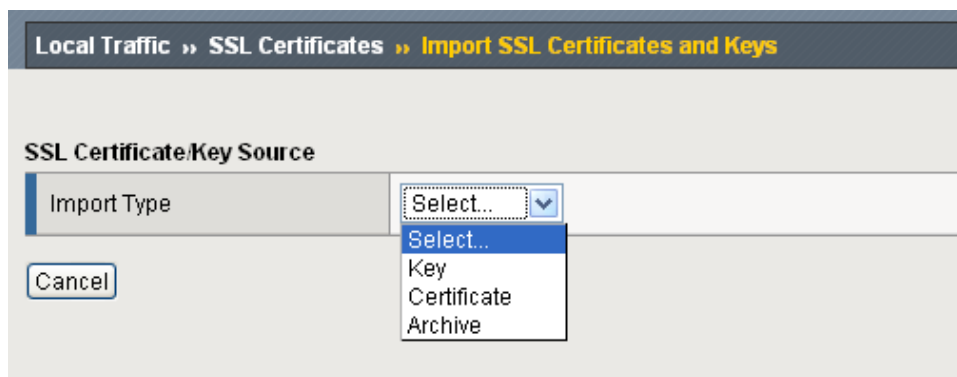
(更新時には改めての設定は不要です)

中間証明書インストール手順(1)



必要な中間証明書をインポートします。

- <http://www.jcert.co.jp/support/certificate.html> から、“bundle.crt”形式ファイルを取得。
- [Import]ボタンを押してファイルをアップロードします。



次のページにて、“Import Type”に“Certificate”を選択します。

中間証明書インストール手順(2)

Local Traffic » SSL Certificates » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	<input checked="" type="radio"/> Create New <input type="radio"/> Overwrite Existing SF_intermediate
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text C:\Documents and Settings\test\M; 参照...

Cancel Import

任意の”Certificate Name”を設定し、該当する中間証明書を選択。
[Import]ボタンを押してファイルをアップロードします。

Local Traffic » SSL Certificates

Certificate List

* Search Import... Create...

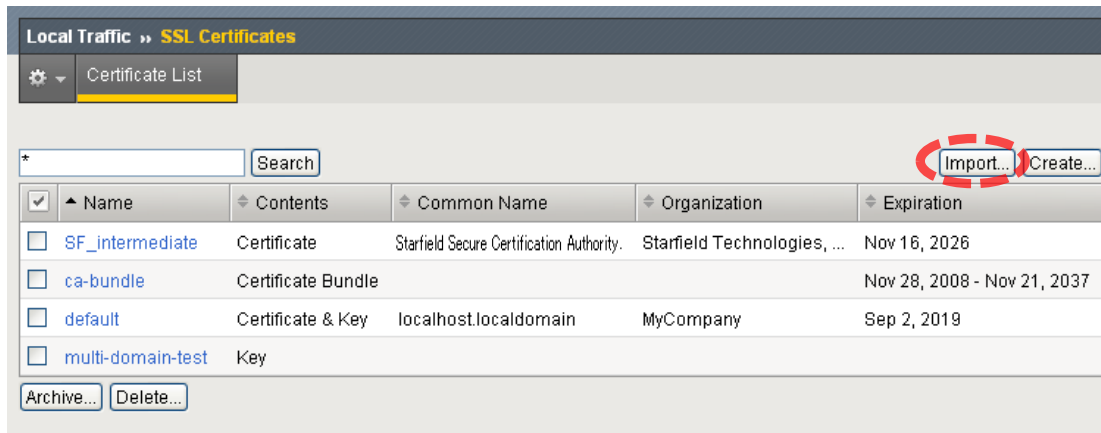
<input checked="" type="checkbox"/>	Name	Contents	Common Name	Organization	Expiration
<input type="checkbox"/>	SF_intermediate	Certificate	Starfield Secure Certification Authority	Starfield Technologies, ...	Nov 16, 2026
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Nov 28, 2008 - Nov 21, 2037
<input type="checkbox"/>	default	Certificate & Key	localhost.localdomain	MyCompany	Sep 2, 2019
<input type="checkbox"/>	multi-domain-test	Key			

Archive... Delete...

SSL Certificatesの画面にて、該当する中間証明書がインポートされていることと確認できます。

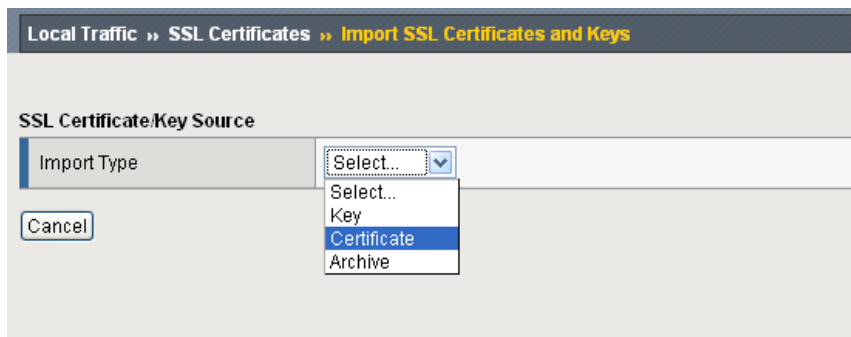
サーバ証明書インストール手順

サーバ証明書インストール手順(1)



認証局より署名されたサーバ証明書をインポートします。

Local Traffic →SSL Certificatesの画面にて、
[Import]ボタンを押します。



次のページにて、“Import Type”に“Certificate”を選択します。

サーバ証明書インストール手順(2)

Local Traffic » SSL Certificates » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	<input checked="" type="radio"/> Create New <input type="radio"/> Overwrite Existing multi-domain-cert
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text C:\Documents and Settings\test\M\ 参照...

Cancel Import

任意の”Certificate Name”を設定し、該当するサーバ証明書を選択。

[Import]ボタンを押してファイルをアップロードします。

Local Traffic » SSL Certificates

Certificate List

Search Import... Create...

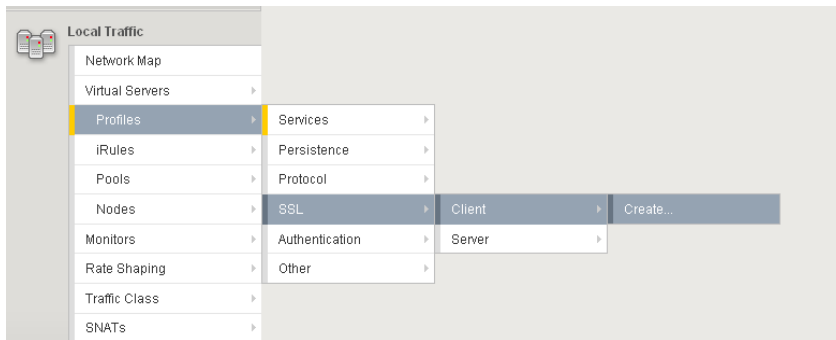
<input checked="" type="checkbox"/>	Name	Contents	Common Name	Organization	Expiration
<input type="checkbox"/>	SF_intermediate	Certificate	Starfield Secure Certification Authority	Starfield Technologies, ...	Nov 16, 2026
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Nov 28, 2008 - Nov 21, 2037
<input type="checkbox"/>	default	Certificate & Key	localhost.localdomain	MyCompany	Sep 2, 2019
<input type="checkbox"/>	multi-domain-cert	Certificate	www.sample-a.jp		! Sep 18, 2009
<input type="checkbox"/>	multi-domain-test	Key			

Archive... Delete...

SSL Certificatesの画面にて、該当する証明書がインポートされていることと確認できます。

サーバ証明書適用手順(例)

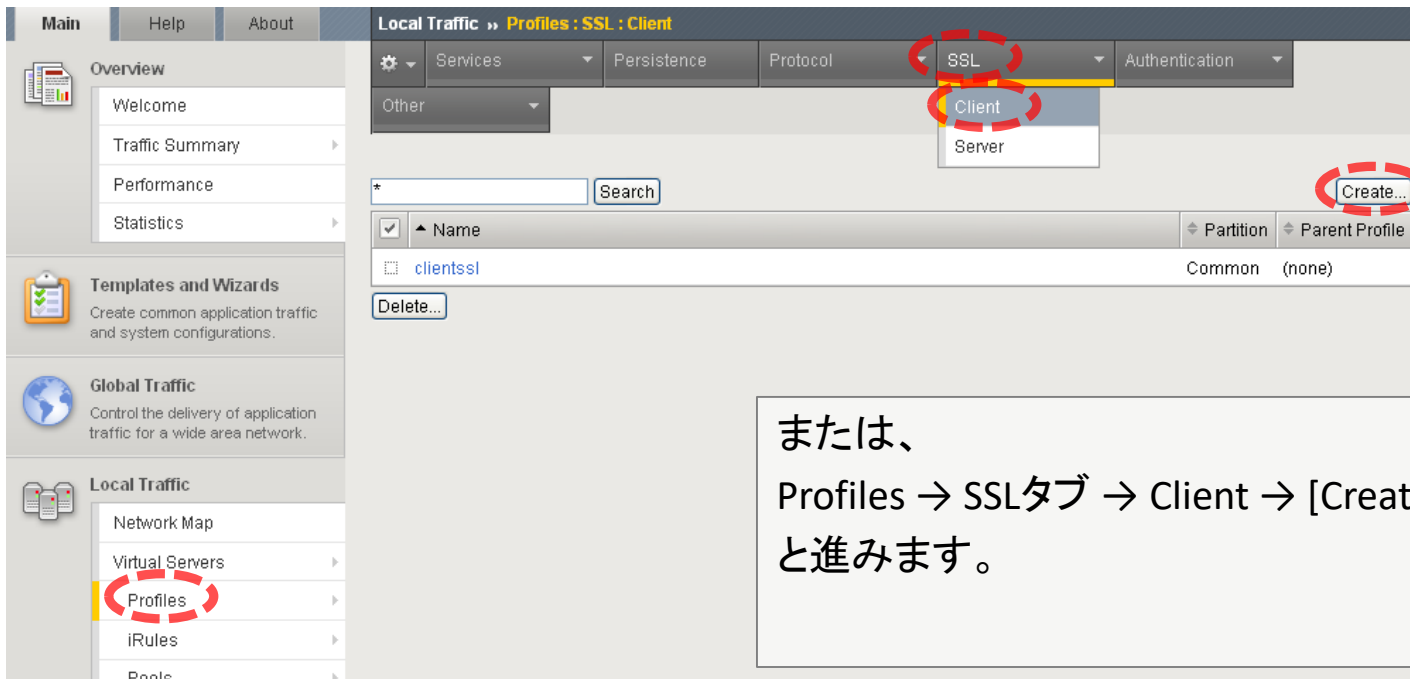
サーバ証明書適用手順(1) SSLプロファイル



インポートしたサーバ証明書を適用するためのClientSSLプロファイルを作成します。

左図のようにFly-outメニュー(v10以降の機能)から
Profiles → SSL → Client → Create

または



または、
Profiles → SSLタブ → Client → [Create]ボタン
と進みます。

サーバ証明書適用手順(2) SSLプロファイル

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

Name: clientssl-md-test

Parent Profile: clientssl

Configuration: Basic

Certificate: Basic (Advanced selected) | default

Key: default

Options List

Enabled Options: Don't insert empty fragments

Disable

Available Options: Netscape@ reuse cipher change bug workarou, Microsoft@ big SSLv3 buffer, Microsoft@ IE SSLv2 RSA padding

任意のプロファイル名を設定し、
“Configuration”を“Advanced”メニューに
切り替えます。

サーバ証明書適用手順(3) SSLプロファイル

必要な設定項目は以下の通りです。

各項目の右側のチェックボックスにチェックを入れることで、値の編集が可能になります。

“Certificate”

認証局によって署名され、先の手順でインポートしたサーバ証明書です。

BIG-IPにインポートした際につけた名称をプルダウンメニューから選択します。

“Key”

BIG-IP上でCSRを作成した場合にはCSRと同じ名称のKey(サーバ秘密鍵)を、外部からインポートしたKeyを使う場合はインポート時につけた名前を選択します。

“Pass Phrase”

上で選択したKey(サーバ秘密鍵)を作成する際に設定したパスワードです。

The screenshot shows the 'New Client SSL Profile...' configuration page in the BIG-IP management console. The breadcrumb trail is 'Local Traffic >> Profiles : SSL : Client >> New Client SSL Profile...'. The 'General Properties' section includes 'Name' (clientssl-md-test) and 'Parent Profile' (clientssl). The 'Configuration' section is set to 'Advanced' and includes the following fields:

Field	Value	Checkmark
Certificate	multi-domain-cert	<input checked="" type="checkbox"/>
Key	multi-domain-test	<input checked="" type="checkbox"/>
Pass Phrase	*****	<input checked="" type="checkbox"/>
Confirm Pass Phrase	*****	<input checked="" type="checkbox"/>
Chain	SF_intermediate	<input type="checkbox"/>
Trusted Certificate Authorities	None	<input checked="" type="checkbox"/>
Ciphers	DEFAULT	<input type="checkbox"/>
Options	Options List...	<input type="checkbox"/>

“Chain”

先の手順でインストールした中間証明書をプルダウンメニューから選択します。

サーバ証明書適用手順(3) SSLプロファイル

The screenshot shows a configuration window for an SSL profile. On the left is a sidebar with menu items: High Availability, Archives, Services, Preferences, SNMP, Users, Logs, and Support. The main area contains several settings:

Handshake Timeout	Specify... 60 seconds	<input type="checkbox"/>
Renegotiate Period	Indefinite	<input type="checkbox"/>
Renegotiate Size	Indefinite	<input type="checkbox"/>
Renegotiate Max Record Delay	Specify... 10 records	<input type="checkbox"/>
Unclean Shutdown	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/>
Strict Resume	<input type="checkbox"/>	<input type="checkbox"/>
Non-SSL Connections	<input type="checkbox"/>	<input type="checkbox"/>

Below these is the 'Client Authentication' section, which is set to 'Custom'.

Client Certificate	ignore	<input type="checkbox"/>
Certificate Revocation List (CRL)		<input type="checkbox"/>

At the bottom are three buttons: 'Cancel', 'Repeat', and 'Finished'. The 'Finished' button is circled in red.

[Finished] ボタンを押してSSL
プロファイルの作成を完了
します。

サーバ証明書適用手順(4) Virtual Server設定

The screenshot shows the configuration page for a Virtual Server named 'sample-a-www'. The 'General Properties' section includes fields for Name, Partition, Destination (Type: Host, Address: 10.1.1.101), Service Port (443, HTTPS), Link, Availability, and State (Enabled). The 'Configuration' section is set to 'Basic' and includes fields for Type (Standard), Protocol (TCP), OneConnect Profile (None), NTLM Conn Pool (None), HTTP Profile (None), FTP Profile (None), SSL Profile (Client) (None), SSL Profile (Server) (clientssl), SIP Profile (None), VLAN Traffic (All VLANs), and iSession Profile (None, Context: server). The 'Update' button is circled in red.

サーバ証明書の適用対象であるVirtual Serverの設定画面にて、“SSL Profile (Client)”のプルダウンメニューより先ほど作成したSSLプロファイルを選択します。

[Update]ボタンを押して設定を反映します。

サーバ証明書適用手順(5)

Hostname: bigip.localnet Date: Sep 10, 2009 User: admin
IP Address: 172.28.4.207 Time: 7:17 PM (JST) Role: Administrator Partition: Common Log out

State: ACTIVE
Licensed yet unprovisioned: GTM

Main Help About

Local Traffic » Network Map

Network Map

Status: Any Status Type: All Types Search: * Search IRule Definition:

Show Summary Update Map

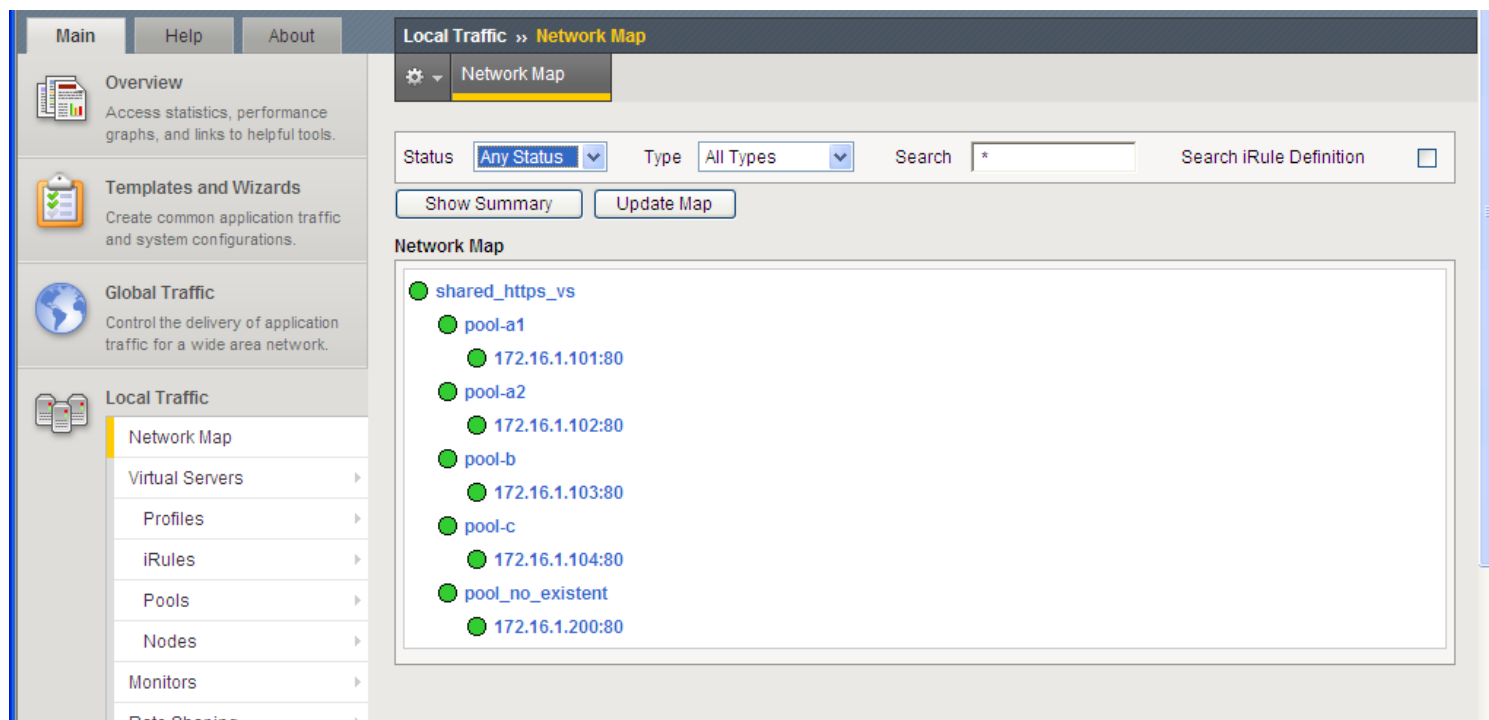
Network Map

sample-a-www pool-a1 172.16.1.101:80	sample-b-www pool-b 172.16.1.103:80	sample-c-www pool-c 172.16.1.104:80
sample-a-www2 pool-a2 172.16.1.102:80		

MultiDomain証明書の対象となるWebサーバが個別にIPアドレスを持つ場合は、BIG-IP上でのVirtual ServerはIPアドレス(およびポート)ごとに個別に作成しますが、

- 一つのSSL証明書を複数のSSLプロファイルに割り当てる、または
- 一つのSSL証明書を一つのSSLプロファイルに割り当て、それを複数のVirtual Serverに適用することのどちらも可能です。

サーバ証明書適用手順(6)



MultiDomain証明書の対象となるWebサーバが一つのIPアドレスを共有する場合は、BIG-IP上でのVirtual Serverは一つ作成し、BIG-IPのHTTP Class機能等を用いて、リクエストされたホスト名に応じて適切なWebサーバにトラフィックを振り分けます。

この場合は、MultiDomain証明書を一つのSSLプロファイルに割り当て、それを一つのVirtual Serverに適用して利用します。