IBM i Virtual Host uses wrong certificate when there is more than one

Issue

Customers may have more than one SSL certificate, intending each for a different named Virtual Host. When deploying a Virtual Host using the Zend Server User Interface, or when defining the Virtual Host manually in the Apache configuration, the certificate is specified using the SSLAppName directive to identify the Application Name assigned to the certificate in the Digital Certificate Manager (DCM). If Virtual Hosts are given different application names, the certificate used in every Virtual Host is the certificate named in the first Virtual Host container. The different application names seem to be ignored.

Environment

IBM i V7.2 or later.

> ⚠ **This issue also occurs in 7.1, but 7.2 or later is needed to fix it.**
>
> Server Name Indication (SNI) does not appear to be available in 7.1.

Resolution

SSL requests wrap an SSL layer around the HTTP layer. The SSL session does not tell which Virtual Host to use, so Apache will use the default. The SSL protocol has been extended with Server Name Indication (SNI) to fix this. To use SNI, both your Apache server and the requester's browser must be at a version that supports it. Most major browsers at the current version will support this. IBM HTTP Server for i supports it at version 7.2 (Apache 2.4) or higher.

To enable SNI in your virtual host, IBM Support has recommended that the Virtual Host should specify the specific IP address, rather than the asterisk wild card. Also, an additional directive needs to be applied to identify the SSL Server Cert.

In a typical Zend Server Apache configuration, the IP address is the wild card. This is so the configuration can run on any system as installed, without modification. So you would need to change it for your SSL Virtual Hosts. You may have added a Listen at port 443 like this:

```
Listen *:443
```

To use SNI you would change it to use your IP. For example, if your IP was 10.1.2.3, you would change the Listen directive to look like this:

```
Listen 10.1.2.3:443
```

The VirtualHost container directive for each Virtual Host using SSL would also need to be changed, from this:

```
<VirtualHost *:443>
```

to this:

```
<VirtualHost 10.1.2.3:443>
```

Remember 10.1.2.3 is just an example. Please use your actual IP address.

When you add SSL support to a Virtual Host using the Zend Server UI, you specify the Application Name for the certificate. Then, these two lines are inserted into the template:

```
SSLEngine On
SSLAppName QIBM_HTTP_SERVER_EXAMPLE
```

In this example, the Application Name assigned to the cert is QIBM_HTTP_SERVER_EXAMPLE.

You can have one or more certificates assigned to the Application Name, so you need to further identify the specific certificate. In DCM, each certificate has a Certificate Label. You use that Certificate Label in the SSLServerCert directive. For each Virtual Host, please add the SSLServerCert directive just below the SSLAppName directive.

> ⚠ **Certificate Label must not have trailing blanks**
>
> Be careful not to include any leading or trailing blanks when entering the Certificate Label into DCM. Additional blank spaces may cause the SSLServerCert directive to be unable to match the label.

Assume you have two certificates defined to Application Name QIBM_HTTP_SERVER_EXAMPLE, labeled Example1 and Example2, to be used for named Virtual Hosts example1.com and example2.com, respectively. Your VirtualHost containers would look something like this:

```
Listen 10.1.2.3:443

<VirtualHost 10.1.2.3:443>
....(some more stuff here)


SSLEngine On
SSLAppName QIBM_HTTP_SERVER_APACHE
SSLServerCert Example1


ServerName example1.com
...(some more stuff here)
</VirtualHost>

<VirtualHost 10.1.2.3:443>
...(some more stuff here)


SSLEngine On
SSLAppName QIBM_HTTP_SERVER_APACHE
SSLServerCert Example2


ServerName example2.com
...(some more stuff here)
</VirtualHost>
```

Please remember that if the Virtual Host was created in the Zend Server UI, you should modify the template in the UI, and not go directly to the include file to edit it there.