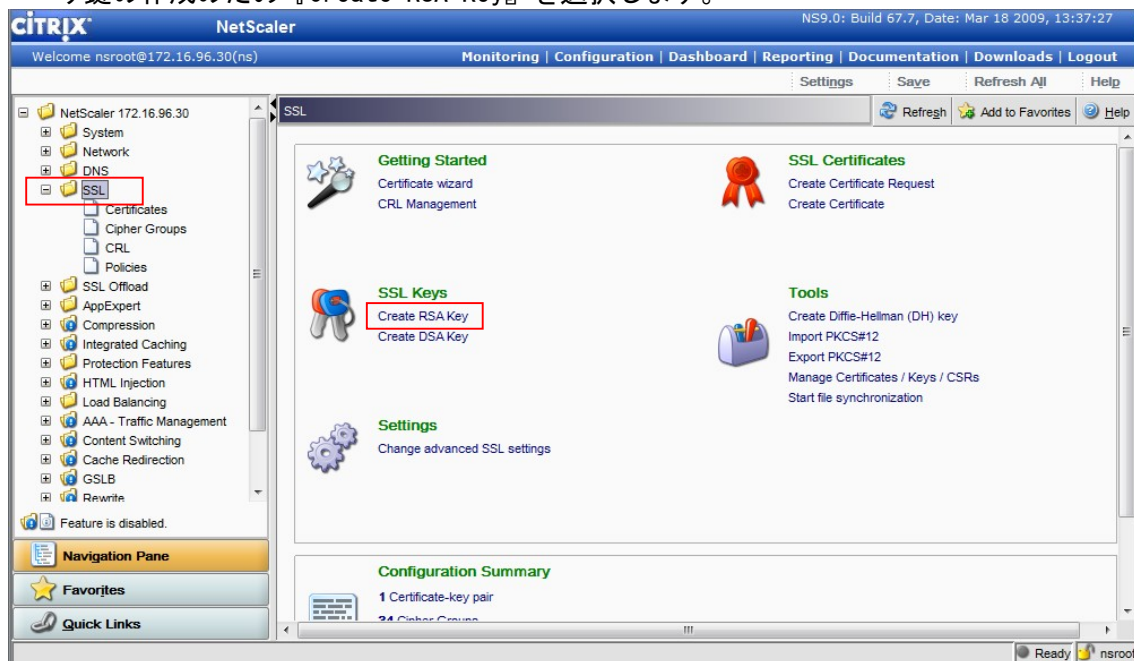


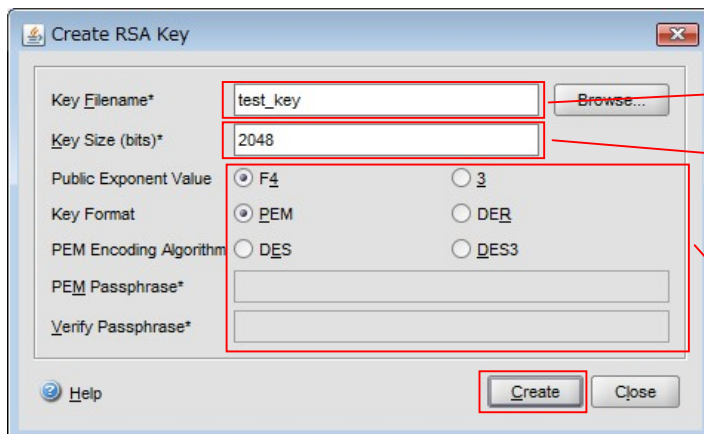
Citrix NetScaler サーバ証明書設定手順書

① 鍵ペア及び CSR の作成

1. NetScaler に WebUI よりログインし、SSL を画面左より選択します。選択後、画面右より鍵の作成のため『Create RSA Key』を選択します。



2. 鍵の作成画面にて鍵の名前やサイズを設定し、Create ボタンをクリックします。

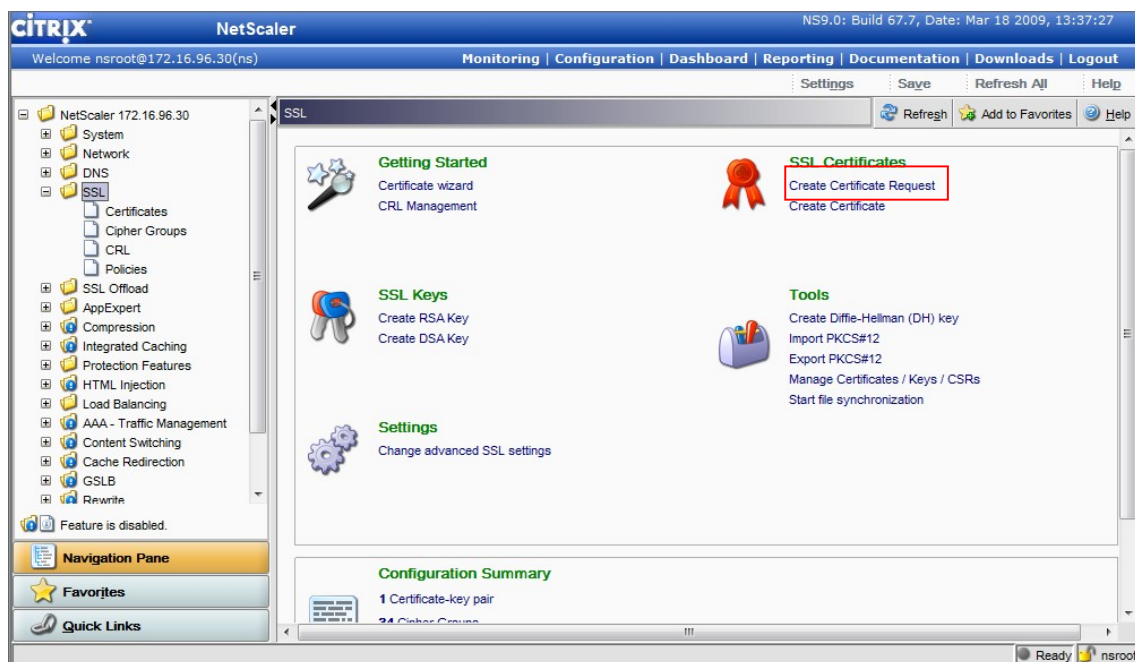


任意の鍵の名前を指定します。

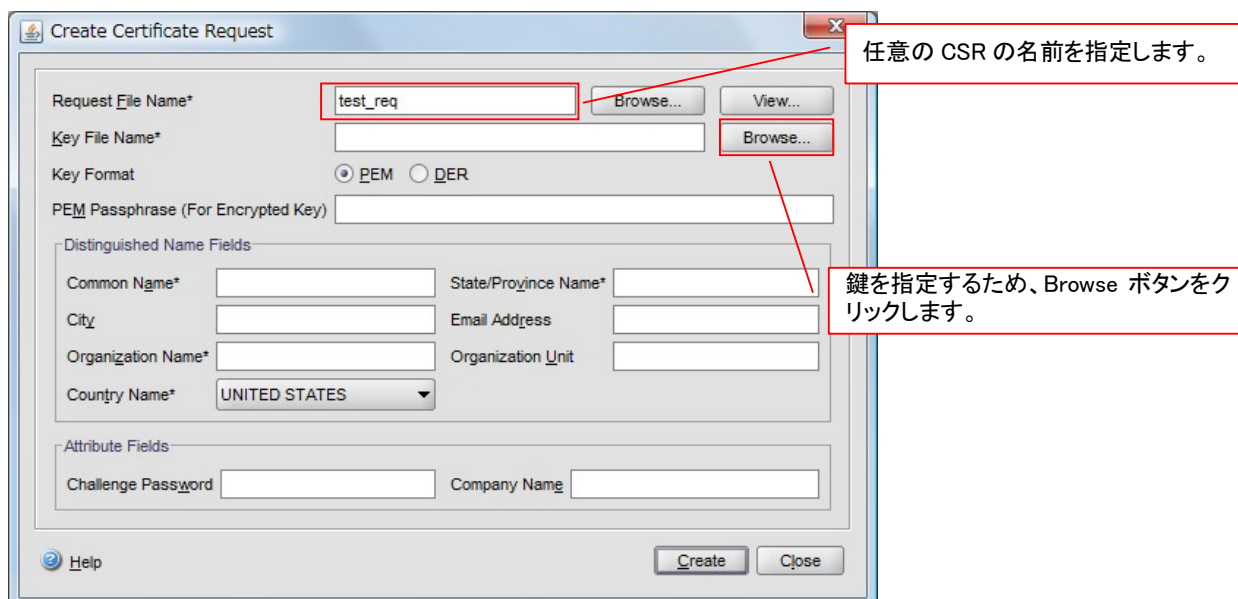
2048bit を指定します。

必要に応じて選択、入力を行います。

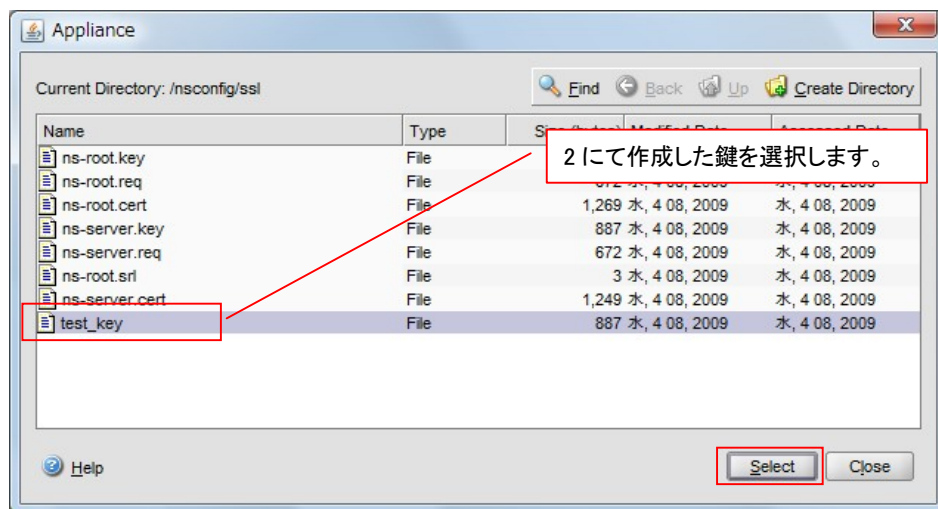
- 再度画面左より SSL を選択します。(Ver8.0 及び 8.1 の場合は画面左より SSL→CA Tools を選択)
選択後、画面右より CSR 作成のため『Create Certificate Request』を選択します。



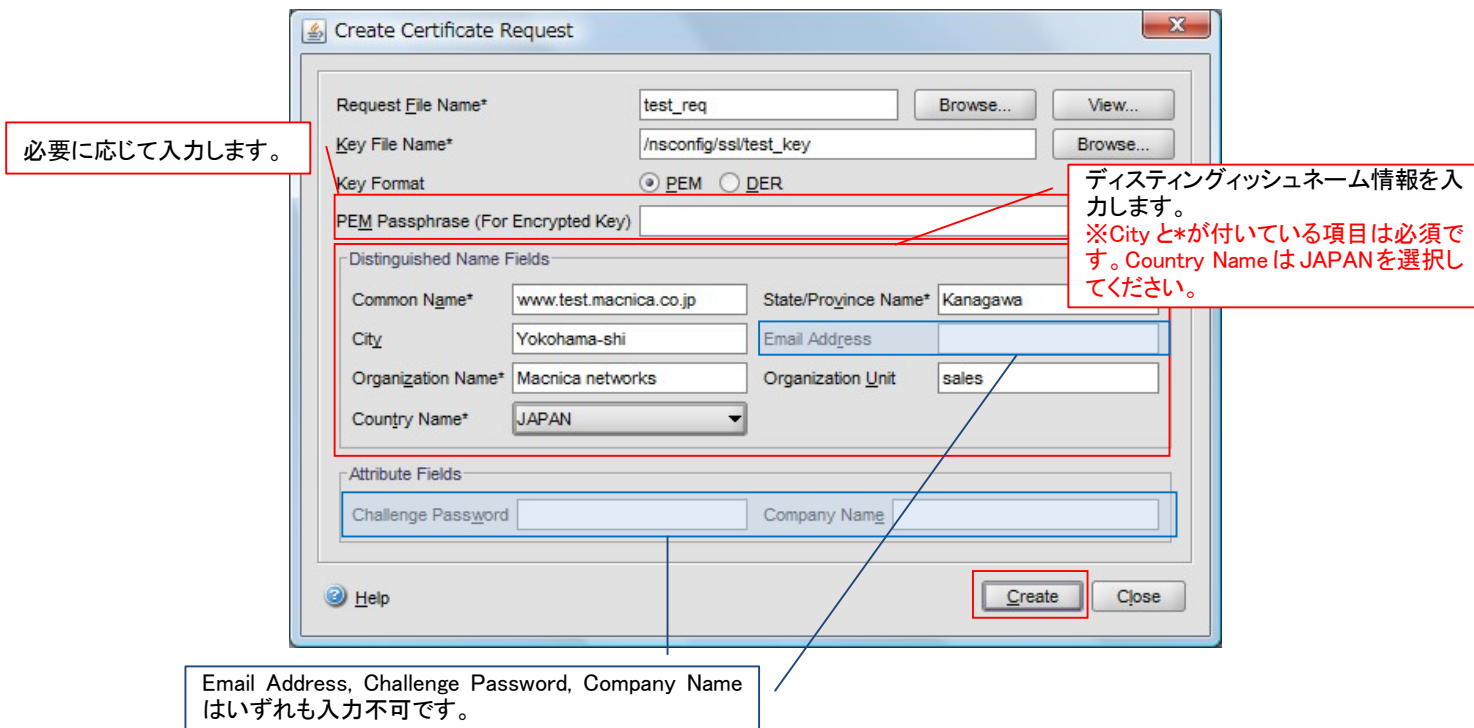
- CSR の名前を入力し、Browse ボタンをクリックして鍵を指定します。



5. 鍵の選択画面にて 2 にて作成した鍵を選択し、Select ボタンをクリックします。



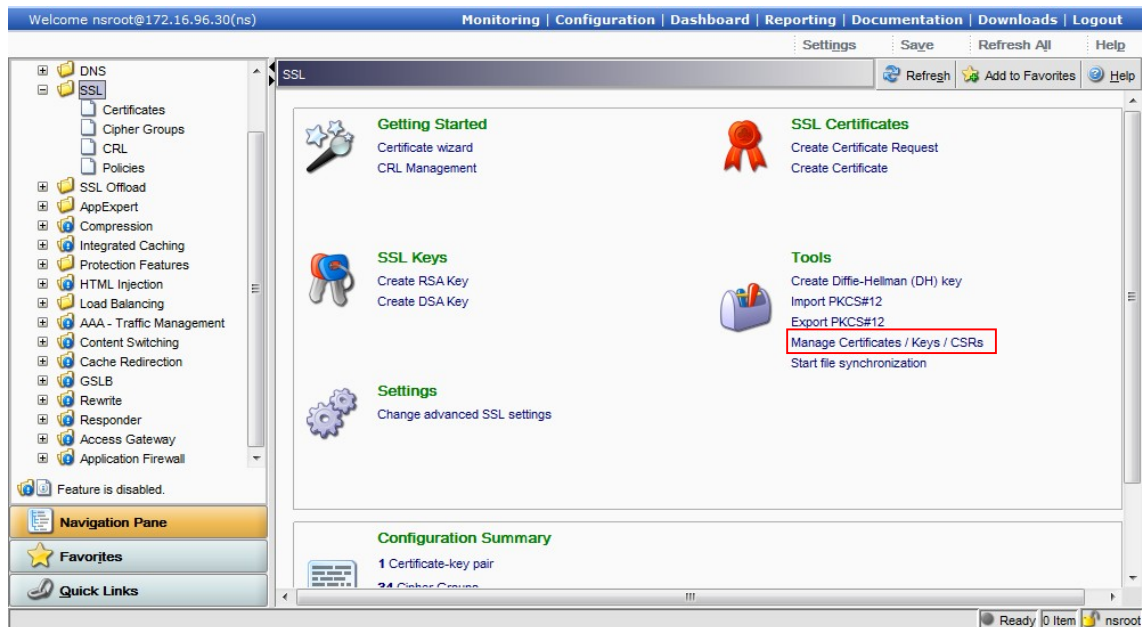
6. ディスティンギッシュネーム情報などを入力し、Create ボタンをクリックします。
*が付いている項目は、入力必須です。



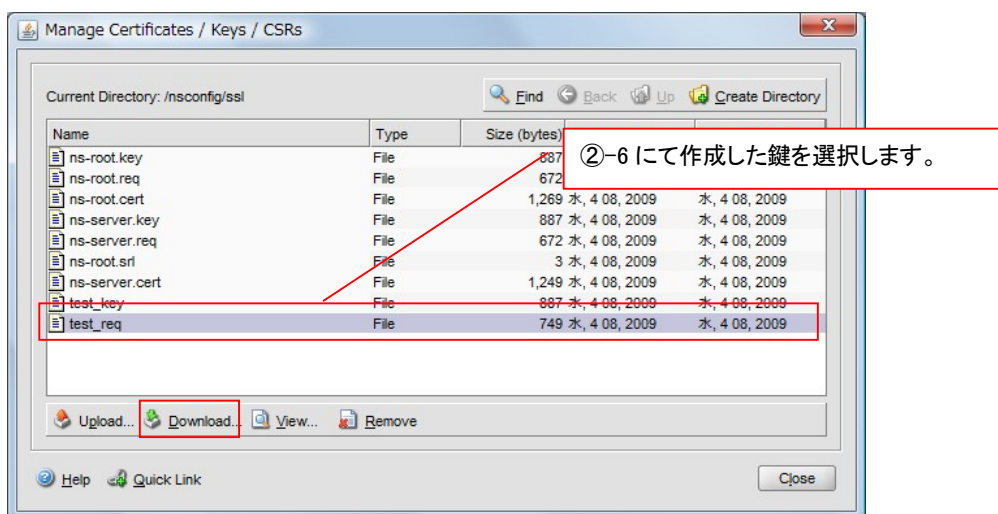
② CSR のエクスポート

1. 画面左より SSL を選択します。

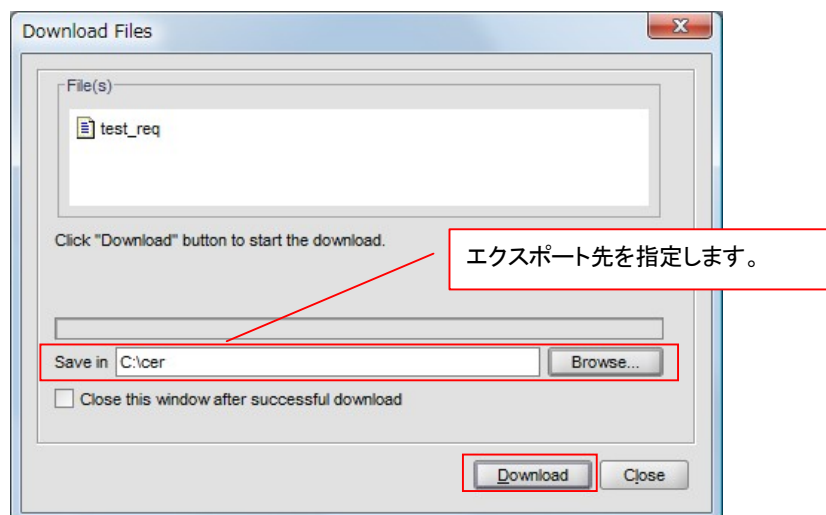
選択後、CSR をエクスポートするため画面右より Manage Certificates/Keys/CSRs を選択します。



2. 選択画面にて①-6にて作成した CSR を選択し、Download ボタンをクリックします。



- CSR のエクスポート先の指定画面にて、管理端末のどこにエクスポートするのかを指定し、Download ボタンをクリックします。



- エクスポートした CSR ファイルをテキスト等で開き中身を確認します。
下記のようなファイルであることを確認します。

```

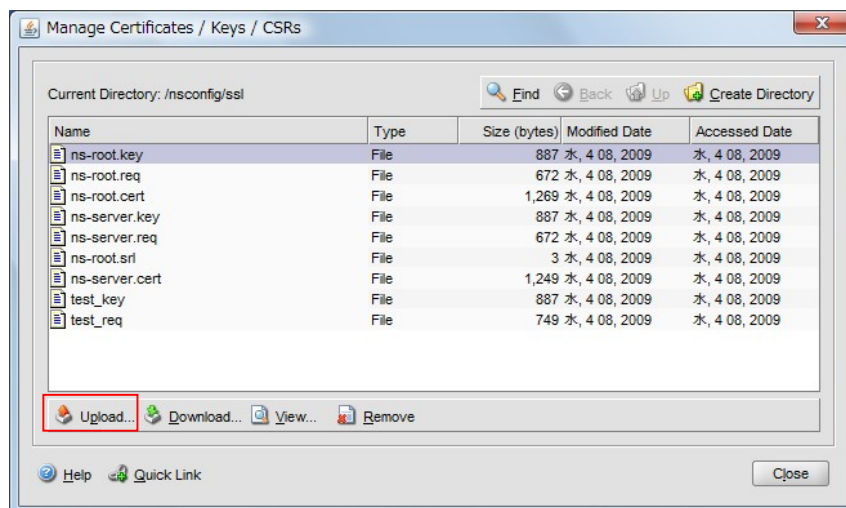
1  -----BEGIN NEW CERTIFICATE REQUEST-----
2  MIIB6zCCAVQCAQAwgaoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTEV
3  MBMGA1UEBxMMW9rb2hhbWEtc2hpMRkwFwYDVQQKExBNlYNuaWNhIG5ldHdvcmtz
4  MQ4wDAYDVQQLEwVzYWxlc2EfmBOGA1UEAxMwd3d3LnRlc3QubWJbm1jYS5jb5q
5  cDEIMCMGCSqGSIb3DQEJARYWdGVzdGFkZHZHJlc0BtYWNuaWNhLm5ldCBnzANBgkq
6  hkiG9w0BAQEFAAOBjQAwgYkCgYEAOL+9WU4wJMCxwkgjbs39Ne0pH+tzy6gJrgfx
7  ITfp6CreMcaEYsFYVjptHZ7Axi4Jo4jGszcWt+hQxgXVb/V94XfMCLy2rlqPSc9B
8  JCCaSeM3moob+j4p8BR9p3cGkYXXzYZRd+vv9gqJPTreaN9ow8vWdBSxKXaHoem
9  j iM82UcCAwEAaAAMA0GCSqGSIb3DQEBBQUAA4GBABifxtv8SkPOZAZ0bcryWZ48
10  3RQQiCgdNwKcfNBfV0cNgHugNAQIw7f gwRHsPCM3pYIZX1o6QF5wsAT4cFdZFivB
11  UBug6GOBA3rGPUeEH+eZUjzpG97vB3xEKz5uy21QTVtyU+5xqLnX4PDsMgArstC
12  gaHvgI5SYV5Dfat1ZK4o
13  -----END NEW CERTIFICATE REQUEST-----
[EOF]

```

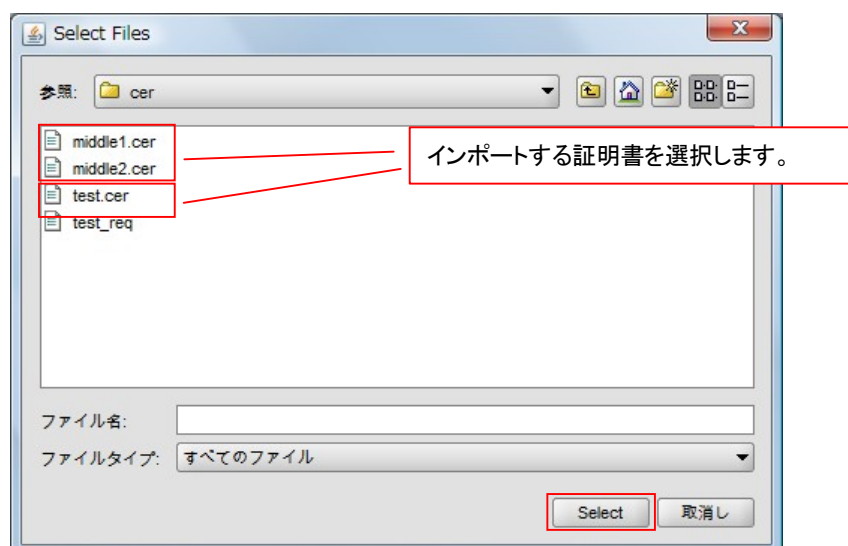
- エクスポートした CSR を証明書発行機関に送付し、証明書を作成してもらいます。
- CSR をもとに、証明書発行機関より証明書が発行されます。

③ 証明書のインポート

1. 証明書を NetScaler に取り込むため WebUI よりログインし、SSL を画面左より選択します。選択後、画面右より Manage Certificates/Keys/CSRs を選択し、Upload ボタンをクリックします。



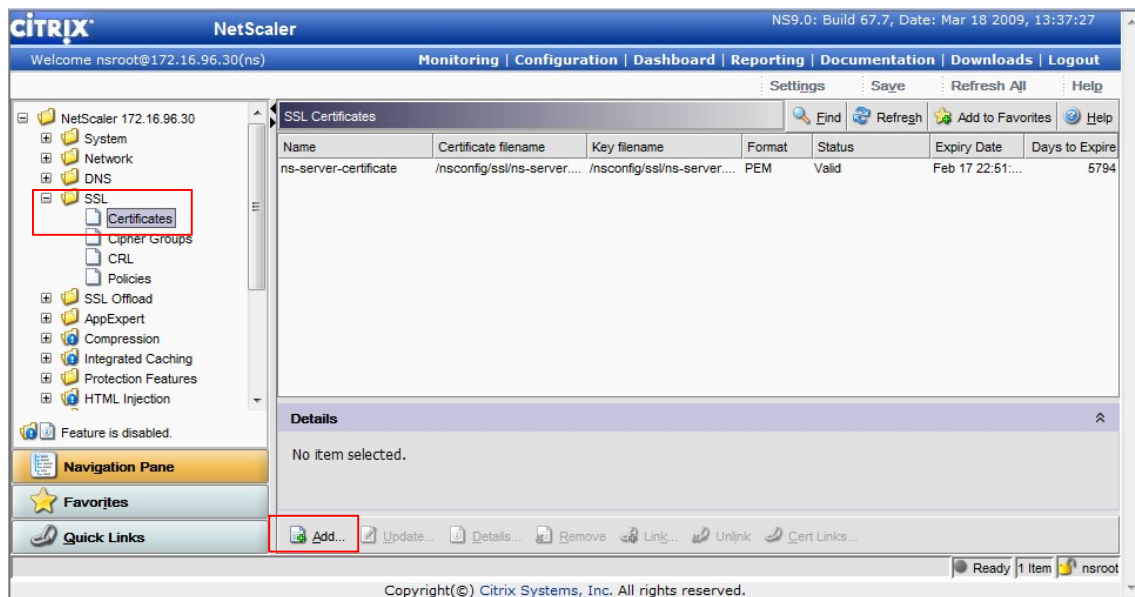
2. インポートするファイルを選択し、Select ボタンをクリックします。
本例ではサーバ証明書 1 枚、中間証明書 2 枚をインポートしています。



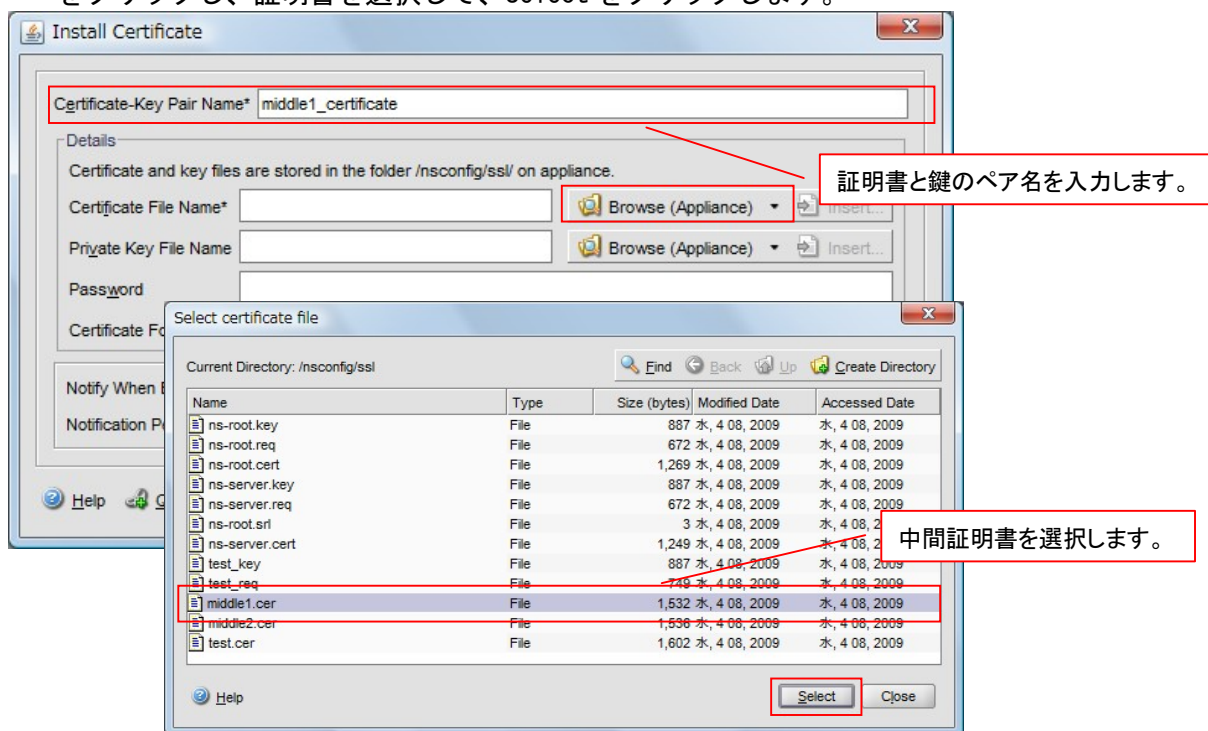
④ 証明書の設定と、Vserver との紐付け

1. 画面左より SSL → Certificates を選択します。

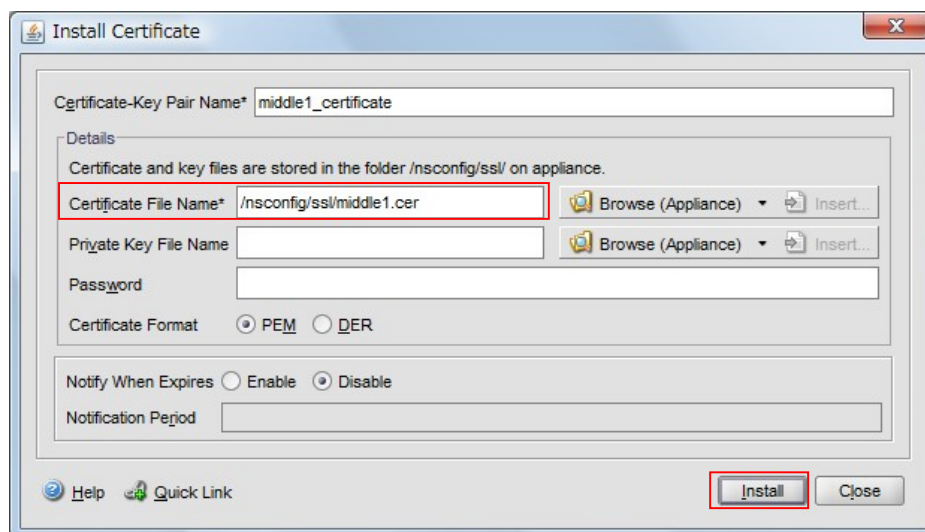
選択後、証明書を設定するため画面下の Add ボタンをクリックします。



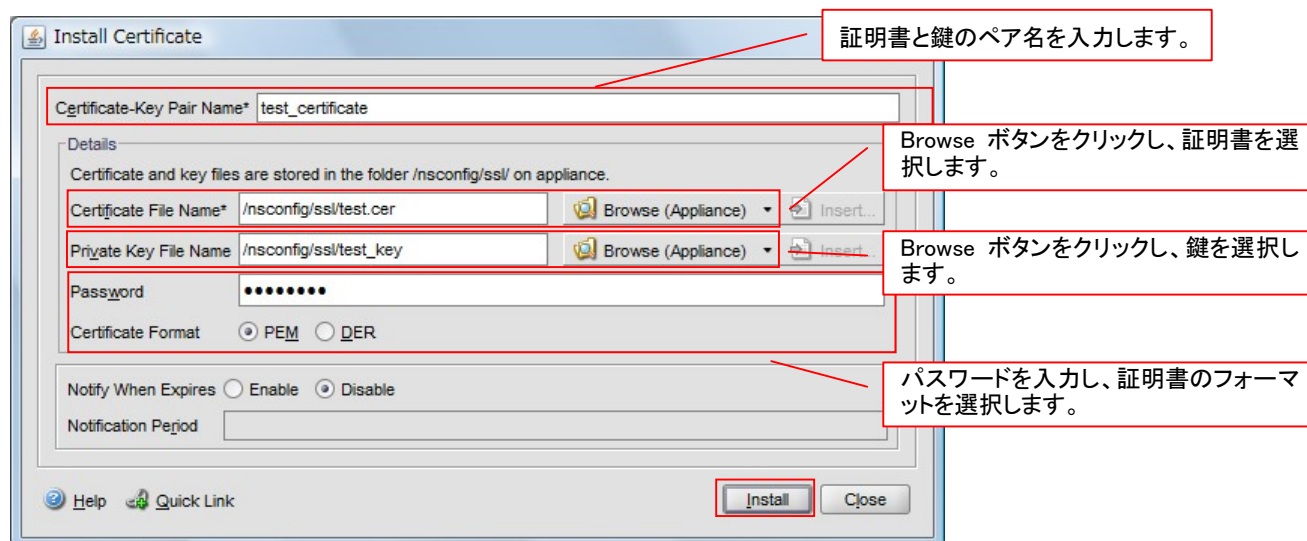
2. 中間証明書を設定するため、証明書と鍵のペア名を入力します。その後、Browse ボタンをクリックし、証明書を選択して、Select をクリックします。



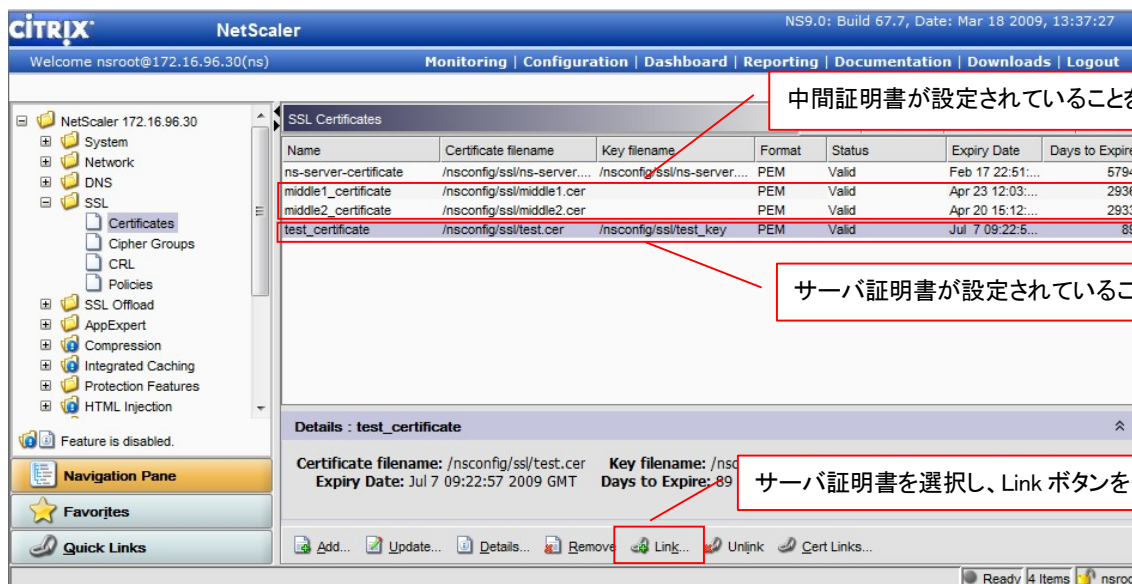
3. 選択した証明書が表示されていることを確認して、Install ボタンをクリックします。
中間証明書の場合、鍵の設定は必要ありません。
本例では中間証明書を2つ使用しますので、もう一方の中間証明書も同様に設定します。



4. サーバ証明書を設定するため、証明書と鍵のペア名を入力します。その後、Browse ボタンをクリックし、証明書と鍵を選択して、必要項目を入力し Install ボタンをクリックします。
本例では、②-6 にて証明書発行機関より発行された証明書と、①-2 にて作成した鍵のペアを設定しています。



5. 中間証明書とサーバ証明書が設定されていることを確認します。その後、サーバ証明書と中間証明書を紐付けるため、サーバ証明書を選択して、画面下の Link ボタンをクリックします。



NetScaler NS9.0: Build 67.7, Date: Mar 18 2009, 13:37:27

Welcome nsroot@172.16.96.30(ns) | Monitoring | Configuration | Dashboard | Reporting | Documentation | Downloads | Logout

SSL Certificates

Name	Certificate filename	Key filename	Format	Status	Expiry Date	Days to Expire
ns-server-certificate	/nsconfig/ssl/ns-server....	/nsconfig/ssl/ns-server....	PEM	Valid	Feb 17 22:51:...	5794
middle1_certificate	/nsconfig/ssl/middle1.cer		PEM	Valid	Apr 23 12:03:...	2936
middle2_certificate	/nsconfig/ssl/middle2.cer		PEM	Valid	Apr 20 16:12:...	2933
test_certificate	/nsconfig/ssl/test.cer	/nsconfig/ssl/test_key	PEM	Valid	Jul 7 09:22:5...	89

Details : test_certificate

Certificate filename: /nsconfig/ssl/test.cer Key filename: /nsconfig/ssl/test_key
Expiry Date: Jul 7 09:22:57 2009 GMT Days to Expire: 89

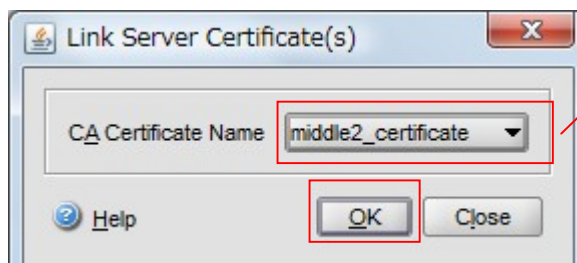
Navigation Pane: System, Network, DNS, SSL (Certificates, Cipher Groups, CRL, Policies), SSL Offload, AppExpert, Compression, Integrated Caching, Protection Features, HTML Injection

Buttons: Add..., Update..., Details..., Remove, Link..., Unlink, Cert Links...

Annotations:

- 中間証明書が設定されていることを確認します。
- サーバ証明書が設定されていることを確認します。
- サーバ証明書を選択し、Link ボタンをクリックします。

6. 中間証明書の選択画面になりますので、対象の証明書を選択し、OK ボタンをクリックします。

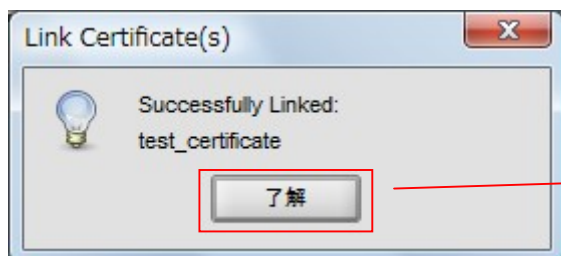


Link Server Certificate(s)

CA Certificate Name: middle2_certificate

Buttons: Help, OK, Close

Annotation: プルダウンより対象の中間証明書を選択します。本例ではサーバ証明書『tes_certificate』と中間証明書『middle1_certificate』のチェーン証明書である『middle2_certificate』と『tes_certificate』を紐付けています。



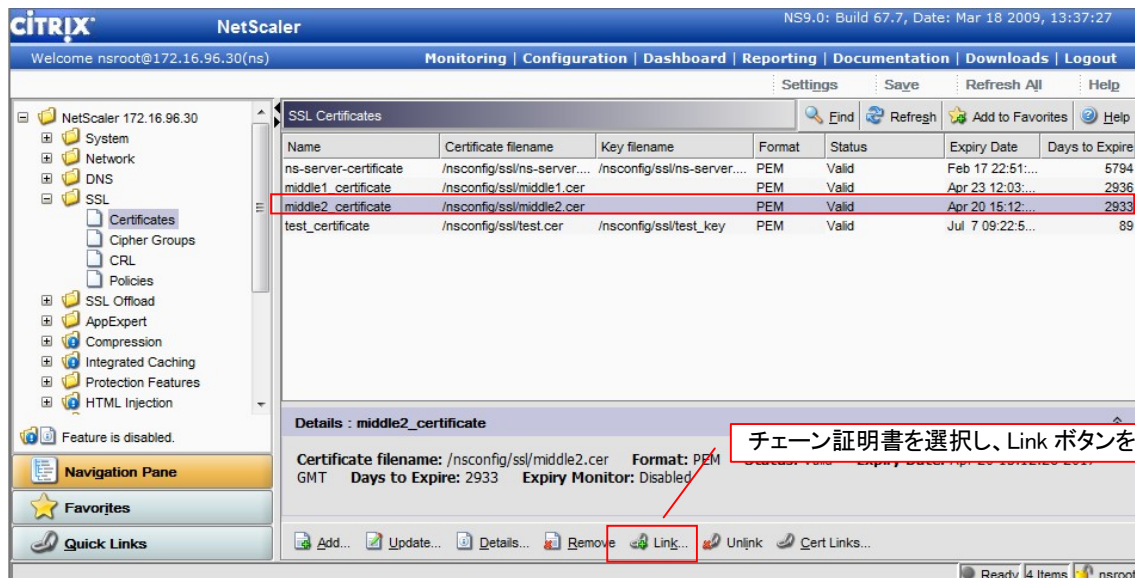
Link Certificate(s)

Successfully Linked: test_certificate

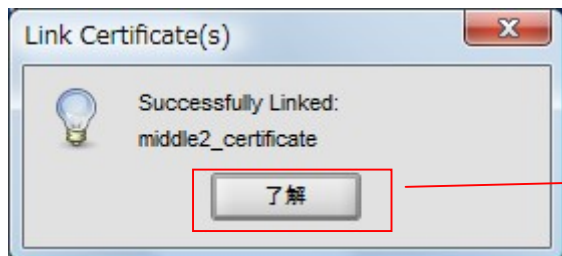
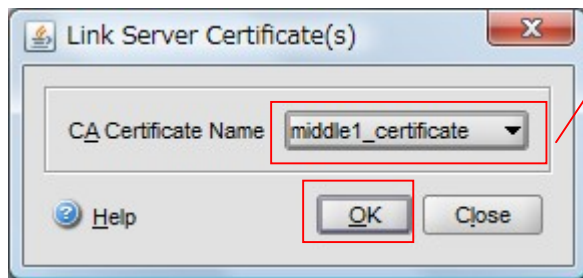
Button: 了解

Annotation: 設定の確認画面が表示されますので、『了解』ボタンをクリックします。

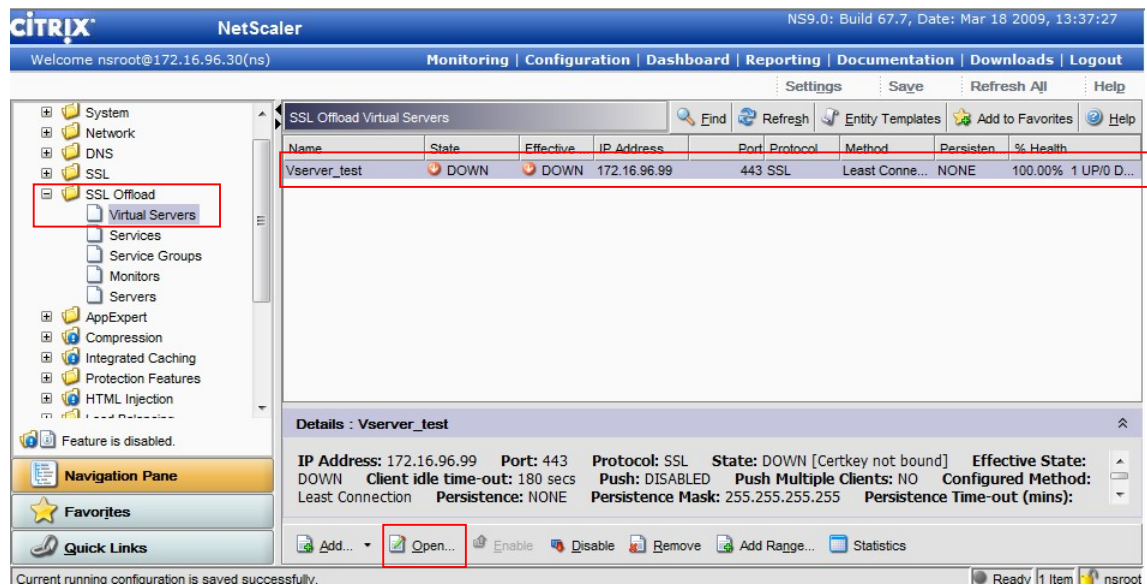
7. チェーン証明書と中間証明書を紐付けるため、チェーン証明書を選択して、画面下の Link ボタンをクリックします。



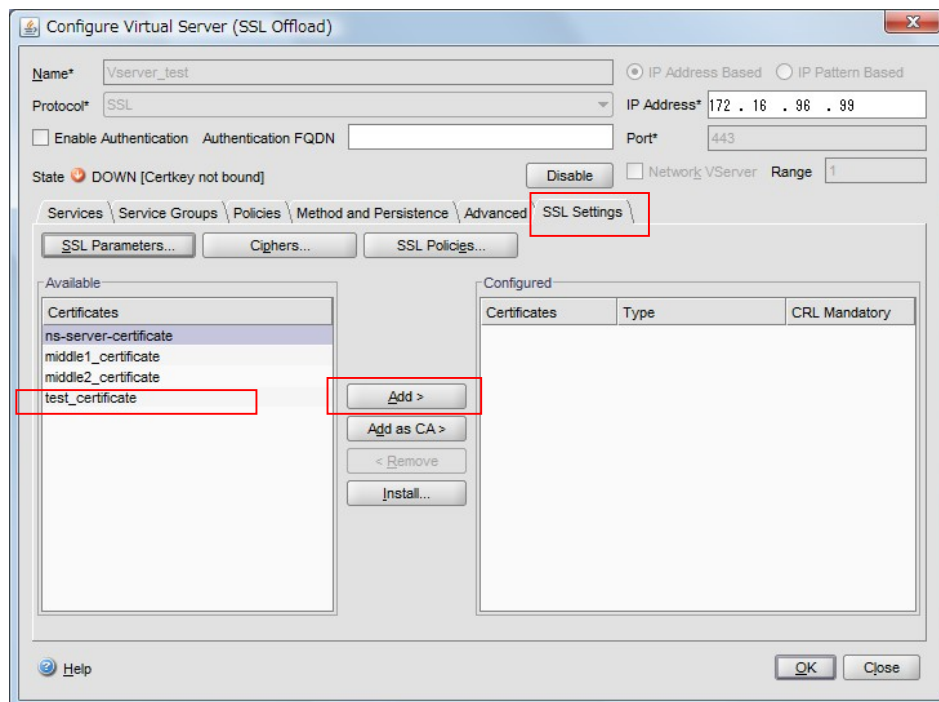
8. 中間証明書の選択画面になりますので、対象の証明書を選択し、OK ボタンをクリックします。



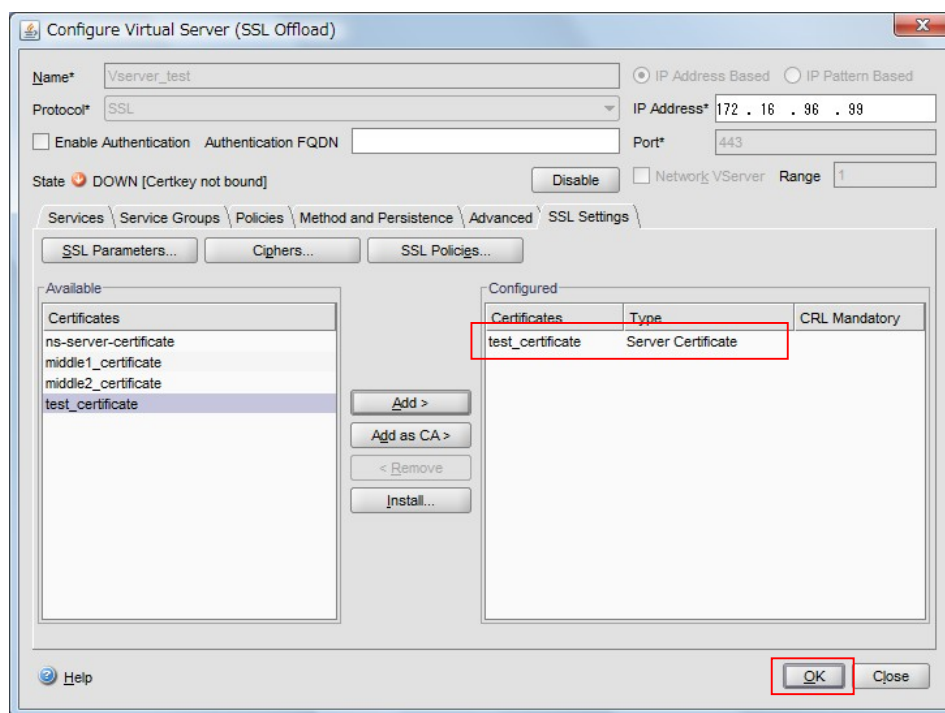
9. Vserve に、設定したサーバ証明書と鍵のペアを紐付けるため、画面右より SSL → Virtual Servers を選択します。その後対象の Vserver を選択し、Open ボタンをクリックします。（証明書の紐付け以外の Vserve の設定は、すべて正常に終了していることを前提としています。）



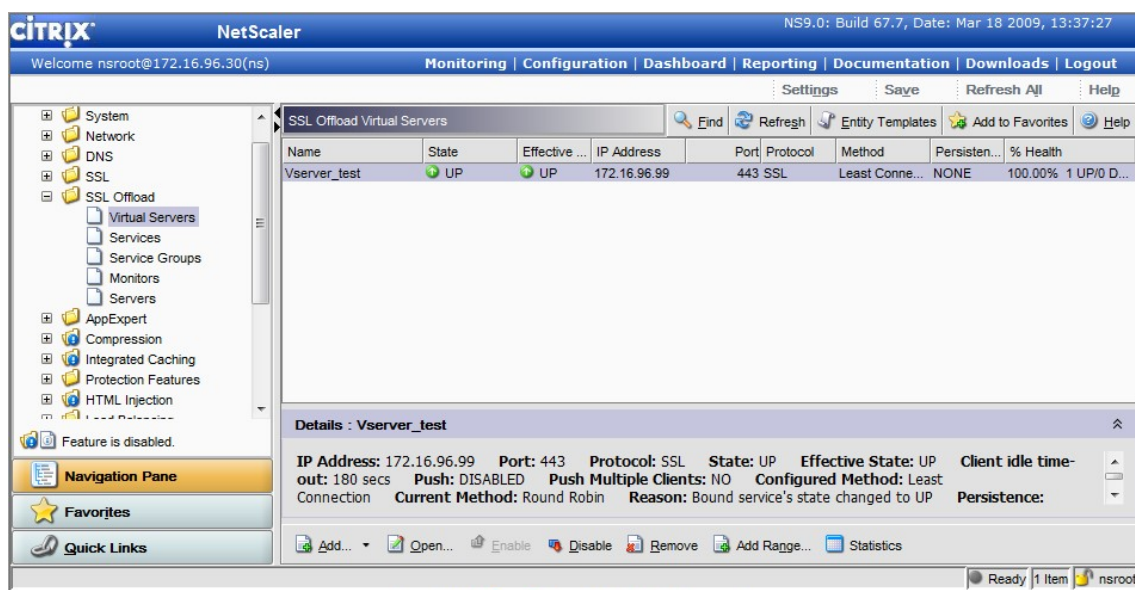
10. SSL Settings タブにて、対象のサーバ証明書と鍵のペアを選択し、Add ボタンをクリックします。



11. 選択した証明書が、画面右に表示されていることを確認し、OK ボタンをクリックします。



12. 証明書が正常に Vserver と紐付けられている場合、State が UP になっているので、確認します。



13. 動作確認をして作業完了です。

※ 設定を保存する場合は、設定画面の右上の『SAVE』ボタンをクリックする必要がありますのでご注意ください。



最後に

マクニカネットワークス株式会社の事前の許可なく、このマニュアルのいかなる部分も、いかなる方法によって複製、または電子媒体に複写することを禁じます。このマニュアルに記載されている製品および仕様に関する情報は、予告なしに変更されることがあります。本マニュアルに記載されている情報の正確性および信頼性には万全を期しておりますが、マクニカネットワークス株式会社は、いかなる利用について一切の責任を負わないものとします。Citrix Systems, Inc. は US およびその他の国において Citrix System, Inc. の登録商標です。その他、本マニュアルに記載されている会社名や製品名は、それぞれ各社の商標または登録商標です。

以上