PKI の Route Processor Redundancy の設定

Route Processor Redundancy は、ハイ システム アベイラビリティ機能の代替機能です。HSA によって、システムはアクティブ ルート スイッチ プロセッサ（RSP）が停止したときに、スタンバイ RSP をリセットして使用できます。RPR を使用すると、アクティブ RSP に重大エラーが発生したとき、RPR がアクティブ RSP とスタンバイ RSP の間で瞬時に切り替えを実現するため、計画外のダウンタイムを削減できます。

Route Processor Redundancy 機能は、現時点では、デュアル RP をサポートする Cisco ASR プラットフォーム（ASR 1006、ASR 1009、ASR 1013 など）で使用できます。

（注） Route Processor Redundancy は、トラストプールのインポートをサポートしています。

Route Processor Redundancy の設定の前提条件

- フェールオーバー時にはセカンダリ RSP がプライマリ RSP をサポートできる必要があるため、両方の RSP で同じメモリを使用する必要があります。

Route Processor Redundancy の設定に関する制約事項

- Route Processor Redundancy 機能は、デュアル RP をサポートするプラットフォームのみをサポートします。
- Route Processor Redundancy は、デュアル RSP をサポートするルータ上でのみサポートされます。

• RA（登録局）は検証されていないため、設定することは推奨されません。

Route Processor Redundancy の設定方法

Route Processor Redundancy SSO モードの設定

```
configure terminal
redundancy
 mode sso
 main-cpu
  standby console enable
exit
```

Route Processor Redundancy の確認

```
show redundancy states
show crypto pki server
show crypto pki certificates tname
```

Route Processor Redundancy SSO モードの設定例

サーバー側の設定例：

```
asr1k(config)#ip http server

asr1k(config)#crypto pki trustpoint ROOTCA

asr1k(ca-trustpoint)#hash sha512

asr1k(ca-trustpoint)#revocation-check none

asr1k(ca-trustpoint)#rsakeypair  ROOTCA 2048

asr1k(ca-trustpoint)#crypto pki server ROOTCA

asr1k(cs-server)#issuer-name CN=ROOTCA C=pki

asr1k(cs-server)#lifetime certificate 00 00 15

asr1k(cs-server)#lifetime ca-certificate 00 00 25

asr1k(cs-server)#lifetime crl 6

asr1k(cs-server)#serial-number 0x1

asr1k(cs-server)#auto-rollover 00 00 24

% The archive password is not configured. Rollover CA keys and certificates will not be
 automatically archived.

asr1k(cs-server)#grant auto

asr1k(cs-server)#database url tftp://<ip>//
```

```
% Server database url was changed. You need to move the
% existing database to the new location.
asr1k(cs-server)#database url p12 tftp://<ip>//
asr1k(cs-server)#database level complete
asr1k(cs-server)#database archive pkcs12 password <pwd>
asr1k(cs-server)#end
```

クライアント側の設定例：

```
crypto pki trustpoint client
 enrollment url http://<ip>:80
 usage ike
 subject-name CN=R1 C=pki
 revocation-check crl
 rsakeypair client 2048
 hash sha512
```

Route Processor Redundancy SSO モードの確認例

```
show redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
     Maintenance Mode = Disabled
    Manual Swact = enabled
 Communications = Up

   client count = 132
```

```
 client_notification_TMR = 30000 milliseconds

          RF debug mask = 0x0
```

show crypto pki server

```
Certificate Server ROOTCA:

    Status: enabled

    State: enabled

    Server's configuration is locked  (enter "shut" to unlock it)

    Issuer name: CN=ROOTCA C=pki

    CA cert fingerprint: F2BF3707 D9F6F5F3 E0D111D8 A8486437

    Granting mode is: auto

    Last certificate issued serial number (hex): 2

    CA certificate expiration timer: 14:15:50 IST Mar 31 2019

    CRL NextUpdate timer: 14:15:50 IST Mar 31 2019

    Current primary storage dir: tftp://9.45.3.3//

    Current storage dir for .p12 files: tftp://9.45.3.3//

    Database Level: Complete - all issued certs written as <serialnum>.cer

    Auto-Rollover configured, overlap period 0 days

    Autorollover timer: 13:51:50 IST Mar 31 2019

    Redundancy configured.  This is active.
```

（注） サーバーは、アクティブ RP でのみ有効であり、スタンバイモードでは無効状態になります。

show crypto pki certificates client

```
Certificate

  Status: Available

  Certificate Serial Number (hex): 03

  Certificate Usage: General Purpose

  Issuer:

    cn=ROOTCA C=pki

  Subject:

    Name: asr1k

    hostname=asr1k
```

```
    cn=R1 C=pki
  Validity Date:
    start date: 00:42:04 IST Mar 11 2019
    end   date: 01:02:04 IST Mar 11 2019
  Associated Trustpoints: client

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=ROOTCA C=pki
  Subject:
    cn=ROOTCA C=pki
  Validity Date:
    start date: 00:40:34 IST Mar 11 2019
    end   date: 00:40:34 IST Mar 9 2020
  Associated Trustpoints: client
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。