使用AAA和證書身份驗證通過IKEv2到ASA的AnyConnect

目錄

簡介

本檔案介紹如何使用AnyConnect IPsec(IKEv2)以及憑證和驗證、授權及計量(AAA)驗證將PC連線到思科調適型安全裝置(ASA)。

> **附註**：本文檔中提供的示例僅介紹用於獲取ASA和AnyConnect之間的IKEv2連線的相關部分。未提供完整配置示例。本檔案沒有說明或不需要網路位址轉譯(NAT)或存取清單組態。

準備連線

本節介紹在將PC連線到ASA之前所需的準備。

具有正確EKU的證書

必須注意的是，儘管ASA和AnyConnect組合不要求使用RFC，但要求證書具有擴展金鑰使用(EKU):

- ASA的證書必須包含**server-auth** EKU。
- PC的證書必須包含**client-auth** EKU。

> **附註**：具有最新軟體修訂版的IOS路由器可以將EKU置於證書上。

ASA上的配置

本節介紹連線發生之前所需的ASA配置。

> **附註**：Cisco Adaptive Security Device Manager(ASDM)允許您僅按一下幾次即可建立基本配置。思科建議您使用它以避免錯誤。

加密對映配置

以下是密碼編譯對應範例組態：

```
crypto dynamic-map DYN 1 set pfs group1
crypto dynamic-map DYN 1 set ikev2 ipsec-proposal secure
crypto dynamic-map DYN 1 set reverse-route
crypto map STATIC 65535 ipsec-isakmp dynamic DYN
crypto map STATIC interface outside
```

IPsec提議

以下是IPsec方案示例配置：

```
crypto ipsec ikev2 ipsec-proposal secure
 protocol esp encryption aes 3des
 protocol esp integrity sha-1
crypto ipsec ikev2 ipsec-proposal AES256-SHA
 protocol esp encryption aes-256
 protocol esp integrity sha-1
```

IKEv2策略

以下是IKEv2策略示例配置：

```
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
```

```
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
```

使用者端服務和憑證

您必須在正確的介面（本例中為外部介面）上啟用客戶端服務和證書。以下是組態範例：

```
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint OUTSIDE
ssl trust-point OUTSIDE outside
```

附註：安全套接字層(SSL)也指定了相同的信任點，這是預期的和必需的。

啟用AnyConnect配置檔案

必須在ASA上啟用AnyConnect配置檔案。以下是組態範例：

```
webvpn
 enable outside
anyconnect image disk0:/anyconnect-win-3.0.5080-k9.pkg 1 regex "Windows NT"
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect enable
tunnel-group-list enable
```

使用者名稱、組策略和隧道組

以下是ASA上基本使用者名稱、組策略和隧道組的配置示例：

```
group-policy GroupPolicy_AC internal
group-policy GroupPolicy_AC attributes
 dns-server value 4.2.2.2
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
default-domain value cisco.com
webvpn
anyconnect profiles value Anyconnect type user
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
tunnel-group AC type remote-access
tunnel-group AC general-attributes
address-pool VPN-POOL
 default-group-policy GroupPolicy_AC
tunnel-group AC webvpn-attributes
 authentication aaa certificate
 group-alias AC enable
 group-url https://bsns-asa5520-1.cisco.com/AC enable
 without-csd
```

AnyConnect配置檔案

以下是相關部分以粗體顯示的示例配置檔案:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
```

```
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
 "http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false
 </AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="true">Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>




        bsns-asa5520-1
<HostAddress>bsns-asa5520-1.cisco.com</HostAddress>
<UserGroup>AC</UserGroup>
<PrimaryProtocol>IPsec</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

以下是有關此組態範例的一些重要說明：

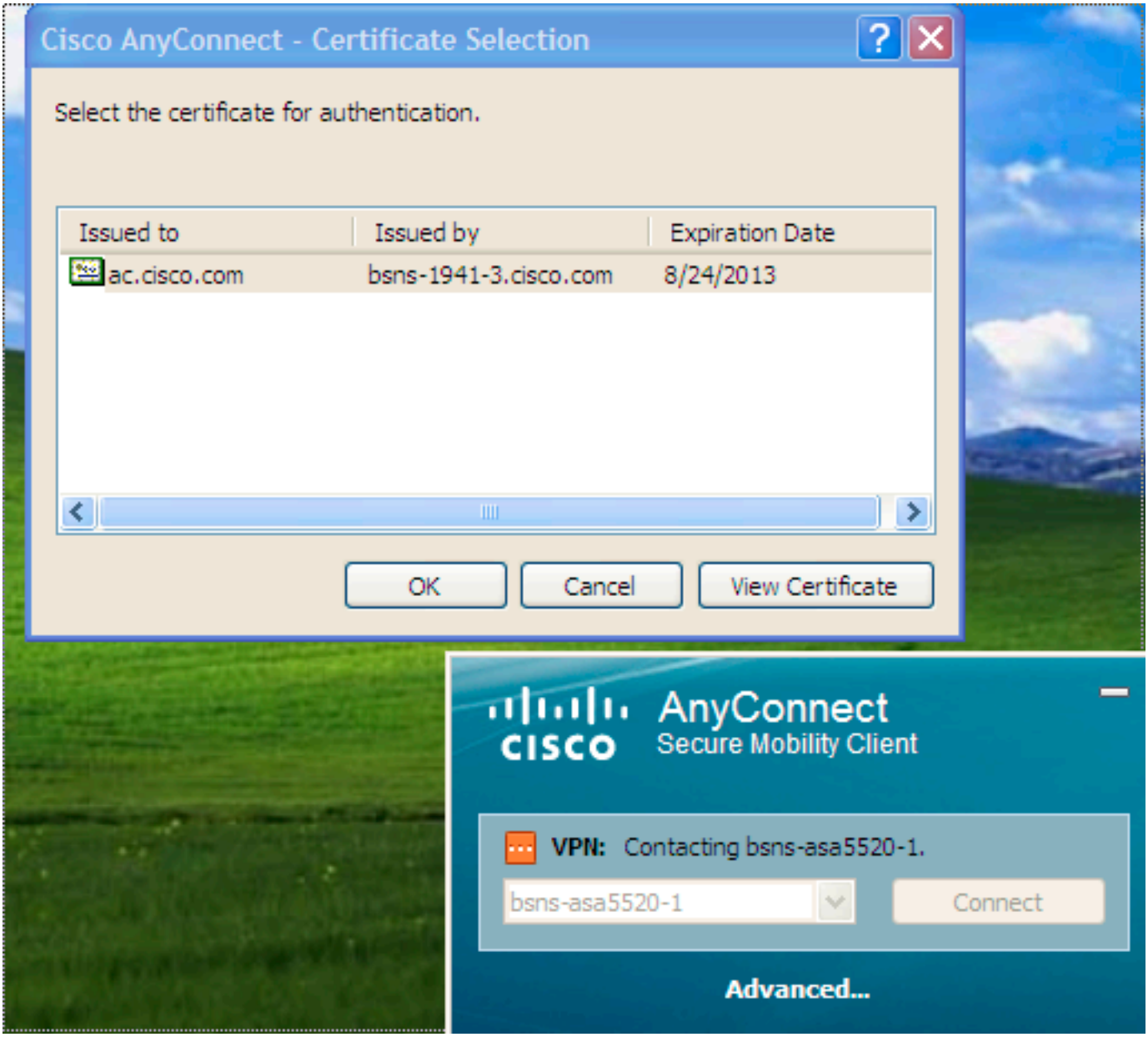
- 建立配置檔案時，HostAddress必須與用於IKEv2的證書上的證書名稱(CN)匹配。輸入**crypto ikev2 remote-access trustpoint** 命令以定義此屬性。
- UserGroup必須與IKEv2連線所屬隧道組的名稱匹配。如果它們不匹配，連線經常會失敗，並且調試指示Diffie-Hellman(DH)組不匹配或類似的假負值。

建立連線

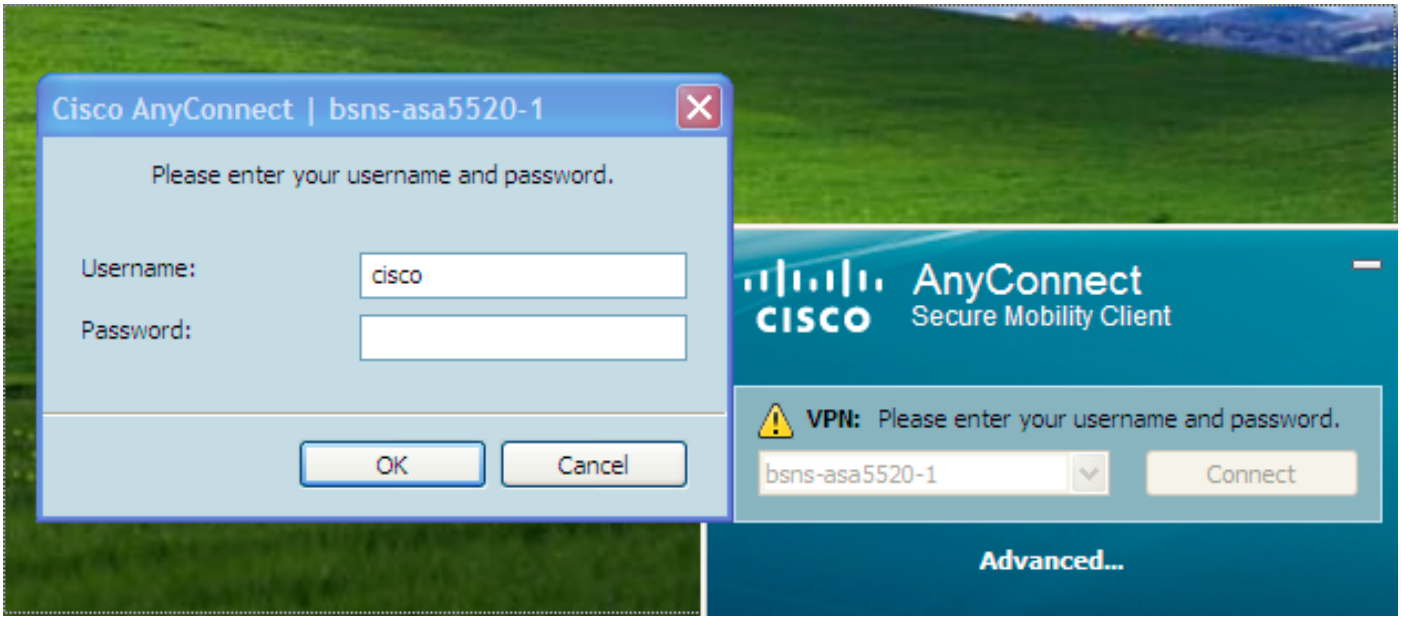
本節介紹配置檔案存在時的PC到ASA連線。

> **附註**：您在GUI中輸入的資訊是AnyConnect配置檔案中配置的<HostName>值。在這種情況下，會輸入**bsns-asa5520-1**，而不是完整的完全限定域名(FQDN)。

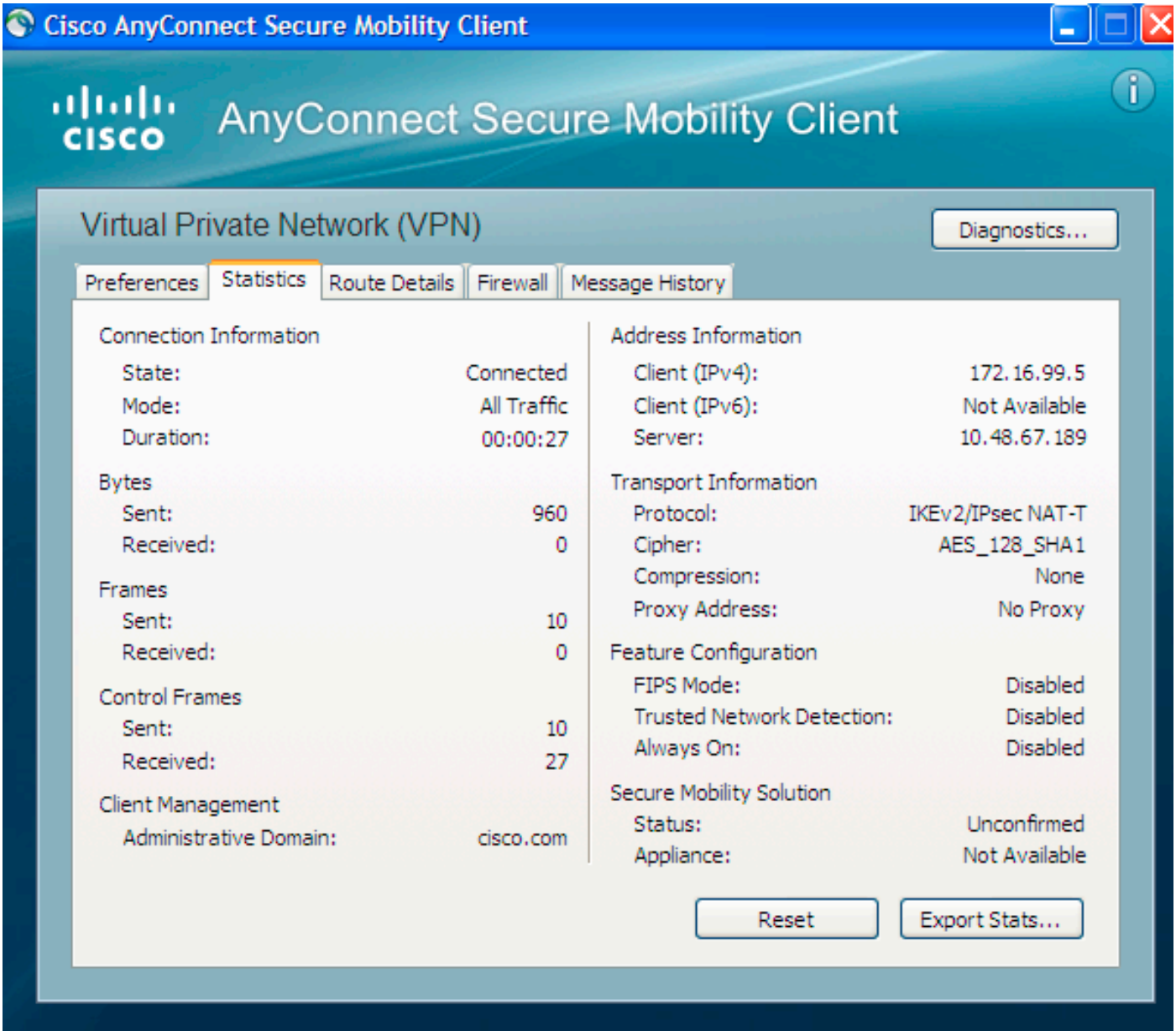
首次嘗試通過AnyConnect連線時，網關會提示您選擇證書（如果禁用了自動證書選擇）：



然後必須輸入使用者名稱和密碼：



接受使用者名稱和密碼後，連線成功，可以驗證AnyConnect統計資訊：



驗證ASA

在ASA上輸入以下命令以驗證連線是否使用IKEv2以及AAA和證書身份驗證：

```
bsns-asa5520-1# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed
Username : cisco Index : 6
Assigned IP : 172.16.99.5 Public IP : 1.2.3.4
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : AES256 AES128 Hashing : none SHA1 SHA1
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_AC Tunnel Group : AC
Login Time : 15:45:41 UTC Tue Aug 28 2012
Duration : 0h:02m:41s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 6.1
Public IP : 1.2.3.4
Encryption : none Auth Mode : Certificate and userPassword
 Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Client Type : AnyConnect
Client Ver : 3.0.08057
IKEv2:
Tunnel ID : 6.2
UDP Src Port : 60468 UDP Dst Port : 4500
Rem Auth Mode: Certificate and userPassword
 Loc Auth Mode: rsaCertificate
 Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86238 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
Client OS : Windows
IPsecOverNatT:
Tunnel ID : 6.3
Local Addr : 0.0.0.0/0.0.0.0/0/0
Remote Addr : 172.16.99.5/255.255.255.255/0/0
Encryption : AES128 Hashing : SHA1\
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 28638 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 27 Minutes
Bytes Tx : 0 Bytes Rx : 960
Pkts Tx : 0 Pkts Rx : 10
```

已知警告

以下是已知警告以及與本文檔中所述資訊相關的問題：

- IKEv2和SSL信任點必須相同。
- 思科建議您使用FQDN作為ASA端證書的CN。確保在AnyConnect配置檔案中<HostAddress>引用相同的FQDN。

- 連線時請記得從AnyConnect配置檔案中插入<HostName>值。
- 即使在IKEv2配置中，當AnyConnect連線到ASA時，也會通過SSL下載配置檔案和二進位制更新，但不會通過IPsec下載。
- 通過IKEv2到ASA的AnyConnect連線使用EAP-AnyConnect，這是一種允許更簡單實施的專有機制。