CHAPTER 14

サポートするツールと高度な概念

この章では、Broadband Access Center（BAC）の保守、および製品のインストール、配備、使用の高速化と改善に役立つツールとその使用方法について説明します。

この章では、次のトピックについて説明します。

（注） この項では、ツールの使用方法の例をいくつか示します。多くの場合、ツールのファイル名には *BPR_HOME* と指定されたパスが含まれます。これは、デフォルトのホーム ディレクトリ位置を示しています。

BAC ツール

BAC には、特定の機能をより効率的に実行するための自動ツールが用意されています。表 14-1 に、この BAC リリースでサポートされている各種ツールを示します。

表 14-1　BAC ツール

ツール	説明	参照先
設定ファイル　ユーティリティ	BAC のテンプレートと設定ファイルをテスト、検証、および表示するために使用されます。	設定ファイル ユーティリティの使用方法（P.5-23）
BAC プロセス ウォッチドッグ	BAC ウォッチドッグ デーモンと連動して BAC システム コンポーネントの状態を監視し、サーバを停止または起動します。	コマンドラインからの BAC プロセス ウォッチドッグの使用方法（P.9-2）
RDU ログ レベル ツール	RDU のログ レベルを設定し、デバッグ ログ出力をイネーブルまたはディセーブルにします。	RDU ログ レベル ツールの使用方法（P.10-5）
PacketCable 証明書ツール	KDC で動作するために必要とされる KDC 証明書をインストールおよび管理します。	PKCert.sh ツールの使用方法（P.14-3）
KeyGen ツール	PacketCable サービス キーを生成します。	KeyGen ツールの使用方法（P.14-9）
Network Registrar のプロパティ変更ツール	Cisco Network Registrar DHCP サーバに組み込まれる BAC 拡張が使用するキー設定プロパティを変更するために使用されます。	changeNRProperties.sh ツールの使用方法（P.14-11）
SNMP エージェント設定ツール	SNMP エージェントを管理します。	snmpAgentCfgUtil.sh ツールの使用方法（P.10-11）
診断ツール	システム パフォーマンスおよびトラブルシューティングに関連するサーバ データを収集します。	診断ツールによるトラブルシューティング（P.16-6）
BundleState.sh ツール	サポート拡大のサーバ状態に関連した診断データを組み込みます。	サポートを受けるためのサーバ状態のバンドル（P.16-11）
ディスク容量監視ツール	1 つまたは複数のファイル システムのしきい値を設定します。これらのしきい値を超えると、追加のディスク領域が利用可能になるまでアラートが生成されます。	disk_monitor.sh ツールの使用方法（P.14-13）

PKCert.sh ツールの使用方法

PKCert ツールにより、KDC 証明書とそれに対応する秘密鍵を作成します。また、証明書チェーンを検証し、コピーして、名前を KDC で要求される名前に変更することもできます。

（注）　このツールは、KDC コンポーネントがインストールされている場合にのみ使用可能です。

PKCert ツールの実行

PKCert ツールを動作させるには PKCert.sh コマンドを実行します。このコマンドは、デフォルトで *BPR_HOME/kdc* ディレクトリにあります。

シンタックスの説明　**PKCert.sh** *function option*

- *function*：実行する関数を指定します。次のオプションを選択できます。
  - ***-c***：KDC 証明書を作成します。P.14-3 の「KDC 証明書の作成」を参照してください。
  - ***-v***：PacketCable 証明書セットを検証および正規化します。P.14-4 の「KDC 証明書の検証」を参照してください。
  - **-z**：*pkcert.log* ファイルに保存されるデバッグ出力のログ レベルを設定します。P.14-5 の「デバッグ出力のログ レベルの設定」を参照してください。

（注）　これらのオプションの使用方法が不明な場合は、***-?*** と指定してヘルプ情報を表示できます。

- *option*：選択する関数に応じて、オプションの関数を実装します。

KDC 証明書の作成

KDC 証明書を作成するには、次の手順に従います。

ステップ 1　*/opt/CSCObac/kdc* にディレクトリを変更します。

ステップ 2　次の構文を使用して PKCert.sh ツールを実行します。

PKCert.sh -s *dir* **-d** *dir* **-c** *cert* **-e -r** *realm* **-a** *name* **-k** *keyFile* [**-n** *serial#*] [**-o**]

- **-s** *dir*：作成元ディレクトリを指定します
- **-d** *dir*：作成先ディレクトリを指定します
- **-c** *cert*：サービス プロバイダーの証明書（DER 暗号化）を使用します
- **-e**：証明書を Euro-PacketCable 証明書として指定します
- **-r** *realm*：KDC 証明書の Kerberos レルムを指定します
- **-a** *name*：KDC の DNS 名を指定します
- **-k** *keyFile*：サービス プロバイダーの秘密鍵（DER 暗号化）を使用します
- **-n** *serial#*：証明書のシリアル番号を設定します
- **-o**：既存ファイルに上書きします

新しい証明書が作成およびインストールされると、その新しい証明書により、サブジェクトの代替名フィールドのレルムが指定されます。新しい証明書は現在の環境に対して固有であり、その環境には次の要素が含まれます。

- KDC レルム。
- マルチメディア ターミナル アダプタ（MTA）が使用する KDC に関連付けられた DNS 名。

例

```
# ./PKCert.sh  -c "-s . -d /opt/CSCObac/kdc/solaris/packetcable/certificates
-k CLCerts/Test_LSCA_privkey.der -c CLCerts/Test_LSCA.cer -r PCTEST.CISCO.COM -n 100
-a kdc.pctest.cisco.com -o"
Pkcert Version 1.0
Logging to pkcert.log
Source Directory: .
Destination Directory: /opt/CSCObac/kdc/solaris/packetcable/certificates
Private Key File: CLCerts/Test_LSCA_privkey.der
Certificate File: CLCerts/Test_LSCA.cer
Realm: PCTEST.CISCO.COM
Serial Number: 100
DNS Name of KDC: kdc.pctest.cisco.com
WARNING - Certificate File will be overwritten
SP Cert subject name: C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01
CableLabs Local System CA
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/KDC_private_key.pkcs8
File written:
/opt/CSCObac/kdc/solaris/packetcable/certificates/KDC_private_key_proprietary.
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/KDC_PublicKey.der
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/KDC.cer
KDC Certificate Successfully Created at
/opt/CSCObac/kdc/solaris/packetcable/certificates/KDC.cer
```

このコマンドを使用すると、*/opt/CSCObac/kdc/solaris/packetcable/certificates/KDC.cer* ファイルと */opt/CSCObac/kdc/solaris/packetcable/certificates/KDC_private_key.pkcs8* ファイルが作成されます。この KDC 証明書では、レルムが PCTEST.CISCO.COM に、シリアル番号が 100 に、KDC サーバの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が kdc.pctest.cisco.com に設定されます。

KDC 証明書の検証

このコマンドにより、指定された作成元ディレクトリのすべてのファイルを調べ、X.509 証明書としての識別を試みます。正規の X.509 証明書が見つかると、ファイルの名前が適正に変更され、作成先ディレクトリにコピーされます。特定の目的（サービス プロバイダーまたはデバイス）での正規の証明書チェーンが複数特定されると、エラーが生成されます。この場合は、作成元ディレクトリから余分な証明書を削除し、もう一度コマンドを実行する必要があります。

（注） **PKCert.sh -v -?** コマンドを入力すると、PKCert ツールを使用した KDC 証明書の検証方法の指示が表示されます。

KDC 証明書を検証するには、次の手順に従います。

ステップ 1　*/opt/CSCObac/kdc* にディレクトリを変更します。

ステップ 2　次の構文を使用して PKCert.sh ツールを実行します。

PKCert.sh -v -s *dir* **-d** *dir* **-r** *dir*

- **-s** *dir*：作成元ディレクトリを指定します
- **-d** *dir*：作成先ディレクトリを指定します
- **-o**：既存のすべてのファイルに上書きします
- **-r** *dir*：参照証明書ディレクトリを指定します

検証は、このパッケージに組み込まれた参照証明書に対して実行されます。**-d** オプションを指定する場合、証明書は名前を正規化して作成先ディレクトリにインストールされます。

例

```
# ./PKCert.sh  -v "-s /opt/CSCObac/kdc/TestCerts -d
/opt/CSCObac/kdc/solaris/packetcable/certificates -o"
Pkcert Version 1.0
Logging to pkcert.log
Output files will overwrite existing files in destination directory

Cert Chain(0)    Chain Type: Service Provider
[Local File]                          [Certificate Label]
[PacketCable Name]
CableLabs_Service_Provider_Root.cer   CableLabs_Service_Provider_Root.cer
Service_Provider.cer                  Service_Provider.cer
Local_System.cer                      Local_System.cer
KDC.cer                               KDC.cer

Cert Chain(1)    Chain Type: Device
[Local File]                          [Certificate Label]
[PacketCable Name]
MTA_Root.cer                          MTA_Root.cer
File written:
/opt/CSCObac/kdc/solaris/packetcable/certificates/CableLabs_Service_Provider_Root.cer
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/Service_Provider.cer
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/Local_System.cer
File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/KDC.cer

Service Provider Certificate Chain Written to Destination Directory
/opt/CSCObac/kdc/solaris/packetcable/certificates


File written: /opt/CSCObac/kdc/solaris/packetcable/certificates/MTA_Root.cer

Device Certificate Chain Written to Destination Directory
/opt/CSCObac/kdc/solaris/packetcable/certificates
```

デバッグ出力のログ レベルの設定

このコマンドにより、*BPR_HOME/kdc* ディレクトリの *pkcert.log* に記録されるデバッグ出力のログ レベルを設定できます。ログ ファイルのデータを使用して、要求されたタスクの実行中に発生した問題のトラブルシューティングを行うことができます。

デバッグ出力のログ レベルを設定するには、次の手順に従います。

ステップ 1　*/opt/CSCObac/kdc* にディレクトリを変更します。

ステップ 2　次の構文を使用して PKCert.sh ツールを実行します。

PKCert.sh -s *dir* **-d** *dir* **-k** *keyFile* **-c** *cert* **-r** *realm* **-a** *name* **-n** *serial#* **-o** {**-z error** | **info** | **debug**}

- **-s** *dir*：作成元ディレクトリを指定します

- **-d** *dir*：作成先ディレクトリを指定します
- **-k** *keyFile*：サービス プロバイダーの秘密鍵（DER 暗号化）を使用します
- **-c** *cert*：サービス プロバイダーの証明書（DER 暗号化）を使用します
- **-r** *realm*：KDC 証明書の Kerberos レルムを指定します
- **-a** *name*：KDC の DNS 名を指定します
- **-n** *serial#*：証明書のシリアル番号を設定します
- **-o**：既存ファイルに上書きします
- **-z** : *pkcert.log* ファイルに保存されるデバッグ出力のログ レベルを設定します。次の値を選択できます。
  - **error**：エラー メッセージのロギングを指定します。
  - **info**：情報メッセージのロギングを指定します。
  - **debug**：デバッグ メッセージのロギングを指定します。これはデフォルト設定です。

例

例 1

この例では、ログ レベルがエラー メッセージの収集に設定されています。

```
# ./PKCert.sh  -c "-s /var/certsInput -d /var/certsOutput -k
/var/certsInput/Local_System.der -c /var/certsInput/Local_System.cer -r
PCTEST.CISCO.COM -n 100 -a kdc.pctest.cisco.com -o -z error"
Pkcert Version 1.0
Logging to pkcert.log
Source Directory: /var/certsInput
Destination Directory: /var/certsOutput
Private Key File: /var/certsInput/Local_System.der
Certificate File: /var/certsInput/Local_System.cer
Realm: PCTEST.CISCO.COM
Serial Number: 100
DNS Name of KDC: kdc.pctest.cisco.com
Setting debug to error
WARNING - Certificate File will be overwritten
SP Cert subject name: C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01
CableLabs Local System CA
File written: /var/certsOutput/KDC_private_key.pkcs8
File written: /var/certsOutput/KDC_private_key_proprietary.
File written: /var/certsOutput/KDC_PublicKey.der
File written: /var/certsOutput/KDC.cer
KDC Certificate Successfully Created at /var/certsOutput/KDC.cer

Copy KDC.cer to the KDC certificate directory (i.e.
/opt/CSCObac/kdc/solaris/packetcable/certificates)
Copy KDC_private_key.pkcs8 to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
Copy KDC_private_key_proprietary. to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
```

例 2

この例では、ログ レベルが情報メッセージの収集に設定されています。

```
# ./PKCert.sh -c "-s /var/certsInput
> -d /var/certsOutput
> -k /var/certsInput/Local_System.der
> -c /var/certsInput/Local_System.cer
> -r PCTEST.CISCO.COM
> -n 100
> -a kdc.pctest.cisco.com
> -o -z info"
 INFO [main] 2007-05-02 06:32:26,280 (PKCert.java:97) - Pkcert Version 1.0
Pkcert Version 1.0
Logging to pkcert.log
Source Directory: /var/certsInput
Destination Directory: /var/certsOutput
Private Key File: /var/certsInput/Local_System.der
Certificate File: /var/certsInput/Local_System.cer
Realm: PCTEST.CISCO.COM
Serial Number: 100
DNS Name of KDC: kdc.pctest.cisco.com
Setting debug to info
 INFO [main] 2007-05-02 06:32:26,289 (PKCCreate.java:69) - PKCCreate startup
WARNING - Certificate File will be overwritten
 INFO [main] 2007-05-02 06:32:26,291 (PKCCreate.java:341) - WARNING - Certificate File
will be overwritten
SP Cert subject name: C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01
CableLabs Local System CA
File written: /var/certsOutput/KDC_private_key.pkcs8
File written: /var/certsOutput/KDC_private_key_proprietary.
File written: /var/certsOutput/KDC_PublicKey.der
File written: /var/certsOutput/KDC.cer
KDC Certificate Successfully Created at /var/certsOutput/KDC.cer

Copy KDC.cer to the KDC certificate directory (i.e.
/opt/CSCObac/kdc/solaris/packetcable/certificates)
Copy KDC_private_key.pkcs8 to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
Copy KDC_private_key_proprietary. to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
```

例 3

この例では、ログ レベルがデバッグに設定されています。

（注） サンプル出力は、説明のために省略されています。

```
# ./PKCert.sh -c "-s /var/certsInput -d /var/certsOutput -k
/var/certsInput/Local_System.der -c /var/certsInput/Local_System.cer -r
PCTEST.CISCO.COM -n 100 -a kdc.pctest.cisco.com -o -z debug"
 INFO [main] 2007-05-02 06:32:06,029 (PKCert.java:97) - Pkcert Version 1.0
Pkcert Version 1.0
Logging to pkcert.log
Source Directory: /var/certsInput
Destination Directory: /var/certsOutput
Private Key File: /var/certsInput/Local_System.der
Certificate File: /var/certsInput/Local_System.cer
Realm: IPFONIX.COM
Serial Number: 100
DNS Name of KDC: bacdev3-dpe-4.cisco.com
Setting debug to debug
 INFO [main] 2007-05-02 06:32:06,038 (PKCCreate.java:69) - PKCCreate startup
WARNING - Certificate File will be overwritten
```

```
 INFO [main] 2007-05-02 06:32:06,039 (PKCCreate.java:341) - WARNING - Certificate File
will be overwritten
DEBUG [main] 2007-05-02 06:32:06,054 (PKCert.java:553) - Characters Read: 1218
DEBUG [main] 2007-05-02 06:32:06,056 (PKCert.java:583) - Binary File:
/var/certsInput/Local_System.der Read. Length: 1218
DEBUG [main] 2007-05-02 06:32:06,062 (PKCert.java:553) - Characters Read: 943
DEBUG [main] 2007-05-02 06:32:06,063 (PKCert.java:583) - Binary File:
/var/certsInput/Local_System.cer Read. Length: 943
DEBUG [main] 2007-05-02 06:32:06,064 (PKCert.java:455) - Jar File Path:
/opt/CSCObac/lib/pkcerts.jar
DEBUG [main] 2007-05-02 06:32:06,065 (PKCert.java:456) - Opened jar file:
/opt/CSCObac/lib/pkcerts.jar
DEBUG [main] 2007-05-02 06:32:06,067 (PKCert.java:460) - Jar entry unfiltered:
Tag_Packetcable_Tag/
DEBUG [main] 2007-05-02 06:32:06,068 (PKCert.java:460) - Jar entry unfiltered:
Tag_Packetcable_Tag/CableLabs_Service_Provider_Root.cer
...
DEBUG [main] 2007-05-02 06:32:06,115 (PKCert.java:472) - File:
Tag_Packetcable_Tag/Manu.cer
DEBUG [main] 2007-05-02 06:32:06,116 (PKCert.java:472) - File:
Tag_Packetcable_Tag/Service_Provider.cer
DEBUG [main] 2007-05-02 06:32:06,121 (PKCCreate.java:91) - Found 7 files in jar.
DEBUG [main] 2007-05-02 06:32:06,827 (KDCCert.java:98) - SP Cert subject name:
C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01 CableLabs Local System CA
SP Cert subject name: C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01
CableLabs Local System CA
DEBUG [main] 2007-05-02 06:32:07,687 (KDCCert.java:293) - Setting issuer to:
C=US,O=CableLabs\, Inc.,OU=ABC Cable Company,CN=Shared-01 CableLabs Local System CA
DEBUG [main] 2007-05-02 06:32:07,699 (KDCCert.java:231) - DERVisibleToGeneral
org.bouncycastle.asn1.DERGeneralString@bd0b4ea6

DEBUG [main] 2007-05-02 06:32:07,700 (KDCCert.java:231) - DERVisibleToGeneral
org.bouncycastle.asn1.DERGeneralString@5035bc0

DEBUG [main] 2007-05-02 06:32:07,701 (KDCCert.java:231) - DERVisibleToGeneral
org.bouncycastle.asn1.DERGeneralString@5035bc0

DEBUG [main] 2007-05-02 06:32:07,703 (KDCCert.java:210) - DERCombineTagged [0]
IMPLICIT
    DER ConstructedSequence
        ObjectIdentifier(1.3.6.1.5.2.2)
        Tagged [0]
            DER ConstructedSequence
                Tagged [0]
                    org.bouncycastle.asn1.DERGeneralString@5035bc0
                Tagged [1]
                    DER ConstructedSequence
                        Tagged [0]
                            Integer(2)
                        Tagged [1]
                            DER ConstructedSequence
                                org.bouncycastle.asn1.DERGeneralString@bd0b4ea6
                                org.bouncycastle.asn1.DERGeneralString@5035bc0

File written: /var/certsOutput/KDC_private_key.pkcs8
File written: /var/certsOutput/KDC_private_key_proprietary.
File written: /var/certsOutput/KDC_PublicKey.der
File written: /var/certsOutput/KDC.cer
KDC Certificate Successfully Created at /var/certsOutput/KDC.cer

Copy KDC.cer to the KDC certificate directory (i.e.
/opt/CSCObac/kdc/solaris/packetcable/certificates)
Copy KDC_private_key.pkcs8 to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
Copy KDC_private_key_proprietary. to the KDC platform directory (i.e.
/opt/CSCObac/kdc/solaris)
```

KeyGen ツールの使用方法

KeyGen ツールを使用して PacketCable サービス キーを生成します。サービス キーは、KDC 通信で必要な Triple Data Encryption Standard（triple DES または 3DES）対称キー（共有秘密情報）です。KDC サーバでは、DPE のプロビジョニング FQDN ごとにサービス キーを必要とします。DPE コマンドライン インターフェイス（CLI）から DPE プロビジョニング FQDN に変更を加えるには、対応する変更を KDC サービス キーのファイル名でも行う必要があります。この変更が必要なのは、KDC サービス キーではそのファイル名の一部として DPE プロビジョニング FQDN が使用されるからです。

KeyGen ツールは、*BPR_HOME/kdc* ディレクトリにあり、DPE プロビジョニング FQDN、レルム名、およびパスワードのコマンドライン引数を使用し、サービス キー ファイルを生成します。

（注）　このツールを実行する場合は、DPE で（DPE CLI から **service packetCable** *1..1* **registration kdc-service-key** コマンドを使用して）サービス キーを生成するために使用したのと同じパスワードを入力してください。このパスワードの設定方法の詳細については、『*Cisco Broadband Access Center DPE CLI Reference 4.0*』を参照してください。

KDC サーバは起動時にサービス キーを読み取ります。サービス キーを修正するには、どんな場合でも KDC サーバを再起動する必要があります。

シンタックスの説明

keygen *options fqdn realm password*

- *options* は次のとおりです。
  - ***-?***：この使用方法メッセージを表示してコマンドを終了します。
  - ***-v*** または ***-version***：このツールのバージョンを表示してコマンドを終了します。
  - ***-q*** または ***-quiet***：出力が何も作成されないクワイエット モードを実装します。
  - ***-c*** または ***-cms***：CMS システムのサービス キーを作成します。
- *fqdn*：DPE の FQDN を指定します。必須の入力項目です。
- *realm*：Kerberos レルムを指定します。必須の入力項目です。
- *password*：使用するパスワードを指定します。これも必須のフィールドです。パスワードの長さは 6 ～ 20 文字にする必要があります。

このファイル名構文を使用して、次の 3 つのサービス キー ファイルが KDC キー ディレクトリに書き込まれます。

mtafqdnmap,*fqdn@REALM*

mtaprovsrvr,*fqdn@REALM*

krbtgt,*REALM@REALM*

- *fqdn*：DPE の FQDN を指定します。
- *REALM*：Kerberos レルムを指定します。

サービス キー ファイルには、必ずバージョン フィールド 0x0000 が含まれています。

例

```
# keygen dpe.cisco.com CISCO.COM changeme
```

このコマンドを実行すると、これらの KDC サービス キーが *BPR_HOME/kdc/solaris/keys* ディレクトリに書き込まれます。

```
mtafqdnmap,dpe.cisco.com@CISCO.COM
mtaprovsrvr,dpe.cisco.com@CISCO.COM
krbtgt,CISCO.COM@CISCO.COM
```

KDC を再起動し、新しいキーが認識されるようにします。次の BAC プロセス ウォッチドッグ コマンドを使用して KDC を再起動します。

```
# /etc/init.d/bprAgent restart kdc
```

ここでは、CMS サービス キーの生成例を示します。

```
# keygen -c cms-fqdn.com CMS-REALM-NAME changeme
```

このコマンドを実行すると、この CMS サービス キーが *BPR_HOME/kdc/solaris/keys* ディレクトリに書き込まれます。

```
cms,cms-fqdn.com@CMS-REALM-NAME
```

KDC サービス キーの検証

KDC と DPE でサービス キーを生成したら、両方のコンポーネントでサービス キーが一致するかどうかを検証します。

KeyGen ツールでは、**service packetCable** *1..1* **registration kdc-service-key** コマンドによって DPE でサービス キーを生成するために使用したのと同じパスワードを入力する必要があります。DPE でこのパスワードを設定した後は、*BPR_HOME/dpe/conf* ディレクトリにある *dpe.properties* ファイルからサービス キーを表示できます。*/pktcbl/regsvr/KDCServiceKey=* プロパティに対する値を見つけてください。

次に例を示します。

```
# more dpe.properties
/pktcbl/regsvr/KDCServiceKey=2e:d5:ef:e9:5a:4e:d7:06:67:dc:65:ac:bb:89:e3:2c:bb:
71:5f:22:bf:94:cf:2c
```

（注） この例の出力は、説明のために省略されています。

KDC で生成されたサービス キーを表示するには、*BPR_HOME/kdc/solaris/keys* ディレクトリから次のコマンドを実行します。

od -Ax -tx1 mtaprovsrvr,*fqdn@REALM*

- *fqdn*：DPE の FQDN を指定します。
- *REALM*：Kerberos レルムを指定します。

このコマンドによって生成される出力は、*dpe.properties* ファイルの */pktcbl/regsvr/KDCServiceKey=* プロパティの値と一致します。

次に例を示します。

```
# od -Ax -tx1 mtaprovsrvr,dpe.cisco.com@CISCO.COM
0000000 00 00 2e d5 ef e9 5a 4e d7 06 67 dc 65 ac bb 89
0000010 e3 2c bb 71 5f 22 bf 94 cf 2c
000001a
```

ここで示す例では、KDC で生成されたサービス キーが DPE のサービス キーと一致しています。

changeNRProperties.sh ツールの使用方法

BAC インストール プログラムは、Network Registrar DHCP サーバに組み込まれる BAC 拡張によって使用される、設定プロパティの値を確立します。キー設定プロパティを変更するには、*BPR_HOME/cnr_ep/bin* ディレクトリの **changeNRProperties.sh** コマンドを使用します。

パラメータを何も指定せずにスクリプトを呼び出すと、設定可能なプロパティの一覧を示したヘルプ メッセージが表示されます。

このコマンドを実行するには、次の手順に従います。

ステップ 1　*BPR_HOME/cnr_ep/bin* にディレクトリを変更します。

ステップ 2　次の構文を使用して **changeNRProperties.sh** コマンドを実行します。

changeNRProperties.sh *options*

options は次のとおりです。

- **-help** : ヘルプ メッセージを表示します。**-help** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。
- **-ep enabled** | **disabled** : PacketCable プロパティをイネーブルまたはディセーブルにします。プロパティをイネーブルにするには **-ep enabled** と入力し、ディセーブルにするには **-ep disabled** と入力します。
- **-ec enabled | disabled** : CableHome プロパティをイネーブルまたはディセーブルにします。プロパティをイネーブルにするには **-ec enabled** と入力し、ディセーブルにするには **-ec disabled** と入力します。
- **-d** : 現在のプロパティを表示します。**-d** オプションは排他的に使用する必要があります。他のオプションと一緒に使用しないでください。
- **-s** *secret* : BAC 共有秘密情報を指定します。たとえば、共有秘密情報がワード *secret* である場合は、**-s secret** と入力します。
- **-f** *fqdn* : RDU FQDN を指定します。たとえば、完全修飾ドメイン名として rdu.example.com を使用する場合は、**-f rdu.example.com** と入力します。
- **-p** *port* : 使用する RDU ポートを指定します。たとえば、ポート番号 49187 を使用する場合は、**-p 49187** と入力します。
- **-r** *realm* : PacketCable レルムを指定します。たとえば PacketCable レルムが EXAMPLE.COM の場合は、**-r EXAMPLE.COM** と入力します。

（注）　レルムは大文字で入力する必要があります。

- **-g** *prov_group* : プロビジョニング グループを指定します。たとえば group1 というプロビジョニング グループを使用する場合は、**-g group1** と入力します。
- **-t 00** | **01** : PacketCable TGT をオフまたはオンに設定するかどうかを指定します。たとえば、TGT をオフに設定するには **-t 00** と入力し、オンに設定するには **-t 01** と入力します。
- **-a** *ip* : PacketCable プライマリ DHCP サーバのアドレスを指定します。たとえば、プライマリ DHCP サーバの IP アドレスが 10.10.10.2 の場合は、**-a 10.10.10.2** と入力します。
- **-b** *ip* : PacketCable セカンダリ DHCP サーバのアドレスを指定します。たとえば、セカンダリ DHCP サーバの IP アドレスが 10.10.10.4 の場合は、**-b 10.10.10.4** と入力します。必要に応じて、**-b null** と入力して NULL 値に設定することもできます。
- ***-y ip*** : PacketCable プライマリ DNS サーバのアドレスを指定します。たとえば、PacketCable のプライマリ DNS サーバの IP アドレスが 10.10.10.6 の場合は、***-y 10.10.10.6*** と入力します。

- ***-z ip*** : PacketCable セカンダリ DNS サーバのアドレスを指定します。たとえば、セカンダリ DNS サーバの IP アドレスが 10.10.10.8 の場合は、***-z 10.10.10.8*** と入力します。必要に応じて、**-z null** と入力して NULL 値に設定することもできます。
- **-o** *prov_ip man_ip* : 指定されたプロビジョニング アドレスによって識別される DPE との通信で使用する管理アドレスを設定します。たとえば、プロビジョニング グループの IP アドレスが 10.10.10.7 の場合は **-o 10.10.10.7 10.14.0.4** と入力します。必要に応じて NULL 値を入力することもでき、たとえば **-o 10.10.10.7 null** のように指定します。

ステップ 3　DHCP サーバを再起動します。

例

NR 拡張プロパティ ツールを使用することによって Network Registrar 拡張を変更する例を次に示します。

```
# /opt/CSCObac/cnr_ep_bin/changeNRProperties.sh -g primary1
Current NR Properties:
RDU Port: 49187
RDU FQDN: rdu.example.com
Provisioning Group: primary1
Shared Secret: fggTaLg0XwKRs
PacketCable Enable: enabled
CableLabs client TGT: 01
CableLabs client Realm: EXAMPLE.COM
CableLabs client Primary DHCP Server: 10.10.1.2
CableLabs client Secondary DHCP Server: NOT SET
CableLabs client Primary DNS Server: 10.10.1.2
CableLabs client Secondary DNS Server: NOT SET
```

（注）　変更を有効にするには、NR DHCP サーバを再起動する必要があります。

現在のプロパティを表示する例を次に示します。

```
# /opt/CSCObac/cnr_ep_bin/changeNRProperties.sh -d
Current NR Properties:
RDU Port: 49187
RDU FQDN: rdu.example.com
Provisioning Group: primary1
Shared Secret: fggTaLg0XwKRs
PacketCable Enable: enabled
CableLabs client TGT: 01
CableLabs client Realm: EXAMPLE.COM
CableLabs client Primary DHCP Server: 10.10.1.2
CableLabs client Secondary DHCP Server: NOT SET
CableLabs client Primary DNS Server: 10.10.1.2
CableLabs client Secondary DNS Server: NOT SET
```

disk_monitor.sh ツールの使用方法

利用可能なディスク領域を監視することは、重要なシステム管理作業です。多数のカスタム スクリプトまたは市販のツールを使用して、この作業を実行できます。

disk_monitor.sh コマンドは、*BPR_HOME/rdu/samples/tools* ディレクトリにあり、1 つ以上のファイル システムのしきい値を設定します。これらのしきい値を超えると、追加のディスク領域が利用可能になるまで、60 秒ごとに Solaris の syslog 機能によってアラートが生成されます。

（注）　少なくとも、**disk_monitor.sh** スクリプトを使用して *BPR_DATA* および *BPR_DBLOG* ディレクトリを監視することをお勧めします。

シンタックスの説明

disk_monitor.sh *filesystem-directory x [filesystem-directory* x*]*

- *filesystem-directory*：監視するファイル システムのディレクトリを示します。
- *x*：指定したファイル システムに適用するしきい値をパーセントで示します。
- *filesystem-directory**：複数のファイル システムを示します。
- *x**：複数のファイル システムに適用するしきい値をパーセントで指定します。

例

例 1

この例では、*/var/CSCObac* ファイル システムの利用率が 80 パーセントに到達した場合に通知が送信されるように指定しています。

```
# ./disk_monitor.sh /var/CSCObac 80
```

データベース ログのディスク領域の利用率が 80 パーセントに達すると、次のようなアラートが syslog ファイルに送信されます。

```
Dec 7 8:16:06 perf-u80-1 BPR: [ID 702911 local6.warning] File system /var/bpr usage is
81% (threshold is 80%)
```

例 2

この例では、disk_monitor.sh ツールをバックグラウンド プロセスとして実行する方法を示しています。コマンドの終わりにアンパサンド（&）を指定すると、バックグラウンドでのプロセスの実行中に出力がただちに返されます。

```
# ./disk_monitor.sh /var/CSCObac 80 &
1020
```