CHAPTER 2

Before Installing Cisco Broadband Access Center

This chapter explains how to prepare for a successful installation of Cisco BAC and describes:

Cisco BAC Components

The Cisco BAC component installation program prompts you to install:

- Regional Distribution Unit (RDU)

  The RDU is the primary server in the Cisco BAC provisioning system. You should install the RDU on a server that fulfills the requirements that are described in Chapter 1, "Overview."

  The RDU:

  - Manages the generation of device configurations.
  - Processes application programming interface (API) requests for all Cisco BAC functions.
  - Manages the Cisco BAC system.

  When you install the RDU, the installation program also installs the administrator user interface. The program also preloads required data into the RDU database, and starts the RDU daemon through the Cisco BAC process watchdog. The SNMP agent is also installed for the RDU. For details on configuring the SNMP agent, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*. For information on the Cisco BAC process watchdog, see the *Cisco Broadband Access Center Administrator Guide 4.2*.

- Device Provisioning Engine (DPE)

  The DPE is the major component of the provisioning group, handling all device interactions with the RDU. You should install a DPE on a server that meets the requirements described in Chapter 1, "Overview."

  The DPE:

  - Caches device configurations generated at the RDU.
  - Manages various CPE protocol services. These services obtain their operating instructions from the instruction cache.

  The installation program installs a CLI on your system to help configure the DPE. The Cisco BAC process watchdog and the SNMP agent are installed for the DPE also. For information on configuring the DPE and configuring the SNMP agent, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

  Note The DPE is separately licensed and must be installed from the administrator user interface. For details on licensing in this Cisco BAC release and how to install your license, see Licensing Cisco BAC, page 5-1.

- Cisco Network Registrar extensions

  The Cisco Network Registrar extensions are the link between Cisco BAC and Cisco Network Registrar. You should install this component on all Cisco Network Registrar servers in your Cisco BAC environment. If you are deploying Cisco BAC in a failover environment, ensure that you install the extensions on the failover servers also.

  Note You must install the Cisco Network Registrar extensions on a server running Cisco Network Registrar 7.2.

- Key Distribution Center (KDC)

  The KDC, along with the DPE registration service, handles the authentication of PacketCable voice technology MTAs. For performance reasons, install the KDC on a separate server that meets the requirements described in Chapter 1, "Overview."

  Note The KDC is required only when configuring a system to support voice technology operations using Secure PacketCable. The BASIC.1 and BASIC.2 packetcable voice technologies do not require KDC.

  The KDC requires service keys, which allow it to communicate with the DPE. For details, see the *Cisco Broadband Access Center DPE CLI Reference 4.2* and the *Cisco Broadband Access Center Administrator Guide 4.2*.

  Note The KDC requires a license, which continues to be proprietary, as in previous Cisco BAC releases, and is licensed during Cisco BAC installation. For information on installing a KDC license, see Installing Your KDC License, page 5-4.

Database Requirements

Before you install Cisco BAC, be aware of these database considerations:

- File-system block size
- Large file support

File-System Block Size

For optimum performance and reliability of the Cisco BAC database, configure the file system or systems that contain the database files and database log files with an 8 KB or greater block size. If your system configuration does not support an 8-KB block size, then configure the block size in multiples of 8 KB; for example, 16 KB or 32 KB.

Note The block size cannot be changed after the Unix File System (UFS) is mounted with a value. The value has to be set during Solaris disk partition.

ZFS is a new file system in Solaris 10 OS which provides excellent data integrity and performance compared to other file systems. The default block size for ZFS is 128 KB. In Cisco BAC, the RDU and DPE file system support a blocksize of 8 KB to 64 KB. So it is recommended to configure a block size of 8KB for optimal performance.

The installation program prompts you to specify a directory in which to install database files, and database transaction log files. These directories are identified in Cisco BAC with the system variables *BPR_DATA*, and *BPR_DBLOG,* respectively.

To verify that a directory resides on a file system with a minimum of 8-KB block size:

Step 1 Run the UNIX **mount** command without any parameters to determine on which file-system device the directory resides. The default directory is */var/CSCObac*.

For example:

```
# mount
/var on /dev/dsk/c0t0d0s4 read/write/setuid/intr/largefiles/logging/xattr/onerror=panic/
dev=2200004 on Thu Jun 15 16:58:21 2006
```

In this example, the file-system device is */dev/dsk/c0t0d0s4*.

Step 2 To determine the file-system block size, use the **df** command.

For example:

```
# df -g /dev/dsk/c0t0d0s4

/var     (/dev/dsk/c0t0d0s4):    8192 block size    1024 frag size
  961240 total blocks    851210 free blocks    755086 available    243712 total files
   239730 free files    35651588 filesys id
     ufs fstype    0x00000004 flag    255 filename length
```

In this example, the block size is 8192 bytes, which is 8 KB. The block size of the selected directory, therefore, is correct.

Large File Support

Ensure that the file system in which you place database files is configured to support files larger than 2 GB. To verify large file support:

Step 1 Run the UNIX **mount** command without parameters.

Step 2 Note whether the intended file system contains the keyword **largefiles**.

For example:

```
/var on /dev/dsk/c0t0d0s4 read/write/setuid/intr/largefiles/onerror=panic/dev=2200004 on
Thu Jun 15 08:07:53
```

In this example, the output contains the keyword **largefiles**. This file system, therefore, can support files larger than 2 GB.

High-level Installation and Startup

To ensure a smooth installation and startup process:

Step 1 Determine the computers and servers on which you are installing the Cisco BAC components.

Step 2 Verify the file-system block size of the directory in which you intend to install the Cisco BAC database and the database transaction log files. See Database Requirements, page 2-3.

Step 3 Review the installation checklist described in Table 3-1.

Step 4 Install the RDU. Ensure that you know the location for the:

- Home directory
- Data directory
- Database logs directory

Step 5 Install a DPE. Ensure that you know the location for the:

- Home directory
- Data directory
- Database logs directory

Step 6 After installing the RDU, ensure that you:

a. Obtain a valid Cisco BAC license file to provision all technologies. For details on obtaining and installing your license file, see Obtaining a Permanent License, page 5-2.

You still require separate licenses—permanent or evaluation—for the following Cisco BAC components:

- The DPE
- The KDC, if you configure your network to support secure packetcable voice technology

b. Verify that the RDU is running by starting the administrator user interface.

To launch the administrator user interface, enter the administrator's location from your web browser using:

http://*machine_name:port_number*/

Note To access the administrator user interface using HTTP over SSL, enter: https://*machine_name:port_number/*

- *machine_name*—Identifies the computer on which the RDU is running.
- *port_number*—Identifies the computer port on which the server side of the administrator application is running. By default, this port number is:
  - 8100 for HTTP over TCP
  - 8443 for HTTP over SSL

  The main login screen, appears.

c. Change the Cisco BAC administrator's password.

To change the password, enter the default username (**admin**) and password (**changeme**).

Click **Login**.

The Change Password screen appears.

Enter a new password; ensure that this password has at least 8 characters.

Click **Login**.

Step 7 Optionally, configure the syslog file for alerts. See Configuring the Syslog Utility to Receive Cisco BAC Alerts, page 7-1. You can set up the syslog file on any Cisco BAC component server.

Step 8 After installing the DPE, ensure that you:

a. Change the DPE login password and the privileged password from the command-line interface (CLI).

- To change the login password, access the CLI in the privileged mode, and enter:

```
bac_dpe# password password
```

  where *password* identifies the new DPE password.

- To change the DPE privileged password, enter:

```
bac_dpe# enable password password
```

  where *password* identifies the local configured password currently in effect or, optionally, provides a new password. If this parameter is omitted, you are prompted for the password.

  For more information, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

b. Configure the DPE from the CLI as required. For configuration instructions, see the *Cisco Broadband Access Center DPE CLI Reference 4.2*.

Step 9 Install and configure Cisco Network Registrar, if it is not already installed on your system. We recommend that you use Cisco Network Registrar 7.2. For more information on installing Cisco Network Registrar, see the *Installation Guide for Cisco Network Registrar 7.2*.

- When you install the Cisco Network Registrar Local Cluster (LCCM), ensure that you:
  a. Obtain a valid Cisco Network Registrar license file for the local cluster.
  b. Install Cisco BAC extensions on all Cisco Network Registrar local cluster servers. See Installing Cisco BAC, page 3-4.
  c. Configure Cisco Network Registrar, including its extensions. Specifically, you need to configure scopes, policies, client classes, and selection tags. See Configuring Extensions, page 3-17. Also see the *User Guide for Cisco Network Registrar 7.2*.

d. Configure the Cisco Network Registrar syslog for alerts and debugging information. See Configuring the Syslog Utility to Receive Cisco BAC Alerts, page 7-1.

e. Validate the installation by connecting to the Cisco Network Registrar web UI and viewing it.

- When you install Cisco Network Registrar Regional Cluster (RCCM), ensure that you:

  a. Identify the master server for Cisco Network Registrar Regional Installation, which administers all the configured Cisco Network Registrar local clusters. This server can be Solaris, Windows, or Linux. However, we recommend that you have the Solaris operating system on the Cisco Network Registrar Regional Server.

  b. Obtain a valid central-cluster license file for the Cisco Network Registrar Regional Server.

  c. After you install the Cisco BAC extensions on all Cisco Network Registrar local servers, replicate the local data into regional and pull the replica address space. For more information, see the *User Guide for Cisco Network Registrar 7.2*.

     Alternatively, you can also create subnets, client classes, policies, and so on at RCCM and push them to the required LCCM DHCP server. For more information, see the *User Guide for Cisco Network Registrar 7.2*.

Step 10 Install and configure the KDC. When you install the KDC, ensure that you:

- Obtain a valid Cisco BAC license. The KDC license is proprietary and is licensed during Cisco BAC installation. For information on installing the KDC license, see Licensing Cisco BAC, page 5-1.
- Have the following information at hand:
  - KDC realm—Identified by a unique name, the KDC realm consists of a KDC and the clients and servers registered to that KDC.

    Note The realm must match the certificate chain at the KDC.

  - KDC FQDN—Identifies the fully qualified domain name on which the KDC server is located.
  - KDC interface address—Identifies the interface (generally the IP address of the KDC server) on which the KDC listens for requests.