CHAPTER 13

# Troubleshooting Security

The following topics are covered in this chapter:

- Troubleshooting NICI
  - Deleting corrupt NICI files
  - Creating new NICI keys
- Troubleshooting server certificates
- Troubleshooting user certificates
- Troubleshooting the CA
- Troubleshooting the tree key

Chapter 2 went into great detail about the eDirectory security infrastructure and all of its associated objects. This chapter will not repeat that information. Instead, this chapter focuses on different troubleshooting techniques for the key security components. These security components are part of eDirectory's own built-in security infrastructure and enable you to do the following in eDirectory:

- Create server-specific keys
- Generate tree keys
- Encrypt and decrypt data with the generated keys
- Create and sign certificates for servers and users
- Configure applications to use SSL communication

This chapter is designed to help you troubleshoot problems that you may encounter while performing these activities.

# Troubleshooting NICI

NICI is the core of eDirectory security. All keys and certificates are based on the server NICI keys. Each server has a unique set of keys. The NICI keys are created for the server when NICI is installed for the first time. The NICI keys are not stored within eDirectory. They are stored on the file system of the local server.

It is critical to ensure that all NICI keys are protected and backed up on a regular basis. The most critical server is the server that is the certificate authority (CA). If this server loses its NICI keys, the entire security infrastructure will have to be re-created.

---

■ **Note** NICI keys are not re-created when NICI is upgraded or reinstalled. When eDirectory is removed from a server, the NICI keys still remain. The only way to remove the NICI keys is to manually delete them from the file system.

---

When NICI first loads, it looks for the NICI server keys. If the keys are present, it uses the keys to initialize the main NICI engine. If the keys are valid, NICI will successfully initialize. If there is something wrong with the keys, NICI may load but it will not initialize. Both NDS and PKI require NICI to be initialized before they can initialize. A fast way to determine whether NICI initialized correctly is to look for NICI (14xx) errors when the PKI and NDS modules load. You will find the errors by taking the following action, per platform:

- *NetWare*: Load and unload PKI.NLM and DS.NLM and look for errors on the Logger screen.
- *Windows*: Launch the %SystemDrive%:\Novell\Nds\NDSCons.exe file. Stop and start ds.dlm. You will see NICI errors on the console screen.
- *Linux, Solaris, HP-UX, and AIX (*nix)*: Look in the /var/nds/ndsd.log file and look for NICI errors on the NDSD *and* PKI processes.

If NICI errors occur when the DS and PKI modules load, there are three possible issues:

- The NICI files are missing
- The NICI files are corrupt