N1 Provisioning Server 3.1, Blades Edition, Installation Guide

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817–4072–10
March, 2004

040219@7940

Contents

Preface

The *N1 Provisioning Server 3.1, Blades Edition, Installation Guide* describes the process of connecting the Sun Fire™ B1600 Blade system Chassis and associated equipment, installing or upgrading the N1 Provisioning Server software, and performing initial configuration and validation of an N1™ Infrastructure Fabric (I-Fabric).

This guide is part of a four-volume implementation reference set. The set should be read in the following order:

- *N1 Provisioning Server 3.1, Blades Edition, Release Notes*
- *N1 Provisioning Server 3.1, Blades Edition, Installation Guide*
- *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*
- *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*

Who Should Use This Book

This guide is intended for system administrators who are responsible for installing or upgrading the N1 Provisioning Server software. The system administrators are expected to have the following background:

- Knowledge of Sun/Solaris, Linux, and Microsoft Windows, and the network administration tools provided by each operating environment
- Knowledge of network equipment and network devices from a variety of vendors such as Sun and Cisco
- Knowledge of network device interconnections and cabling

Before You Read This Book

Sun recommends that you take the following Sun Education courses before installing the N1 Provisioning Server software:

- N1 Provisioning Server 3.1 Blades Edition Deployment
- N1 Provisioning Server 3.1 Blades Edition Administration

How This Book Is Organized

- Chapter 1 provides an overview of N1 Provisioning Server 3.1, Blades Edition architecture, components, features, and concepts.
- Chapter 2 lists the hardware and software requirements for the B1600 Blade System Chassis, the N1 Provisioning Server machine, the gigabit Ethernet cards, external Ethernet switches, and third-party software.
- Chapter 3 provides the guidelines and procedures for connecting the blade system chassis to the N1 Provisioning Server machine and to the external Ethernet switches, switch and chassis configuration, operating system installation, and patch installation.
- Chapter 4 describes how to do a first-time installation of the N1 Provisioning Server software.
- Chapter 5 describes how to upgrade from N1 Provisioning Server 3.0, Blades Edition to N1 Provisioning Server 3.1, Blades Edition.
- Chapter 6 describes how to validate the N1 Provisioning Server installation, and migrate N1 Provisioning Server data from the Oracle database to the PostgreSQL database.
- Chapter 7 describes how to uninstall N1 Provisioning Server software.
- Appendix A provides a summary of the installation main menu.
- Appendix B lists the packages that are installed and provides a short description of each package.
- Glossary provides definitions of the terms used in the N1 Provisioning Server environment.

Related Books

- *Sun Fire B1600 Blade System Chassis Hardware Installation Guide*
- *Sun Fire B1600 Blade System Chassis Software Setup Guide*
- *Sun Fire B1600 Blade System Chassis Administration Guide*
- *Sun Fire B1600 Blade System Chassis Switch Administration Guide*
- *N1 Provisioning Server 3.1, Blades Edition, Release Notes*
- *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*
- *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*

Accessing Sun Documentation Online

The docs.sun.com[SM] Web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. The URL is `http://docs.sun.com`.

Ordering Sun Documentation

Sun Microsystems offers select product documentation in print. For a list of documents and how to order them, see "Buy printed documentation" at `http://docs.sun.com`.

Typographic Conventions

The following table describes the typographic changes used in this book.

TABLE P–1 Typographic Conventions

Typeface or Symbol	Meaning	Example
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `machine_name% you have mail.`
`AaBbCc123`	What you type, contrasted with on-screen computer output	`machine_name%` **`su`** `Password:`
AaBbCc123	Command-line placeholder: replace with a real name or value	To delete a file, type **`rm`** *filename*.
AaBbCc123	Book titles, new words, or terms, or words to be emphasized.	Read Chapter 6 in *User's Guide*. These are called *class* options. You must be *root* to do this.

Shell Prompts in Command Examples

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, and Korn shell.

TABLE P–2 Shell Prompts

Shell	Prompt
C shell prompt	`machine_name%`
C shell superuser prompt	`machine_name#`
Bourne shell and Korn shell prompt	`$`
Bourne shell and Korn shell superuser prompt	`#`

CHAPTER 1

N1 Provisioning Server Overview

This chapter provides overviews of N1™ Provisioning Server architecture and components, concepts, software, security, and the implementation and installation process.

This chapter discusses the following topics:

Architecture and Components

The N1 Provisioning Server consists of various hardware components, such as one or more blade system chassis, server blades, servers, switches and the N1 Provisioning Server software. N1 Provisioning Server software combines your computing and networking resources into a contiguous automated fabric of infrastructure called an *I-Fabric*, and controls how I-Fabric components interoperate.

N1 Provisioning Server software enables you to manage and control I-Fabric components, and to partition, allocate and assign server blades to specific accounts that are known as a *logical server farms*. I-Fabric resources are dedicated to a server farm until returned to the common *resource pool*. With root access to devices, you can deploy any software or application onto the server blades within a farm. Secure partitions enforced by N1 Provisioning Server software and methodologies enable you to exercise independent administrative control over each farm.

The following sections provide descriptions of the physical and logical components of an N1 Provisioning Server Blades Edition system.

Physical Components

The following diagram is an example of the hardware that comprises a typical N1 Provisioning Server system.

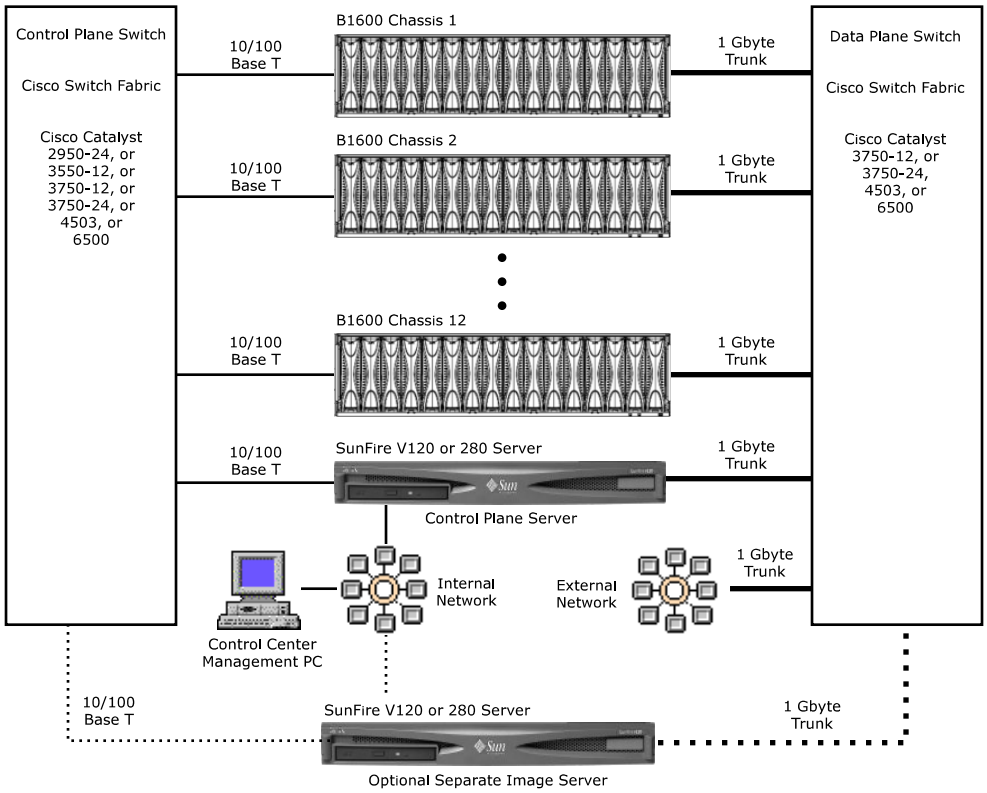

FIGURE 1–1 Representative N1 Provisioning Server System

The following sections describe the hardware components shown by the above diagram.

Sun Fire B1600 Blade System Chassis

Each blade system chassis contains the following components:

- One or two chassis switch and system controllers (SSCs). An SSC must be installed in SSC0 in each chassis.
- One or more of the following server blades:
  - B100s: SPARC architecture, Solaris Operating System
  - B100x: Single processor x86 architecture, Solaris x86 or Linux operating system
  - B200x: Dual processor x86 architecture, Solaris x86 or Linux operating system

Note – The B200x blade occupies 2 chassis slots and is treated as an unmanaged device.

- B10n: Content Load balancing blade
- B10p: SSL Proxy blade

Note – The SSL proxy blade is treated as an unmanaged device.

Each blade system chassis can support up to 8 B200x server blades, or 16 single-slot server blades.

Control Plane Server

The control plane server hosts all N1 Provisioning Server software, which includes the control plane software, the control plane database (CPDB), the Control Center server and database, the Control Center software, and, in a standard install, the N1 Provisioning Image Server.

Control Center Management PC

The Control Center Management PC provides access to the Control Center software using a web browser-based user interface. The Control Center is used to design and deploy logical server farms, and to define numerous characteristics including network topology, storage requirements, monitors, and alerts. The Control Center is also used to define the kinds of monitoring you want to perform. The monitoring definition is saved using the Monitoring Mark-up Language (MML).

N1 Image Server

The N1 Image Server (N1 IS) is used to store operating system disk images for each type of server blade in a chassis, and to load the disk images to server blades using the JumpStart™ and Flash archives depending on the type of server blade and operating system. The image server is typically installed on the control plane server. If desired, the image server can be installed on a separate machine.

Note – For best results, use a Gigabit copper Network Interface Card (NIC) for the image server.

Control Plane Switch and Data Plane Switch

The control plane switch connects all management and control interfaces on a designated control subnet and virtual local area network (VLAN). The control plane switch is optional only for a single blade system chassis installation in which the chassis contains a single switch and system controller (SSC). The control plane switch is required for an installation if any chassis contains two SSCs or if there is more than one chassis.

The data plane switch provides connectivity between the control plane Server, the N1 image server, the blade system chassis SSCs and server blades, and your network.

Logical Components

The following diagram shows a representative example of the N1 Provisioning Server after N1 Provisioning Server software has been installed.

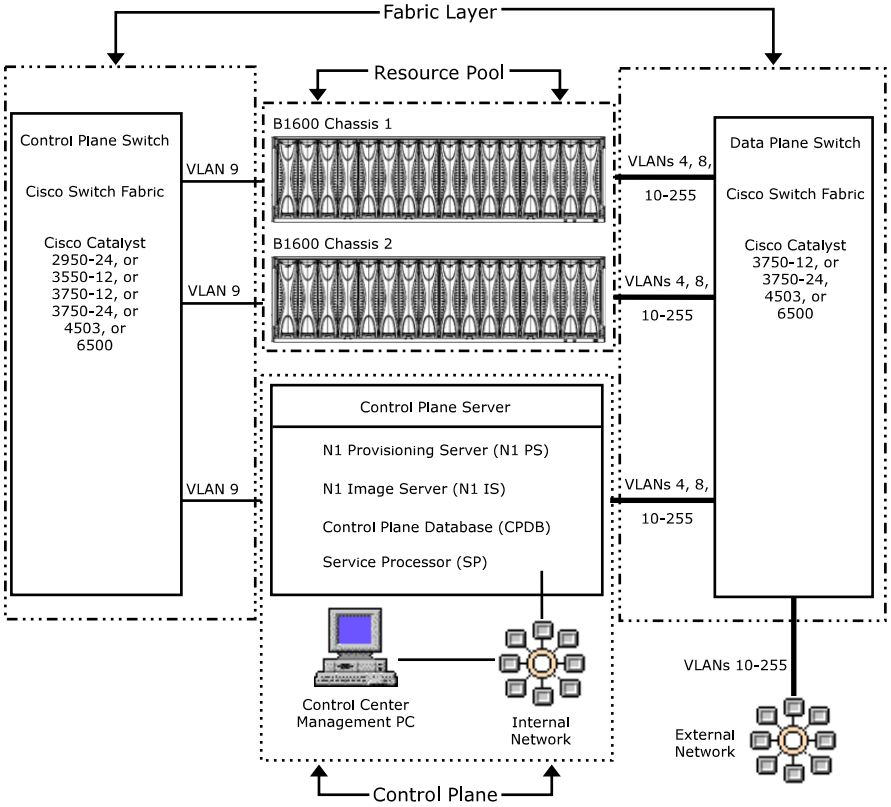

FIGURE 1–2 Example of N1 Provisioning Server System After N1 Provisioning Server Software Installation

The following sections describe the logical components of the N1 Provisioning Server, Blades Edition.

Resource Pool

The Resource Pool contains a one-blade to twelve-blade blade system chassis. Each chassis contains server blades that you can provision to a server farm. The resource pool within an I-Fabric starts out as a blank physical infrastructure with no predefined logical structure. The infrastructure can be configured into many different logical structures under the control of the N1 Provisioning Server software. The different logical structures, called *logical server farms*, are dynamic and securely partitioned.

The following diagram shows an example of the Resource Pool (unallocated server blades) and two farms (allocated server blades).

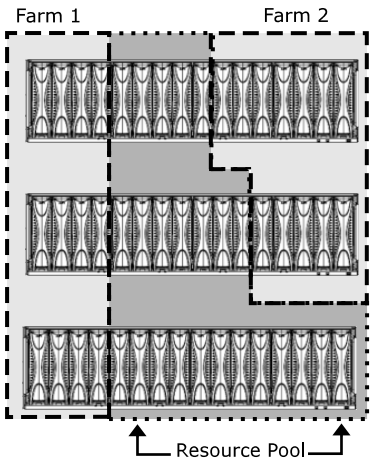

FIGURE 1–3 Example Server Farms and Resource Pool

Each server blade in a farm is allocated to the farm as an individual server, and securely networked to prevent access from other server farms. When the user is finished using a farm, the server blades that were assigned to the farm are returned to the Resource Pool.

Control Plane

The control plane provides intelligence, management, and control of an I-Fabric. The N1 Provisioning Server software, providing the intelligence that enables an I-Fabric, resides within the control plane. The control plane consists of all N1 Provisioning Server software and hardware, third-party software and hardware, and the N1 Provisioning Server databases. The control plane does not include the resource pool and fabric layer. If desired, you can also connect an optional terminal server to the control plane to provide access to all device's console ports.

The control plane resides on a private virtual local area network (VLAN) that ensures that the control plane is securely partitioned from access by unauthorized servers or any external network traffic. N1 Provisioning Server software manages devices within an I-Fabric through secure out-of-band connections over Ethernet or serial connections.

The control plane software automates the configuration of the Ethernet switch connections and assignment of VLANs to the I-Fabric components. The automated management of VLANs enables you to securely add or remove devices in the resource pool from any network topology designed through the Control Center. Additional security is provided by the assignment of one or more VLANs to a farm. A VLAN assigned to one farm cannot be used by a different farm.

The N1 Provisioning Server VLAN assignments are as follows:

- VLAN 1 – reserved
- VLAN 2 – reserved
- VLAN 3 – reserved
- VLAN 4 – assigned to I-Fabric devices that are not allocated to a farm
- VLAN 5 – reserved
- VLAN 6 – reserved
- VLAN 7 – reserved
- VLAN 8 – assigned to disk image transfers from the N1 image server to server blades
- VLAN 9 – assigned to control plane command traffic
- VLANs 10 through 255 – available for farm allocation

Fabric Layer

The fabric layer contains the networking infrastructure that ties the resource pool together. The switched fabric consists of industry-standard Ethernet switching components that provide connectivity to devices within the resource pool and connectivity to internal networks, and optionally, the Internet.

The Ethernet switches provide connectivity to devices within the resource pool as well as network connectivity to the Internet or internal networks. Through the automated management of VLANs on an Ethernet switch, you can add or remove devices in the resource pool from any network topology designed using the Control Center.

N1 Provisioning Server Concepts

This section provides summaries of the major N1 Provisioning Server logical components.

Administration

Administrative functionality for N1 Provisioning Server software and an I-Fabric is available in two forms: through the Administration screen within the Control Center and alternatively, by a set of command-line interface tools that interface directly with the Control Center.

Control Center

The Administration screen is the central point of administration within the Control Center. Using the Control Center from the Control Center Management PC, you can define classes of users that have access to the administration screen and its associated functionality. From the Control Center Administration screen, you have a comprehensive view of all users and logical server farms within an I-Fabric. You can do the following tasks from the Control Center Administration screen:

- Create and delete logical server farms
- Create and delete accounts
- Set usage limits
- Set user and administrator access privileges
- Add and remove logical server farms
- Add images to the image repository
- Remove images from the image repository
- Create and remove contracts
- Publish pertinent news items to accounts

You also can manage security rights and administration privileges from the Administration screen. The Control Center has three levels of access privileges:

- User Level – A standard user level that permits access to logical server farms within an account
- Account Manager Level – A manager within an account that permits the ability to add and delete users within an account
- Administrator – The highest level of access that permits access to the entire I-Fabric (including the control plane) as well as all accounts

For more information about the Control Center, see *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*.

For more information about access privileges, see "Applying Role-Based Access Control" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

Command-Line Tools

The command-line tools provide an interface to the Control Center that is used for managing an I-Fabric in conjunction with the Control Center administration functionality. The tools offer a more granular level of control, and also provide an interface for accessing devices and configuration data.

The tools are commonly used to view and track resources within an I-Fabric. Using the command line tools, you can:

- Check the state of any devices within an I-Fabric

- Trace details, such as physical Ethernet connectivity, from the network interface port in the device back to the physical port on the Ethernet switch within an I-Fabric
- Track and manage the logical assignment of physical devices and ports to logical server farms
- Manage VLANs and subnets within logical server farms
- Update the physical resource pool of an I-Fabric

When a device, such as a server blade, is added to an I-Fabric, the command-line tools facilitate the wiring and configuration auditing required for integrating the new device into the available resource pool. Command-line tools also assist in the management of software images, the reconfiguration of devices, and the activation and updating of logical server farms.

For a list of the available command-line tools and a brief description of each tool, Appendix B, Command-Line Tools in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

Resource and Network Virtualization

An important aspect of the design of N1 Provisioning Server software is the virtualization provided for all the hardware devices within the resource pool of an I-Fabric. This virtualization enables the rapid and dynamic association of devices to network connectivity and provides the capability to create a logical server farm from a pool of physical devices within an I-Fabric. Virtualization of network connectivity provides the foundation for deploying drag-and-drop connectivity between devices that can then be logically wired together.

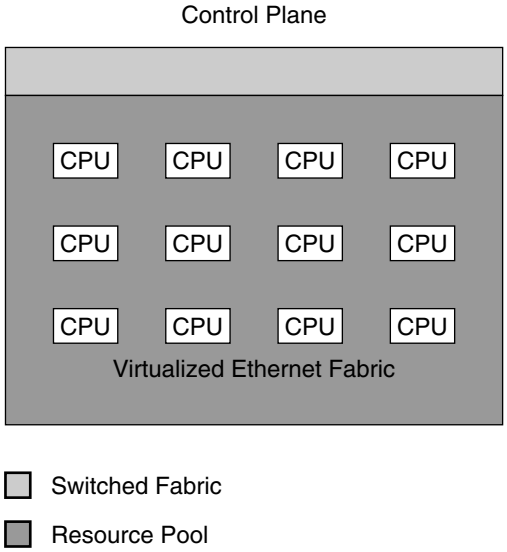

FIGURE 1–4 Control Plane Resource Virtualization

Virtualization of the network provides security, and enables the transparent management, configuration, and allocation of network devices. N1 Provisioning Server software utilizes VLANs and automates all aspects of VLAN configuration to enable network virtualization.

Network virtualization provides two distinct benefits:

- Customized virtual wiring is created for each logical server farm. N1 Provisioning Server Network virtualization enables you to create arbitrary network topologies, associate subnet addresses, and assign IP addresses to servers and network devices placed on the subnets. You can add and remove resources from the logical server farm while automatically configuring newly added and existing devices in the logical server farm as necessary.
- For provisionable devices, the N1 Provisioning Server software performs secure partitioning at the Layer 2 network layer by taking sets of network ports on a large-scale switched fabric and placing them on a protected Layer 2 virtual network. Each virtual network uses physical port-based virtual local area network (VLAN) technology built into current generation Layer 2 switches.

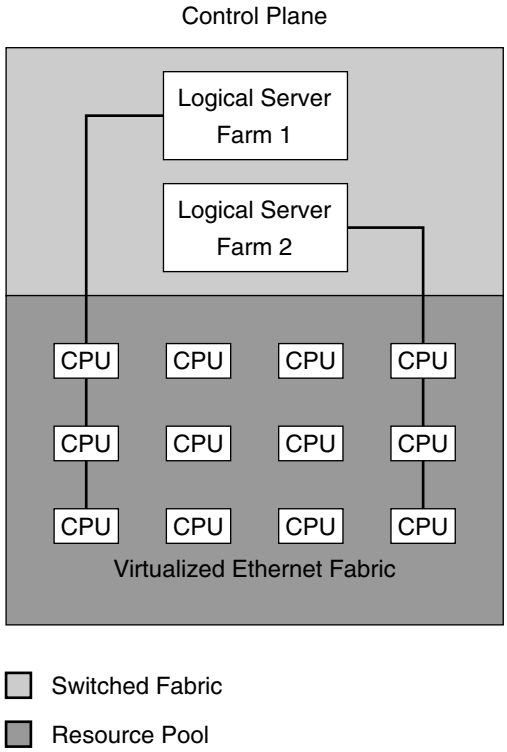

FIGURE 1–5 Control Plane Network Virtualization

Logical Server Farms

The control plane, switched fabric, and resource pool work together to dynamically create logical server farms within an I-Fabric. Logical server farms are securely allocated from the Resource Pool and managed by N1 Provisioning Server software. N1 Provisioning Server software creates server farms from the resources available within the Resource Pool. Logical server farms are built using the same physical resources as traditional server farms but they are established and managed under the flexible control of N1 Provisioning Server software. Logical server farms are analogous to traditional, manually built, dedicated server farms except that you can create, grow, shrink, and delete them as data structures that reside within N1 Provisioning Server software.

Logical server farms have the same performance and control characteristics as traditional server farms. N1 Provisioning Server software is not in the data path and does nothing to limit the performance of the devices or prevent the logical server farm from running at wire speed.

Secure partitions enforced by N1 Provisioning Server software and methodologies enable you to exercise independent administrative control over each logical server farm. Even though the user of a specific logical server farm has full administrative access on all devices within that farm, the user cannot view, access, or modify the devices or data associated with a different logical server farm.

The following graphic illustrates the life cycle of a logical server farm in the Control Center.

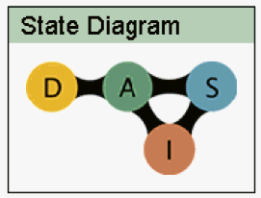

FIGURE 1–6 Logical Server Farm States

- **D** – Design State
- **A** – Active State
- **S** – Standby State
- **I** – Inactive State

For more details on how to manage logical server farms, see Chapter 4, "Building, Updating, and Monitoring Server Farms" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*.

Description Languages

A logical server farm within an I-Fabric is constructed from a number of basic building blocks. Capturing a logical description of these building blocks and their interrelationships enables the creation of a digital blueprint that specifies a farm's logical structure. This logical blueprint facilitates the automation of many manual tasks involved in constructing logical server farms.

N1 Provisioning Server software uses the following three description languages to capture logical descriptions of server farms:

- Farm Mark-Up Language (FML)

  FML is an XML dialect used to represent the logical blueprint of a logical server farm. FML is scalable and capable of describing, with a high degree of abstraction, network and configuration data for servers within a logical server farm.

  The general structure of FML is to describe an I-Fabric as a structure composed of sets of devices that have both connectivity as well as configuration-related information. The connectivity information describes how these various devices are interconnected, for example, how device Ethernet ports are connected to specific

subnets and VLANs. In addition to devices and their interconnectivity, FML provides the ability to describe roles that servers may occupy within a logical server farm, for example, a web server, database server, and application server. This ability enables the Control Center to deploy multiple instances of a given server within a logical server farm.

FML also enables the replication of entire logical server farms. Such replication might be required for creating site mirrors at different geographic locations, implementing business continuance solutions, or for creating a testing and staging area for a future version of a logical server farm.

- Monitoring Mark-Up Language (MML)

  MML is an XML dialect that describes monitor deployments and configurations as defined using the Control Center. MML describes monitoring configurations as they pass from the control center to the provisioning server.

- Wiring Mark-Up Language (WML)

  WML is an XML dialect that describes the physical wiring characteristics within an I-Fabric. WML is also used to describe the physical wiring of an I-Fabric. The difference between FML and WML is that FML describes the logical device wiring of a logical server farm and layout, whereas WML describes the physical wiring of all the devices present within an I-Fabric.

Network Packages

N1 Provisioning Server software runs with the following network packages:

- Packet filtering – `TSPRipf`

  The `TSPRipf` tool filters IP packets based on configurable packet characteristics, such as protocol, port number, source address, or destination address. Each service processor has one packet filtering tool installed to prevent malformed or malicious packets from one account's network entering another account's network or the Control Center network. The tool is statically configured by the Control Center at installation time. The default configuration denies any packets not specifically used by the Control Center.

- Network API – `TSPRnetcf`

  This API defines the Java™ interfaces for networking configuration on the Control Center server. The network API supports the DHCP and DNS protocols.

- DHCP – `TSPRdhcp`

  The DHCP protocol implementation is based on the public domain package from the Internet Software Consortium (http://www.isc.org). The service processor uses the DHCP facility to configure the servers in a logical server farm with their hostname and IP addresses. The DHCP configuration information for a logical server farm is stored in the control plane database (CPDB) for persistency and ease of migrating a logical server farm from one service processor to another. The information in the CPDB is used to create the DHCP configuration file

`/etc/dhcp.conf` at logical server farm activation time.

In the service processor, the `TSPRdhcp` utility assigns IP addresses and parameters to hosts, thus enabling the setup of IP addresses and parameters without having to modify or reboot the host. The utility does not allocate IP addresses. IP addresses are allocated by the Farm Manager.

Note – Do not edit the `dhcpd.conf` file. `dhcpd.conf` is maintained by the N1 Provisioning Server software.

- DNS – `TSPRdns`

  The DNS protocol implementation is based on the public domain package from the Internet Software Consortium (http://www.isc.org). The service processor uses the DNS facility for hostname resolution for servers and network devices in a logical server farm. The service processor that owns the logical server farm also serves as the DNS server for the logical server farm. The DNS information is stored in the CPDB for persistency and ease of migrating a logical server farm from one service processor to another. The information in the CPDB is used to create the DNS configuration file `etc/named.conf` at logical server farm activation time.

Note – Do not manually edit the `named.conf`. `named.conf` is dynamically updated by the service processor.

Hardware Abstraction Layer

Hardware Abstraction Layers (HALs) are sets of application programming interfaces (APIs) that provide device independence for the Control Center software. HALs are used to automate the interaction with physical devices within an I-Fabric. The HAL module translates abstract Control Center actions into device-specific commands. HALs might provide interfaces to specific manufacturer's Ethernet switches.

Because the Control Center software deals with only the abstract behavior of the device, HALs enable the Control Center software to manage different devices that exhibit the same overall behavior but might differ in how they are configured and managed. This difference could exist because the equipment is from different manufacturers or because of differences between current and next-generation products.

Provisioning Server Software

The Provisioning Server software resides on the control plane server and provides the infrastructure automation services required to manage and deploy logical server farms within an I-Fabric. At a high level, the Control Center manages the logical-to-physical mappings between a logical server farm and the physical resources assigned to it. The Control Center also provides an extensive command-line interface (CLI) for I-Fabric and farm management.

Provisioning Server Features

The N1 Provisioning Server software provides the following services.

- Management of all of the blade system chassis and server blades
- DNS resolution for the subnetwork on which it is installed
- Management of both internal and external IP addresses and subnets for the N1 Provisioning Server network

---

Note – N1 Provisioning Server software controls the contents of the `/etc/dhcpd.conf` and `/etc/named.conf` files. Any manual edits to these files are overwritten by the N1 Provisioning Server software.

- Management of the N1 Provisioning Server virtual local area networks (VLANs)
- Distribution and installation of operating system master images to blades in a farm

  The installation program includes a base Solaris Operating System image for booting and running server blades. You can make changes to the base image and then take a snapshot of the new image. This snapshot becomes a new image.

The N1 Provisioning Server software does not offer the following functions:

- Server blade and SSC firmware maintenance and upgrade
- Control plane switch and data plane switch management

  The N1 Provisioning Server software manages only the blade system chassis server blades and SSCs. You must connect and configure the control plane and data plane switches before you install the N1 Provisioning Server software.

Components

The Provisioning Server contains the following software components:

- Service processor (SP)
- Control plane database (CPDB)
- Image server

Service Processor

The Service Processor (SP) provides a variety of infrastructure management services such as provisioning, network virtualization, and monitoring. It contains the following subcomponents:

- Segment Manager

  The Segment Manager controls and coordinates activities for an I-Fabric, and is the only entry point to state transitions in the Control Center. The Segment Manager selects and sets the logical server farm ownership at logical server farm activation time, monitors the Farm Manager process, and sends requests to Farm Managers in the I-Fabric. Each time a request for the logical server farm arrives, a Farm Manager is started. There is one Farm Manager process per logical server farm. The Segment Manager starts the Farm Manager process as needed. See the command-line tools man pages for details.

- Farm Manager

  Farm Managers instantiate, monitor, and control activities related to logical server farms. A single service processor instance can contain many different Farm Manager processes. Each Farm Manager is assigned to one logical server farm. Farm Managers are only present when a change in a logical server farm occurs. Farm Managers communicate through the Segment Manager and through information stored and retrieved from the CPDB.

  Farm Managers use logical descriptions of logical server farms stored in the CPDB in the form of an FML document to identify all resources required for the logical server farm. Farm Managers request resources from the idle pool of resources such as servers.

- Dynamic Host Configuration Protocol (DHCP) and Domain Name Server (DNS) services

  The service processor uses the DHCP facility to configure the servers in a logical server farm with their hostname and Internet Protocol (IP) addresses. The service processor uses the DNS facility for hostname resolution for servers and network devices in a logical server farm.

- Storage Manager Client (STMC)

  The STMC loads global images onto server blades and administers snapshots. The STMC also provides the interfaces required by the Farm Manager to access the storage functionality. The STMC also contains tools that perform the individual storage functions. These tools are available to any control plane server on which

the STMC package is installed.

Control Plane Database

The control plane database (CPDB) is a persistent, central repository of data that guarantees consistent access and updates of data by using database locks and transactions. The CPDB uses an Oracle database featuring remote access and control. This database contains the following information pertaining to logical server farms, physical devices, and software associated with an I-Fabric:

- Properties and connections of devices, such as servers
- Logical server farm configurations
- Resources, such as VLANs and IP addresses
- State of network-specific applications
- State of requests
- Software images and their state
- WML
- FML
- MML
- DNS and DHCP configurations

Note – The request table in the CPDB keeps growing as the Control Center processes requests. By keeping the requests, you can obtain a history of activities in the control plane. You can also manually delete requests that are no longer needed. For more information, see "Managing the Request Queue" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

Image Server

The image server manages operating system images. The image server is installed on the Control Plan server, but can optionally be installed on any standalone server that supports network file server (NFS) file access.

Control Center Functionality

The Control Center software provides the infrastructure automation services required to manage and deploy logical server farms within an I-Fabric. At a high level, the Control Center manages the logical-to-physical mappings between a logical server farm and the physical resources assigned to it. The Control Center understands the physical topology of the resources deployed within the I-Fabric and provides the capability to deploy and configure these devices to unique topologies and configurations to match account-specific designs created in the Control Center.

The Control Center provides six key areas of infrastructure automation services:

- Provisioning and configuration services
- Flexing services
- Software image management services
- Monitoring services
- Physical infrastructure management services

Each of these five capabilities is built on a foundation of I-Fabric and security technologies that are leveraged by each service area.

Provisioning and Configuration

The ability to automatically provision and configure resources within the resource pool of an I-Fabric is a core capability of the Control Center. The following summary of the steps required to activate a logical server farm should help you understand the provisioning and configuration process.

1. **Allocate** – The control center dispatches requests to the provisioning server to provision and configure resources. When this request is received, the Control Center performs resource allocation. Resources are randomly allocated from the resource pool and tracked within the CPDB. IP subnets can be allocated from both public and private IP address spaces.
2. **Wiring** – Following the physical allocation of resources, the network fabrics for Ethernet connections are configured. This process includes configuring network resources such as IP subnets and VLANs. Images are copied to the servers at this time.
3. **Dispatch** – Following the virtual wiring of the logical server farm, DHCP and DNS services are initiated. The Control Center automates the configuration and management of these services. When these services are available, the devices within the logical server farm are powered up through addressable power devices.
4. **Activate** – On activation, the logical server farm is monitored to enable automated failover services.

   The Control Center manages and automates the ongoing evolution of logical server farms as well as their initial activation. As resources are added to or deleted from logical server farms, the Control Center continues to manage and automatically configure all wiring as well as DHCP and DNS services.

Flexing

Flexing is the ability to add or delete capacity on a logical server farm. N1 Provisioning Server software rapidly and automatically provisions and configures resources. You can apply flexing to address temporary surges in demand or to adjust capacity on a long-term basis. In either case, flexing enables you to employ infrastructure resources more efficiently. The N1 Provisioning Server software provides two types of flexing services:

- Adding and deleting individual servers within a logical server farm
- Adding and deleting server groups through a server group mechanism

You can add or delete servers from an active logical server farm at any time. Servers are added from the Control Center by dragging the server icon into the existing logical server farm design and attaching it to the appropriate subnet. All DNS and DHCP services are automatically configured. Adding an additional server does not require you to reinitiate the farm activation process. You also can delete servers by using the Control Center.

The server group is a unique logical structure supported within N1 Provisioning Server software. Server groups enable rapid flexing of servers by associating a predefined role or image for all servers within the group. All servers in a server group are considered identical and start off with the same software image. This software image is a *global image* that is replicated for every server within the server group.

When a server group is flexed up, the global image associated with the server group is automatically stored onto each server added to the group. Although you can make changes to individual servers within a server group, those changes will not be reflected in a flex operation unless you have updated the designated global image. When a server group is flexed down, the servers and their associated storage are returned to the resource pool. Server group flexing is done through the Control Center server configuration dialog box.

Software Image Management

The Control Center manages software images, and the configurations of servers and switches. The Control Center supports creation and management of two categories of images: global and account images.

- *Global images* typically contain baseline operating systems and monitoring software that have been configured to work with an I-Fabric. The purpose of deploying global images is to make available a set of baseline boot images that are accessible across different accounts and different farms in an I-Fabric. Based on the global images, you can then create new server images for subsequent modification and configuration. You must have administrator-level access to the N1 Provisioning Server to create global images. You can create global images only through the Control Center CLI. In addition to an operating system and monitoring software, you might choose to include other software components in an image.

  An I-Fabric supports images based on the Solaris 8, Solaris 9, and Red Hat™ Linux 2.1 operating environments.
- *Account images* are for a particular account and consist of account-specific customizations of one of the following items:
  - Global images
  - Blank disks
  - Application and data images

These images are the result of a snapshot of a disk in use within a logical server farm. The resulting images are available for use by farms within an account. Images that have account-specific software can be either global or account images. Their classification depends on their manner of creation. that is, whether they are created from modifications of an existing global image or from the snapshot of a disk in use within a logical server farm. Thus, you can create identical images by both methodologies, and the images are considered distinct solely on the basis of their methods of creation.

Note – The N1 Provisioning Server software package comes with baseline Solaris 8 and Solaris 9 operating system images that you can copy using the `snapshot` tool and customize.

Using the `snapshot` tool available from the Control Center, you can capture software images to be stored in an image library and use them to subsequently configure similar devices. You can use these images for global or account images. A disk snapshot is the logical equivalent of making a master copy of a local disk image. The original image is stored in an image library and a reference to the image is entered in the CPDB. Depending on the I-Fabric configuration, images reside on the local disk or on a remote NFS file server. Snapshot images are named and catalogued in the Control Center image library. The image library is listed in the Control Center server configuration dialog box. You can choose from prebuilt images to be associated with a server or server group.

You can take a snapshot of any software image associated with any server (individual servers as well as a specific server within a server group). The snapshot function automatically shuts the server down to ensure that the resulting image is a stable, production-ready replication of the original image. After the snapshot is completed, the Control Center reboots the server automatically.

The snapshot function enables functionality such as server flexing and server failover. If a server fails, the system can automatically replace the failed server with a substitute by using the last snapshot of the failed server to create the image for the new server.

Monitoring

The Control Center actively monitors the state and health of devices in an I-Fabric. Monitoring provides visibility of an I-Fabric and supports failover and recovery or to restart failed processes.

The Control Center enables the following farm monitoring capabilities within an I-Fabric:

- Availability of resource pool devices (server farms) to enable automatic failover and availability of these devices for display in the Control Center monitoring screen.

- Basic performance monitors (disk, CPU, memory) for servers. You can display the monitoring information in the Control Center.
- Changes in farm or device status, state, and configuration that is recorded in event logs and optionally can be made available externally using Simple Network Management Protocol (SNMP) traps.
  - Events in monitoring farm state changes include activating, deactivating, and placing a farm in standby mode.
  - Events in farm configuration changes include adding, removing, and reconfiguring farm servers.
  - Events in device state changes and failures include server UP and server DOWN messages.
- Messages for events comprise three categories:
  - Informational messages, such as device availability or failure
  - Farm messages related to devices of a specific farm
  - Billing messages

Monitoring messages are forwarded to the service processor. The service processor then sends the messages to a central message repository in the CPDB. You can view monitoring data using the Control Center monitoring screen. You can also configure monitoring events for farm server utilization, such as disk and CPU, by using the Control Center monitoring screen.

Optionally, you can configure the CPDB to forward messages to an external network management system (NMS). An SNMP connection and a management information base (MIB) extension are required for forwarding messages to an external NMS.

Additional tools for monitoring system health include operating system and Control Center commands. For details regarding system health monitoring, see Chapter 4, "Monitoring and Messaging" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

Physical Infrastructure Management

As a part of the N1 Provisioning Server initialization process, the Control Center performs resource and wiring validation. This validation enables the Control Center to have a complete physical topology map of all resources within an I-Fabric. The wiring validation provides an automated way of confirming the physical wiring map of equipment in a given data center. The Control Center's ability to successfully manage the virtual wiring of a logical server farm relies on the integrity of the physical wiring of the resources within an I-Fabric. Automating this physical wiring validation removes a common source of errors in an I-Fabric, namely the potential for human error caused by incorrectly cabling the physical infrastructure.

The Control Center uses this wiring data to make resource allocation decisions. Physical infrastructure data is stored in a database that you can access using the Control Center CLI.

N1 Provisioning Server Security

By default, an I-Fabric is configured to apply a high level of security at all levels. You can configure I-Fabric security according to your company's needs by using any suitable combination of security levels as described in the following sections.

An I-Fabric provides several levels of security throughout the infrastructure to ensure that each logical server farm is secure from intrusion or attack from within or outside the I-Fabric. Security solutions have been implemented at the following levels within the I-Fabric:

- Password encryption
- Control plane
- Control center
- Resource pool
- Ethernet
- VLAN
- Physical network
- Network virtualization
- Logical server farms
- External Ethernet port connections

Password Encryption

Password encryption is provided at all levels within the I-Fabric for security purposes. You can configure the system to use clear-text passwords. However, clear-text passwords are problematic.

Control Plane Security

The server responsible for running the N1 Provisioning Server software resides within the control plane. The security of this server depends significantly on the deployment architecture of the servers and network responsible for running the N1 Provisioning Server application. The I-Fabric design provides a secure methodology for deploying the N1 Provisioning Server software.

Depending on the management requirements of an I-Fabric, you can deploy the Control Center without connectivity to external networks or to the Internet. Control Center security is implemented at several levels. For further information, see "Provisioning Server Security" on page 33. The Control Center communicates with the Control Center through a privileged VLAN that is not available from outside of the I-Fabric.

Control Center security prevents tampering from within the I-Fabric. Security for Control Center software is implemented by using dedicated VLANs. For further information, see “Ethernet Security” on page 34.

Provisioning Server Security

The following list describes the three types of connections to the Control Center, each of which has security measures in place:

- Web access secured by Secure Socket Layer (SSL)

  The Control Center uses SSL security (high-strength, 128-bit encryption) with login and password validation. The Control Center can be deployed with or without connectivity to external networks or to the Internet.
- A private, separately secured connection to the monitoring tool.

  The Control Center performs database, monitoring, and management operations through a monitoring agent.
- A private, separately secured connection to each Control Center managed by the Control Center.

  The Control Center communicates with the Control Center using FML, an XML-based dialect, through a dedicated, port-based VLAN that is not available from outside of an I-Fabric.

Accessing the Control Center

Secure access to the Control Center is based on login accounts. These login accounts provide security from accounts outside a company as well as inside a company. An account may have one of the following available login roles assigned to it, depending on the users job functions:

- *User* is a technical user who can create farms and make changes to the state of any farm in the account.
- *Account Manager* is a user who has the same access privileges as User and the added ability to add and remove Users from their accounts.
- *Administrator* is an administrative user who has full access to the entire application, including the configuration of the application and operational access to every account and farm within the Control Center. Administrators do not belong to any account.

For more details about accounts, see the *Control Center Management Guide*.

Login Name and Password Management

The Control Center processes login name and password changes. You are responsible for issuing the initial name and password to the users of an account. The Control Center network system automatically verifies passwords.

Login Lockout

By default, users are locked out of the Control Center if their login attempts fail a configurable number of times within a configurable number of minutes. The lock is automatically released after another configurable number of minutes. However, you can use the Control Center Login Status screen to unlock users before the automatic unlock process takes place. This screen also enables you to force-lock existing users if a security issue involving a user becomes apparent. You can also unlock or force-lock another administrator by using the same method. See the *Control Center Management Guide*.

Reaccessing the Control Center After a Failure

When a software or hardware failure occurs during a session on the Control Center, users must log in again when reaccessing the Control Center.

Encryption and Filtering

Transactions performed using the Control Center are encrypted securely using the hyper-text transfer protocol secure sockets (HTTPS). External access to the Control Center is filtered at all points using IP filtering to ensure secure web access.

Resource Pool Security

The ability to repurpose servers over time as they come in and out of the resource pool presents security challenges. Server integrity is protected by power cycling and scrubbing the storage and memory of all servers before they are added to a resource pool.

Ethernet Security

Within the Ethernet portion of the switched fabric, logical server farms are implemented using port-based virtual local area networks (VLANs). From a security perspective, port-based addressing provides a superior implementation when compared to VLAN implementations that are defined by Media Access Control (MAC)

or IP addresses. This enhanced security is due to devices being connected physically through the switch rather than through logical addresses. The implementation of a network virtualization layer eliminates the possibility of VLAN hopping or IP spoofing, or the possibility of controlling VLAN membership from outside the Control Center.

To prevent IP spoofing attempts, an incoming IP packet on a VLAN must have the same VLAN tag and MAC address as the logical interface on which it is arriving. The Control Center sets VLAN tags for the appropriate ports and networks.

To ensure that the Control Center is protected from unauthorized access from within the I-Fabric, the control plane server on which the Control Center software runs resides within its own dedicated port-based VLAN. This architecture physically eliminates the possibility of unauthorized access to the Control Center from within the I-Fabric. Logical server farm users cannot manipulate their own or any other logical server farm's VLAN configuration.

Server blades within an I-Fabric are dedicated to only one unique logical server farm at any time. While servers may be added or subtracted from a particular logical server farm over its life cycle, no single physical server blade will ever be used by more than one logical server farm simultaneously. Thus, servers are protected from intrusion by the VLAN and the Control Center security measures previously described.

Farms are implemented in an I-Fabric using VLANs, which are based on physical switch ports and configured through the Control Center. The switch configuration is protected by the VLAN, not an administrative password. VLAN configurations are password protected on the applicable switch.

Access to services on the Control Center from the farms is restricted by IP filtering. IP routing through a control plane server is not possible. Access to the Farm Manager and the Segment Manager from a farm is not possible.

Note – Only the Control Center is authorized to make modifications to virtual wiring and virtual farm security perimeters.

Physical Network Security

Implement security policies that protect the physical network from internal unauthorized access based on your site's setup and facilities.

Network Virtualization and Security

By using port-based VLAN technology, network virtualization provides a network security perimeter for all the computing and network devices associated with a given farm. When a device is logically assigned to a farm, the device is transitioned to the appropriate logical network associated with that logical element of the farm.

Network virtualization uses physical port-based VLAN technology built into current generation Layer-2 switches. The VLAN enables you to create a secure virtual network between a set of network nodes that appears as a transparent Layer-2 interconnect to these sets of network nodes. These virtual Layer-2 interconnects are then used as virtual wires to connect the devices on the switched fabric into the desired Layer-2 network topology.

Ethernet switching equipment must be capable of supporting VLAN tagging for use in network virtualization to protect against VLAN hopping or other kinds of VLAN penetration attempts. In addition, standard password encryption protects the management of these switches from unauthorized modifications from any server or device in the resource pool. Any switching equipment must meet the standards of 802.1q.

The management of these switches is protected from unauthorized modifications from any server or device in an I-Fabric. Only the Control Center administrator is authorized to make modifications to the virtual wiring and virtual logical server farm security perimeters.

Logical Server Farm Security

Logical server farms on an I-Fabric are implemented using port-based VLANs. These VLANs are configured through the Control Center. The Control Center restricts access from the farms. Farm users cannot change their own or any other farm's VLAN configuration.

Server blades within an I-Fabric are dedicated to one unique farm at a time. While you can add or subtract server blades from a particular farm over its lifecycle, no single physical server blade is ever used by more than one farm simultaneously.

When you deactivate a server blade, the N1 Provisioning Server software cycle its power sufficiently to clear volatile memory. You should also reset server blades to their factory values before returning them to the idle pool so that any account-specific, nonvolatile memory components are erased. Follow the best practices to configure and check your server blades for security. If you want to perform a recommended audit, an I-Fabric supports industry-standard third-party auditing tools.

Server Accounts and Passwords

Set up administrator server accounts and passwords by following conventions and best practices. See also security web sites such as http://www.cert.org, http://www.sun.com, and http://www.cisco.com for recommendations on keeping network servers protected from unauthorized access.

External Ethernet Port Connection Security

Ethernet port connections are optional with an I-Fabric. The connections can be either virtual private network (VPN) or leased-line connections. You can configure your I-Fabric for Ethernet port connections based on your site's needs and by using industry-standard security mechanisms.

Implementation and Installation Roadmap

This section provides a summary of the N1 Blade Provisioning Server implementation and installation process.

This guide does not discuss the following prerequisite knowledge and tasks:

- Physical design
- Cabling design
- Rack design
- Power requirements

You should have related designs and plans in place before implementing an I-Fabric.

The following diagram describes the major steps required to implement and install N1 Provisioning Server, Blades Edition version 3.1.

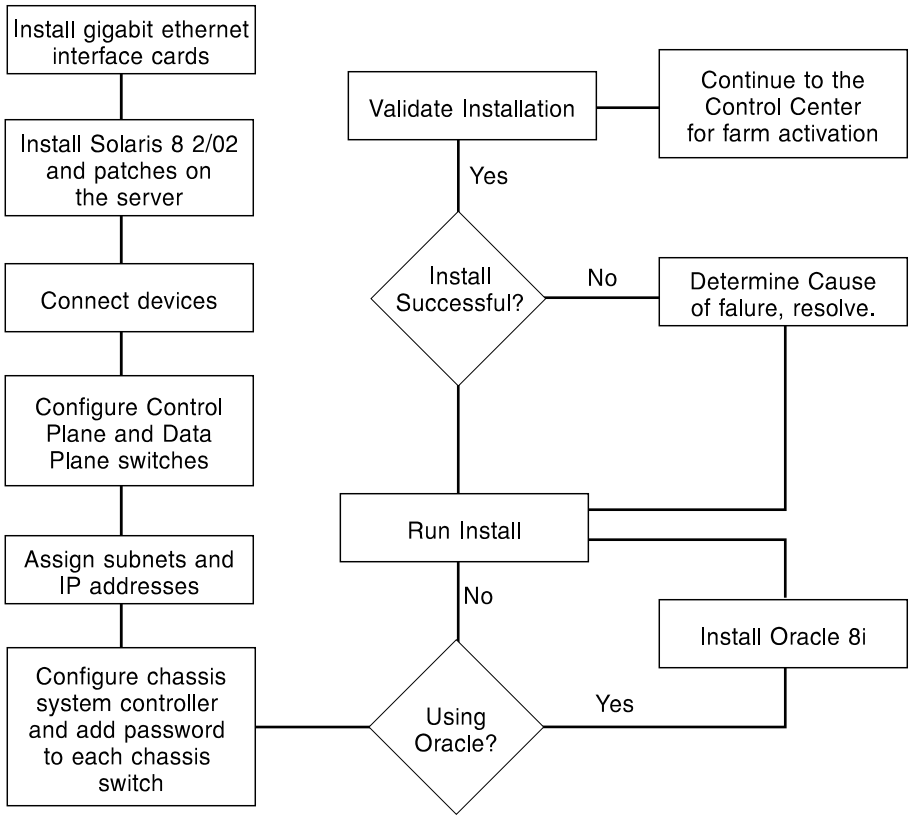

FIGURE 1–7 N1 Provisioning Server Installation Flow Diagram

The following checklist describes the major steps required to implement and install N1 Provisioning Server, Blades Edition:

- ❒ Determine the hardware requirements for your N1 Provisioning Server environment. See Chapter 2.
- ❒ Choose a system configuration based on your hardware selections. See "N1 Provisioning Server Supported Configurations" on page 47.
- ❒ Purchase the software and hardware for the selected configuration.
- ❒ Install the gigabit Ethernet network interface card in the control plane server. "Installing Gigabit Ethernet Network Interface Cards" on page 50See "Installing Gigabit Ethernet Network Interface Cards" on page 50
- ❒ Install the Solaris 8™, release 2/02, operating system on the control plane server. See "Installing the Solaris Operating System, version 8 2/02" on page 52.
- ❒ Disable remote logins from root accounts. See "Disabling Remote Logins From Root Accounts" on page 53.
- ❒ Install required patches. See "Installing Required Patches" on page 54.

- ❒ Install and connect the chassis to the control plane server and external switches according to your selected configuration. See "Connecting the Chassis to the Control Plane Server and Switches" on page 56
- ❒ If you plan to use the Oracle as your control plane database (CPDB), install Oracle 8i database on the control plane server. See "Installing the N1 Provisioning Server Database" on page 70.
- ❒ Decide on and implement an IP address scheme for the configuration. See "Assigning IP Addresses in the Control Plane" on page 68
- ❒ Install the N1 Provisioning Server software.
  - – If you are installing the N1 Provisioning software for the first time, see Chapter 4.
  - – If you are upgrading from N1 Provisioning Server version 3.0 to version 3.1, see Chapter 5.

    If you also plan to use the Postgres as your control plane database, migrate your data from the Oracle CPDB to Postgres. See "Migrating From Oracle to PostgreSQL" on page 112
- ❒ Validate the N1 Provisioning Server installation. See "Validating the N1 Provisioning Server Installation" on page 103.
- ❒ Apply role-based access control. See "Applying Role-Based Access Control" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

CHAPTER 2

Hardware and Software Requirements

The information in this chapter will help you determine what operating system, hardware, and storage resources must be allocated or acquired to implement a specific N1 Provisioning Server, Blades Edition

This chapter discusses the following topics:

B1600 Blade System Chassis

This section provides the Blade System Chassis hardware and firmware requirements.

Blade System Chassis Hardware Requirements

Blade System chassis hardware requirements are listed in the following table.

TABLE 2–1 B1600 Blade System Chassis Hardware Requirements

Chassis Component	Description
Switch and System Controller (SSC)	Each chassis must have at least one SSC. **Caution –** An SSC must be installed in SSC0.
Sun Fire™ Server Blades	1 to 16 single-slot server blades in combination: ■ B100s SPARC®-based blades for Solaris ■ B100x single processor and B200x dual processor blades - x86–based blades for Solaris x86 and Linux **Note –** The B200x blade occupies two chassis slots, and requires a two-processor operating system image. The B200x is treated as an unmanaged device. ■ B10n content load balancing blade ■ B10p SSL Proxy blade **Note –** The B10p blade is treated as an unmanaged device.

Blade System Chassis Firmware Requirements

Blade System chassis firmware version requirements are listed in the following table.

Note – This version of the N1 Provisioning Server, Blades Edition supports chassis firmware version 1.2 and version 4D.2.

TABLE 2–2 Blade System Chassis Firmware Requirements

Device	Firmware
Switch	■ Loader version 0.0.6.7 ■ Boot ROM version 1.0.0.9 ■ Operation Code version 1.0.0.16
System controller	■ SC version 1.2.7 ■ SC Boot version 1.2.7
B10n Load Balancing Blade	■ Blade Support Chip version 5.1.4 ■ Firmware version 1.2.1
B100s SPARC Server Blade	■ Blade Support Chip version 5.0.2 ■ Open Boot Prom version 4.7.5
B100x Server Blade	■ Blade Support Chip version 5.1.3 ■ BIOS version 4.0 (R6.0)

TABLE 2–2 Blade System Chassis Firmware Requirements *(Continued)*

Device	Firmware
B200x Server Blade	■ Blade Support Chip version 5.1.8 ■ BIOS version P1.1.27

Before installing N1 Provisioning Server software, make certain that the firmware versions for the blade system chassis and each server blade meet the firmware version requirements listed by the previous table. Procedures for determining firmware versions and upgrading firmware are provided in the administration guide for each server blade.

Control Plane System Requirements

Control plane system hardware and operating environment requirements are listed in the following table.

Note – The image server software can optionally be installed on a separate machine.

TABLE 2–3 System Requirements

Item	Hardware	Operating System	Disk Space	RAM	Swap
Control plane server	Sun Fire V120 server or a Sun Fire V280R server, 650 MHz or better with a DVD-ROM drive	Solaris 8, release 2/02	20 Gbyte disk minimum	4 Gbytes	5 Gbytes
Image server (optional)	Sun Fire V120 server or a Sun Fire V280R server, 650 MHz or better with a DVD-ROM drive	Solaris 8, release 2/02	20 Gbyte disk minimum	4 Gbytes	2 Gbytes

TABLE 2–3 System Requirements *(Continued)*

Item	Hardware	Operating System	Disk Space	RAM	Swap
Control Center Management PC	x86 , 800 MHz minimum 10/100 Megabit network interface card	Microsoft Windows 2000 or Windows XP and Microsoft Internet Explorer 6.0 with 128–bit encryption	Not applicable	256 Mbytes minimum, 512 Mbytes recommended	Not applicable

Network Interface Card (NIC) Requirements

A VLAN-capable gigabit NIC card and appropriate drivers must be installed in the control plane server. If you have chosen to install the image server software on a separate machine, you should install a gigabit NIC card in the image server. The following table lists the supported VLAN-capable gigabit NIC cards.

TABLE 2–4 Network Interface Card (NIC) Requirements

NIC	Driver Version	Interface
Sun GigaSwift Copper	Version 1.21	ce0
SysKonnect Copper	Version 6.08	skge0

Switch Requirements

Control plane switch requirements are listed in the following table.

TABLE 2–5 Switch Requirements

Switch	Provisioning Server Plane	Notes
Cisco Catalyst 2950-24	Control plane Ethernet switch	The control plane Switch is optional in a setup of a combined Provisioning and image server with a single chassis containing a single Switch and System Controller (SSC) unit. Any other configuration requires the addition of a control switch.
Cisco Catalyst 3550-12T	Control plane Ethernet switch	Minimum suggested requirement for three or more chassis.
Cisco Catalyst 3750-12 or 3750–24	Control plane or Data plane Ethernet switch	Minimum suggested requirement for three or more chassis.
Cisco Catalyst 4503 Switch Chassis	Control plane or data plane Ethernet switch	Minimum suggested requirement for six or more chassis. A 48-port switch module needs to be added to the Cisco switch.
Cisco Catalyst 6500 Switch Chassis	Control plane or data plane Ethernet switch	Minimum suggested requirement for a six or more B1600 Blade System chassis installation. A 48-port switch module needs to be added to the Cisco switch.

JRE Version Requirements

The N1 Provisioning Server and Application Server include the Java Runtime Edition, version 1.4.1_01, which is automatically installed as part of the N1 Provisioning Server, Blades Edition installation process.

Third-party Software Requirements

The following table describes third-party software that must be purchased in order to complete an I-Fabric implementation. The software is not included on the N1 Provisioning Server installation DVD-ROM.

Note – PostgreSQL, version 7.4 is provided on the installation DVD-ROM. If you choose to use the Oracle database instead of the PostgreSQL database, you must purchase and install Oracle before you install the N1 Provisioning Server software.

TABLE 2–6 Third-party Software Requirements

Software	I-Fabric Component	License Provider	Install Location
Microsoft Windows 2000 or Windows XP	Control Center Management PC	Microsoft	Control Center Management PC
Internet Explorer 6.0 with 128–bit security encryption	Control Center	Microsoft	Control Center Management PC
Adobe® Acrobat Reader version 5.0	Control Center PC	Adobe	Control Center Management PC
Oracle® Client 8i, version 8.1.7	Control plane database (CPDB)	Oracle	Control plane server

CHAPTER 3

N1 Provisioning Server System and Network Preparation

This chapter provides the guidelines and procedures for connecting and configuring your N1 Provisioning Server components. The tasks provided in this chapter must be performed before you can install the N1 Provisioning Server software.

This chapter discusses the following topics:

N1 Provisioning Server Configuration and Connections Overview

This section provides a list of the supported N1 Provisioning Server configurations, the requirements for each type of connection in an I-Fabric, a summary of the chassis SSC connections, and the naming conventions used for connections.

N1 Provisioning Server Supported Configurations

The following N1 Provisioning Server configurations are supported:

- One Sun Fire B1600 Blade System Chassis with a single Switch and System Controller (SSC). An external switch is not required, but is recommended.
- One blade system chassis with two SSCs. An external control plane switch and an external data plane switch is required.
- Two or more chassis. An external control plane switch and an external data plane switch is required.

Required Connection Information

The following information is required for each connection.

TABLE 3–1 Connection Information

Information	Description
Starting Device ID	The device ID of the starting device
Starting Port	Identifies the port in the starting device
Ending Device ID	The device ID of the ending device
Ending Device Port	Identifies the port of the ending device

Chassis Switch and System Controller (SSC) Connections

The following diagram illustrates the physical connections of a single SSC.

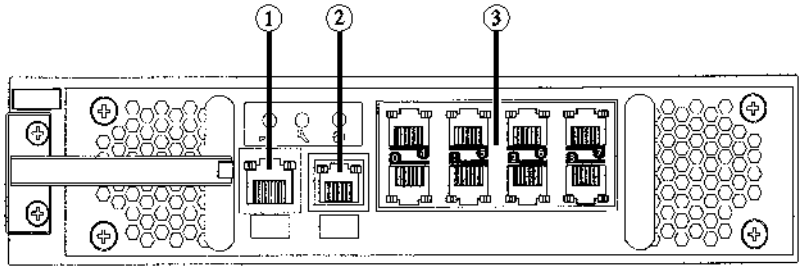

FIGURE 3–1 B1600 Switch and System Controller (SSC) Connections: Physical View

The SSC connections are as follows:

- 1 – RS232 serial console port
- 2 – 10/100 Base-T network management port, referred to as the NETMGT port

- 3 – 10/100/1000 Base-T data network ports, referred to as NETP0 to NETP3 from left to right on the bottom row, and as NETP4 through NETP7 from left to right on the top row

The following diagram shows the representative connections of a chassis with two SSCs. The diagram shows only those connections used by the N1 Provisioning Server software, and is used in the following sections to illustrate the connections required for the three supported configurations.

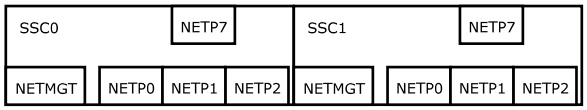

FIGURE 3–2 B1600 Switch and System Controller (SSC) Connections: Logical View

Connection Port Naming

The following table shows the port naming used in the following sections for the servers, switches, and chassis SSC devices.

TABLE 3–2 Device Port Naming

Logical Port Name	Role
`eri0`	Control plane server connection to the control plane switch for the Service Processor (SP), control plane database (CPDB), and Control Center (CC) provisioning command transfer. **Note –** In a single chassis-single SSC installation with no external switch, `eri0` connects to the `NETMGT` port of the SSC.
`eri1`	Control plane server connection to the local intranet. The Control Center Management PC is usually connected to the local intranet.
`ce0/skge0`	Control plane server gigabit connection to the data plane switch for operating system image flash and JumpStart installations for server blades
`NETMGT`	Chassis switch and system controller connection to the control plane switch for provisioning command transfer.
`NETP0`	Chassis switch and system controller gigabit connection to the data plane switch for operating system image flash and JumpStart installations for server blades
`NETP1`	Chassis switch and system controller gigabit connection to a separate image server if an external data plane switch is not used.

TABLE 3–2 Device Port Naming *(Continued)*

Logical Port Name	Role
`NETP1` through `NETP6`	Unused chassis switch and system controller connections.
`NETP7`	Uplink when the installation does not have a data plane switch. See Figure 3–3.

- The Wiring Mark-up Language (WML) file contains the logical port name. The table shows only the physical name for each type of connection. Gigabit Ethernet connections are recorded in WML as `eth0`, `eth1`, or `ethN`.
- The gigabit Ethernet card is designated `ce0/skge0`, and can be either the Sun GigaSwift card (`ce`) or the SysKonnect card (`skge0`). If you select a card made by another vendor this designation might change. Control plane servers can also have a Gigabit Ethernet card.

Connecting a Separate Image Server

The image server can be any machine that supports a network file server (NFS) access. The image server must have at least one 10/100 Base T Ethernet network interface card (NIC), and one 10/100/1000 VLAN-capable gigabit NIC. The Provisioning Server control plane software is set to use the default image server user account `root` with the password `root` that has read and write access for NFS. The image server username and password are configurable during installation. You must set up the image server with `telnetd` allowing access as user `root` and password `root`.

The N1 image server 10/100 Base T port must be connected to the control plane switch, and the 10/100/100 NIC port must be connected to the data plane switch.

Installing Gigabit Ethernet Network Interface Cards

You can install either the Sun GigaSwift Ethernet network interface card (NIC) or the SysKonnect Gigabit NIC in the control plane server to support the data trunks.

Note – If you are installing the image server software on a separate machine, you should install either the Sun GigaSwift NIC or the SysKonnect Gigabit NIC on the image server machine as well.

Sun GigaSwift Gigabit Ethernet Network Interface Card

Install the GigaSwift VLAN-capable gigabit Ethernet network interface card on the server.

The driver configuration file for the GigaSwift gigabit Ethernet card is configured automatically by the N1 Provisioning Server installation program at the beginning of the installation process. The GigaSwift driver is enabled to support VLANs and configured for VLANs from vlan-id 0 to vlan-id 999. You do not need to configure the driver for network connectivity or add VLANs to the configuration file.

Note – The Sun GigaSwift Ethernet card is designated `ce0`. If you select a card made by another vendor this designation might change.

At the beginning of the N1 Provisioning Server installation, you are prompted reboot the server in order to enable the GigaSwift card configuration.

```
The GigaSwift configuration file has been updated to support vlans.
A reboot is required to enable the new configuration to take effect.
```

As root, type the following command at the command-line prompt:

```
shutdown -i6 -g0 -y
```

When the server finishes rebooting, install the system and GigaSwift patches as directed in “Installing Required Patches” on page 54.

SysKonnect Gigabit Ethernet Network Interface Card

Install the SysKonnect VLAN-capable gigabit Ethernet network interface card (SK98xx) on the control plane server. You must install the Solaris 64-bit driver version 6.02. The drivers for SysKonnect cards are available at http://www.syskonnect.com/syskonnect/support/driver/d0102_driver.html.

Note – The SysKonnect Gigabit Ethernet card is designated `skge0`. If you select a card made by another vendor this designation might change.

Type **`N`** when prompted whether you want to configure the interfaces. After you have installed the card, reboot the server. The N1 Provisioning software installation automatically creates the interfaces.

The driver configuration file for the SysKonnect gigabit Ethernet card is configured automatically by the N1 Provisioning Server install program at the beginning of the installation process. The SysKonnect driver is enabled to support VLANS and configured for VLANs from vlan-id 0 to vlan-id 999. You do not need to configure the driver for network connectivity or add VLANS to the configuration file.

At the beginning of the N1 Provisioning Server installation, you are prompted reboot the server in order to enable the SysKonnect card configuration.

```
The SysKonnect configuration file has been updated to support vlans.
A reboot is required to enable the new configuration to take effect.
```

As root, type the following command at the command-line prompt:

```
shutdown -i6 -g0 -y
```

Installing the Solaris Operating System, version 8 2/02

The Solaris Operating System, version 8 2/02, must be installed on the control plane server before you can install N1 Provisioning Server software. If you are installing the image server software on a separate machine, you must also install Solaris version 8 2/02 on the image server machine before installing the N1 Provisioning Server software.

To install the Solaris software, follow the installation instructions provided with that software. To satisfy the N1 Provisioning Server requirements for the Sun Fire B1600 Blade System, you must make the following selections during the installation of the Solaris Operating System:

- Install the 64-bit version.
- Select the `en_US` locale.
- Set up the file partition to allocate a minimum of 8 GBytes in the root directory.
- When you are prompted to setup DNS, select NO.
- When you are prompted to setup DHCP, select NO.
- When you are prompted to select the type of configuration, select End User.
- If you are using a non-interactive JumpStart™ installation, include the bash package `SUNWbash` and `SUNWgzip` in the profile. If you are using an interactive JumpStart or CD install, customize your configuration selection to include these packages.
- Make sure that you have installed the following packages, which are part of the end-user install:

- SUNWbzip
- SUNWbzipx
- SUNWzip
- SUNWtcsh
- SUNWscpux
- SUNWbtool
- SUNWtoo
- SUNWsprot

Disabling Remote Logins From Root Accounts

Remote root login must be disabled on all N1 Provisioning servers as described by the following procedure. When remote root login is disabled, root accounts can log in only on the system console.

Note – If the N1 Image server is installed on a separate machine, the following procedure must also be done on the image server machine.

▼ To Disable Remote Root Account Logins

Steps

1. **Log in as root (su - root) on the control plane server.**
2. **Edit the file `/etc/default/login`.**
3. **Locate the line that contains the text string `CONSOLE=/dev/console`.**
   If the line is commented out, remove the comment symbol #.
4. **Make certain the `/etc/default/login` file contains only one `CONSOLE=/dev/console` line.**
5. **Save and close the file.**

See Also For more information, see the `login(1)` man page.

Installing Required Patches

This section provides the procedures for installing the Solaris Operating System, version 8 2/02 patches, and the GigaSwift copper gigabit Ethernet interface card patches.

The Solaris Operating System, version 8 2/02, must be installed on the control plane server before you can install N1 Provisioning Server software. If you are installing the image server software on a separate machine, you must also install Solaris version 8 2/02 on the image server machine before installing the N1 Provisioning Server software.

Solaris Operating System, version 8 2/02 Patches

For Solaris operating system, version 8 2/02, you must install the latest recommended patch cluster. You can find the patch cluster at: http://sunsolve.sun.com.

▼ To Install the Solaris Version 8 2/02 Patch Cluster

Steps

1. **Log onto the control plane server as root.**
2. **Open a web browser and go to the SunSolve Web site http://sunsolve.sun.com (`http://sunsolve.sun.com`).**
3. **Download the latest recommended Solaris Version 8 2/02 patch cluster.**
   a. **Click Patch Portal.**
      The Patch Portal screen appears.
   b. **Click Recommended Patch Cluster in the Downloads section.**
      The Patch Finder screen appears.
   c. **Choose 8 from the list of available patch clusters.**
      Scroll down the page and select either HTTP or FTP to download the patch, then click Go. The Save dialog box appears.
   d. **Select a directory into which to download the patch cluster zip file.**
      Make note of the directory to which you downloaded the patch cluster zip file.
4. **Change to the directory where you downloaded the patch cluster zip file and unzip the file.**
   For example:

```
# cd /var/tmp/#unzip /var/tmp/8_Recommended.zip
```

5. **Install the patch cluster by using the install script that is uncompressed from the zip file.**

   For example:

   ```
   #/var/tmp/8_Recommended/install_cluster
   ```

Note – This step might take up to two hours to complete.

GigaSwift Gigabit Ethernet Patch

You can now use the GigaSwift copper gigabit Ethernet interface card, Part No. X1150A, within the N1 Provisioning Server environment. You can use this network interface card (NIC) as a VLAN-capable gigabit Ethernet adapter on the control plane server and, if you have a separate image server, on the image server for farm management.

During the initial installation of the N1 Provisioning Server software, the interface card is detected and configured by the N1 Provisioning Server installer utility. However, prior to the installation, you need to download and install the patch ID 112119-04 for Solaris 8.

▼ To Download and Install the GigaSwift Ethernet Patch

Steps

1. **Log onto the control plane server as root (su - root).**
2. **Open a web browser and go to the SunSolve Web site http://sunsolve.sun.com (`http://sunsolve.sun.com`).**
3. **Download patch 112119-04.**
   a. **Click Patch Portal.**
      The Patch Portal screen appears.
   b. **Type the patch ID `112119-04` in the Patch Finder box, and then click Find Patch.**
      The download patch screen appears.
      The patch is available for downloading in ZIP format using either HTTP or FTP.
   c. **Select either HTTP or FTP to download the patch and then click Go. The Save Dialog appears.**
   d. **Select a directory into which to download the patch zip file.**

Make note of the directory to which you downloaded the patch zip file.

4. **Change to the directory where you downloaded the patch zip file and unzip the file.**

   For example:

   ```
   # cd /var/tmp/
   #unzip /var/tmp/112119-04.zip
   ```

5. **Install the patch.**

   For each patch you downloaded, type **patchadd** *patch-id* where *patch-id* is the ID of the downloaded patch.

   For example:

   ```
   #patchadd 112119-04
   ```

Connecting the Chassis to the Control Plane Server and Switches

This section provides the procedures for connecting the control plane server, blade system chassis, Control Center Management PC, and switches for each of the supported configurations.

Connecting a Single Chassis with a Single SSC

This section illustrates the topology of a single-chassis single-SSC I-Fabric, and provides the procedure for connecting the I-Fabric components.

Caution – The SSC must be installed in chassis slot `SSC0` for a single chassis, single SSC configuration. The Provisioning Server software cannot configure and provision the server blades if the SSC is installed in `SSC1`.

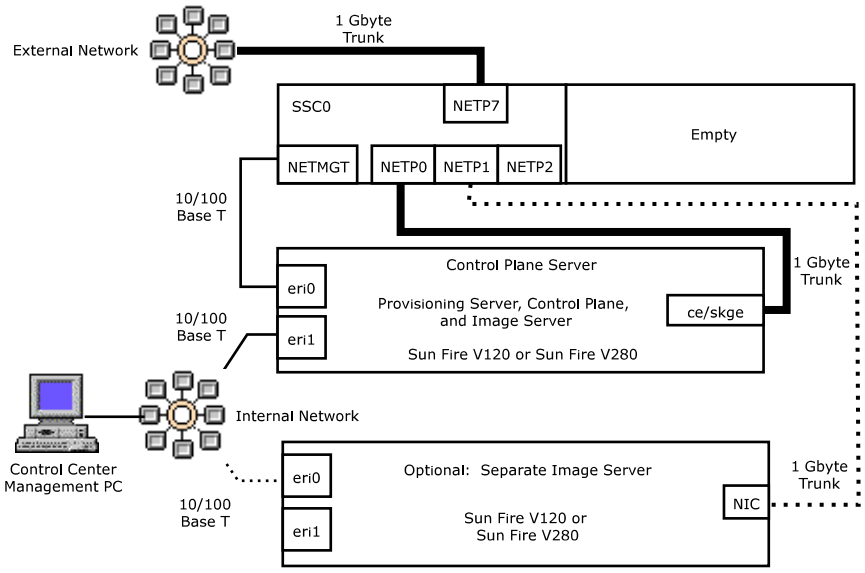

FIGURE 3–3 Single Chassis With a Single SSC and no External Switch

▼ To Connect A Single Chassis With a Single SSC to the Control Plane Server

Steps

1. **Connect the `NETMGT` port of `SSC0` to the `eri0` port of the control plane server with 100 base T copper Ethernet cable.**
2. **Connect the `NETP0` port of `SSC0` to the `ce0/skge0` port of the control plane server with 1000 base T copper Ethernet cable.**
3. **Connect the `NETP7` port of `SSC0` to the external network with 1000 base T copper Ethernet cable. Farms are accessed through the `NETP7` connection.**
4. **Connect the `eri1` port of the control plane server to your internal network switch with 100 base T copper Ethernet cable.**
5. **Connect the Control Center Management PC NIC port to the internal network switch.**

   The type of cable depends on the capacity of the PC NIC and the network switch ports.
6. **If you have chosen to install the image server as a separate machine, connect the image server ports as follows.**

a. **Connect the `NETP1` port of `SSC0` to the NIC port of the image server machine**

   Use a cable appropriate for the type of interface card installed in the image server: 100 base T copper for a 10/100 base T NIC, and 1000 base T copper for a gigabyte-capable NIC.

Note – If you have chosen to install the N1 image server on a separate machine, install a gigabyte-capable card such as the Sun GigaSwift NIC or the SysKonnect NIC in the image server machine.

---

b. **If you have a separate image server machine, connect the `eri0` port of the image server to your internal network switch with 100 base T copper Ethernet cable.**

Connecting a Single Chassis with Two SSCs

This section illustrates the topology of a single-chassis dual-SSC I-Fabric, and provides the procedure for connecting the I-Fabric components.

Note – For security, install a separate control plane switch and data plane switch. Use of a single switch for the control plane and data plane is not supported for an installation where any chassis contains two SSCs.

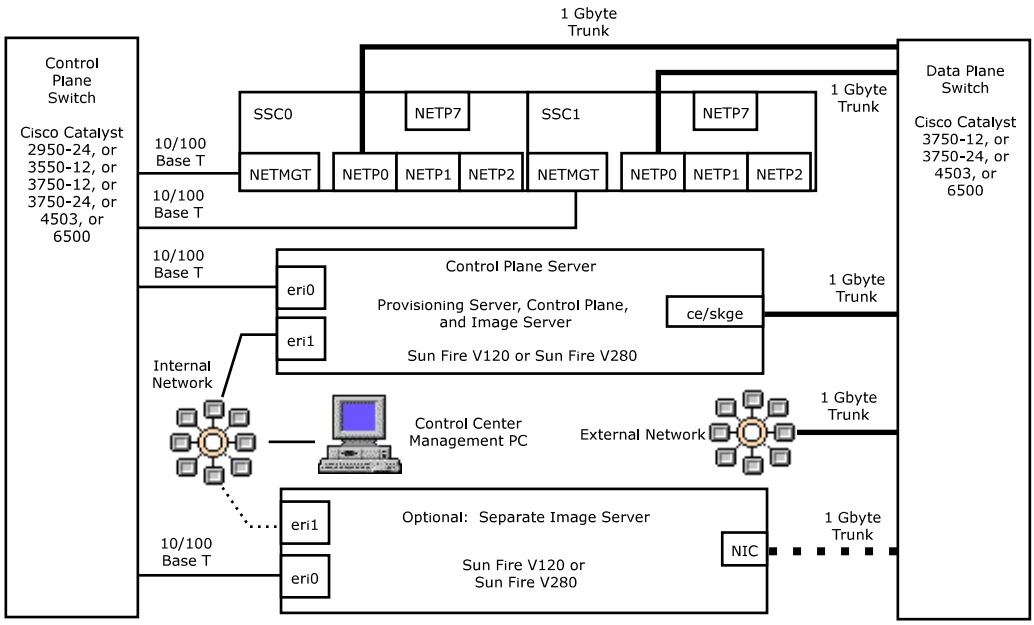

FIGURE 3–4 Single Chassis with Two SSCs and Separate Control Plane and Data Plane Switches

▼ To Connect A Single Chassis with Dual SSCs to the Control Plane Server and Switches

Steps

1. **Connect the `NETMGT` ports of `SSC0` and `SSC1` to the control plane switch with 100 base T copper Ethernet cable.**
2. **Connect the `NETP0` ports of `SSC0` and `SSC1` to a data plane switch gigabit port with 1000 base T copper Ethernet cable.**
3. **Connect the `ce0/skge0` port of the control plane server to data plane switch gigabit port with 1000 base T copper Ethernet cable.**
4. **Connect the `eri0` port of the control plane server to a 100 base T port on the control plane switch with 100 base T copper Ethernet cable.**
5. **Connect the `eri1` port of the control plane server to the internal network switch with 100 base T copper Ethernet cable.**
6. **Connect the Control Center Management PC NIC port to the internal network switch.**

The type of cable depends on the capacity of the PC NIC and the network switch ports.

7. **Connect the data plane switch to the external network with 1000 base T copper Ethernet cable. Farms are accessed through this connection.**

8. **If you have chosen to install the image server as a separate machine, connect the image server ports as follows.**

   a. **Connect the `eri0` port of the image server to a 100 base T port on the control plane switch with 100 base T copper Ethernet cable.**

   b. **Connect the `eri1` port of the image server to the internal network switch with 100 base T copper Ethernet cable.**

   c. **Connect the NIC port of the image server to a port with the same bit-rate capacity on the data plane switch.**

      Use a cable appropriate for the type of interface card installed in the image server and control plane switch: 100 base T copper for a 10/100 base T NIC, and 1000 base T copper for a gigabyte-capable NIC.

Note – If you have chosen to install the N1 image server on a separate machine, install a gigabyte-capable card such as the Sun GigaSwift NIC or the SysKonnect NIC in the image server machine.

Connecting Two or More Chassis

This section illustrates the topology of a two or more chassis I-Fabric, and provides the procedure for connecting the I-Fabric components.

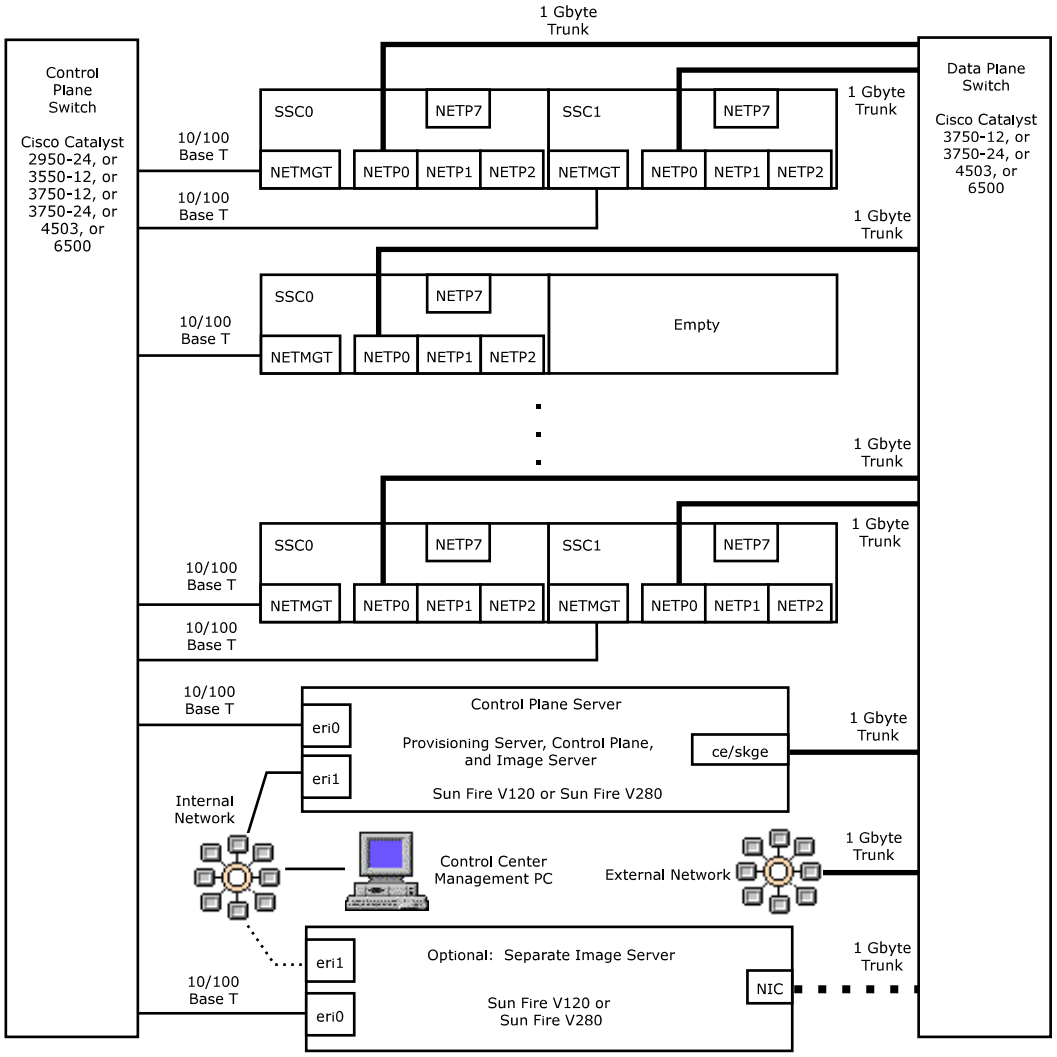

FIGURE 3–5 Two or More Chassis with Separate Control Plan and Data Plane Switches

▼ To Connect Two or More Chassis to the Control Plane Server and Switches

Steps **1. For each chassis, perform the following steps:**

a. Connect the `NETMGT` port of `SSC0` to the control plane switch with 100 base T copper Ethernet cable.

b. **Connect the `NETP0` port of `SSC0` to a data plane switch gigabit port with 1000 base T copper Ethernet cable.**

c. **If `SSC1` present, connect the `NETMGT` port of `SSC1` to the control plane switch with 100 base T copper Ethernet cable.**

d. **If `SSC1` present, connect the `NETP0` port of `SSC1` to a data plane switch gigabit port with 1000 base T copper Ethernet cable.**

2. **Connect the `ce0/skge0` port of the control plane server to data plane switch gigabit port with 1000 base T copper Ethernet cable.**

3. **Connect the `eri0` port of the control plane server to a 100 base T port on the control plane switch with 100 base T copper Ethernet cable.**

4. **Connect the `eri1` port of the control plane server to the internal network switch with 100 base T copper Ethernet cable.**

5. **Connect the Control Center Management PC NIC port to the internal network switch.**

   The type of cable depends on the capacity of the PC NIC and the network switch ports.

6. **Connect the data plane switch to the external network with 1000 base T copper Ethernet cable. Farms are accessed through this connection.**

7. **If you have chosen to install the image server as a separate machine, connect the image server ports as follows.**

   a. **Connect the `eri0` port of the image server to a 100 base T port on the control plane switch with 100 base T copper Ethernet cable.**

   b. **Connect the `eri1` port of the image server to the internal network switch with 100 base T copper Ethernet cable.**

   c. **Connect the NIC port of the image server to a port with the same bit-rate capacity on the data plane switch.**

      Use a cable appropriate for the type of interface card installed in the image server and control plane switch: 100 base T copper for a 10/100 base T NIC, and 1000 base T copper for a gigabyte-capable NIC.

Note – If you have chosen to install the N1 image server on a separate machine, install a gigabyte-capable card such as the Sun GigaSwift NIC or the SysKonnect NIC in the image server machine.

Connecting Terminal Servers

Connecting a terminal server to the control plane is optional. The terminal server typically has power in, one Ethernet port, and 32 serial ports out, as shown in the following figure.

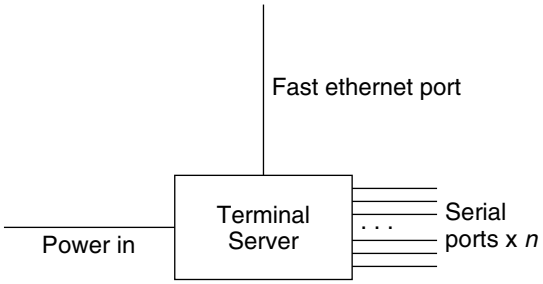

FIGURE 3–6 Terminal Server Connections

Serial connections allow out-of-band access to certain devices. Devices with serial connections have their ports labeled s0, s1, and so forth. Terminal servers have their ports labeled with a number, for example, 1, 2, 3, and so forth.

Note – Only the control plane server, image server, and the chassis SSC switch controller and system controller are automatically discovered during the installation process. Other devices, such as terminal servers, are not added to the database.

The connection guidelines for a terminal server are as follows:

- Connect the terminal server to a power controller or constant power.
- Connect the terminal server serial port to the control plane switch.
- Connect the terminal server Fast Ethernet port to a control plane switch port.

Configuring the Control Plane Switch

You can use the Cisco 2950, 3550, or 4503 switch to provide connectivity for the control plane of the N1 Provisioning Server software. In a typical scenario, the management port of the control plane server and the management port of the chassis switches are connected to this switch.

Note – Refer to the Cisco documentation for login procedures and commands.

The management VLAN configured on this switch should be `vlan 9`. Log onto the control plane switch, and type the following commands to create VLAN 9.

```
enable
vlan database
 vlan 9 name ManageMentVlan state active media ethernet
 exit
```

Although the control plane server does not require the control plane switch to have IP connectivity on the management VLAN, you can optionally configure a management IP address on this switch. Type the following commands to create a management IP on this switch:

```
enable
configure terminal
interface Vlan1
 no ip address
 shutdown
 exit
interface Vlan9
 ip address <IP_address> <IP_subnet_mask>
 no shutdown
 end
```

Because the VLAN 9 interface is configured with an IP address, you also need to move the uplink to the external router to VLAN 9. To move the uplink, type the following commands:

```
configure terminal
interface FastEthernet 0/<port>
switchport access vlan 9
speed 100
duplex full
end
```

To set the default gateway on the device, type the following command :

```
configure terminal
ip default-gateway <IP_of_default_gateway>
end
```

To enable a telnet connection to the switch, type the following commands:

```
configure terminal
line vty 0 4
 password <PASSWORD>
 login
line vty 5 15
 password <PASSWORD>
 login
```

```
 exit
```

To set the `enable` password for the switch, type the following commands:

```
configure terminal
enable password 0 <password>
end
```

To move a port to a particular VLAN, do the following steps:

1. Use `telnet` or `console` to connect to the switch.
2. Enter `enable` and `configure` mode and type the following commands.

```
interface <IF_NAME>
 switchport access vlan <VLAN_ID>
 speed 100
 duplex full
 end
```

You must move all chassis `NETMGT` and control connections from the control plane and image server to VLAN 9.

The following example shows a management port of a chassis switch that is connected to FastEthernet0/24 being moved to `vlan 9`.

```
configure terminal
interface FastEthernet0/24
 switchport access vlan 9
 end
```

When you are done, type **`write mem`** to permanently save all the configurations.

To view the switch configuration type **`show configuration`**. The following example shows an example of the output of the `show configuration` command.

```
sw-2950#show configuration
Using 1647 out of 32768 bytes
!
version 12.1
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sw-2950
!
enable secret 5 $1$byj9$P2S4zO48RKZBG3Sz0F4J/.
enable password root
!
ip subnet-zero
!
spanning-tree extend system-id
!
!
```

```
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address

     .!
     .!
     .!

interface FastEthernet0/23

!
interface FastEthernet0/24
 switchport access vlan 9
 no ip address
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan9
 ip address 10.5.131.210 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
line vty 0 4
 password root
 login
line vty 5 15
 password root
 login
!
end
```

Configuring Data Plane Switch Connections

You can use the Cisco 3750, 4503, or 6500 switch to provide connectivity for the data plane of the N1 Provisioning Server software. In a typical scenario, the data plane switch is connected to the gigabit VLAN-capable network interface cards (NIC) of the provisioning servers, and to the switch ports of each chassis. The data plane switch can also be optionally attached to an external router or switch.

The presence or absence of these connections and the number of ports used depends on the network topology implemented. Ensure that the duplex and speed on both ends of the connection is properly auto-negotiated. Otherwise, network performance might be adversely affected. Also, if multiple ports are used for improving bandwidth between switches or switch—router connections, enable link aggregation on these ports.

Note – Refer to the Cisco documentation for login procedures and commands.

Before setting VLAN rules to ports, VLANs need to exist in the switch's VLAN database. Log onto the data plane switch, and type the following commands:

```
c3750-eng1>enable
Password:c3750-eng1# vlan database
c3750-eng1(vlan)# vlan 1 name DefaultVlan media Ethernet state active
c3750-eng1(vlan)# vlan 4 name IdleVlan media Ethernet state active
c3750-eng1(vlan)# vlan 8 name ImageVlan media Ethernet state active
c3750-eng1(vlan)# vlan 10 name VLAN10 media Ethernet state active
c3750-eng1(vlan)# vlan 11 name VLAN11 media Ethernet state active.
.
.
```

Ensure that the data plane trunk connections to the server gigabit NICs and chassis `NETP0` ports allow traffic on VLANs 4, 8, and 10 through 255.

When done creating all VLANs, press control-z or end to leave the configuration mode.

The following describes the configuration steps for ports involved in these connections.

▼ To Configure Data Plane Switch Ports

Steps

1. **Connect ports to the external switch or router.**

   Configure these ports as trunk ports that allow tagged packets using `dot1q` notation. By default, most Cisco switches allow all created VLANs to pass through if a port is in trunk mode. However, if this behavior is not implicit to the external switch being used, explicitly set the ports to allow all VLANs to pass through.

   For example, on the Cisco 3750 and 4503 switches, the set of commands to achieve this for port `GigabitEthernet 0/6` are as follows:

   ```
   c3750-eng1>enable
   Password:
   c3750-eng1#config term
   Enter configuration commands, one per line.  End with CNTL/Z.
   ```

```
c3750-eng1(config)#interface Gigabitethernet 0/6
c3750-eng1(config-if)#switchport trunk encapsulation dot1q
c3750-eng1(config-if)#switchport mode trunk
c3750-eng1(config-if)#^Z
c3750-eng1#
```

2. **Connect ports to the `NetP0` switch port of the chassis.**

   Configure the remaining ports in the same manner and execute the same commands as described in the previous step.

3. **Connect the port to a VLAN-aware NIC of the provisioning server.**

   Configure the port in the same manner and execute the same commands as described in step 1.

Assigning IP Addresses in the Control Plane

Each N1 Provisioning Server control plane component must be assigned IP addresses within a single subnet. Each chassis SSC controller must be IP-accessible from the control plane server and the subnet. For added security, the subnet to which you assign the components should be an *internal subnet* and not an *external subnet*:

- **Internal subnets** are used to create IP address namespaces for I-Fabric CPU devices that do not require network connectivity outside the corporate network (for example, to the Internet) via an external router. Internal subnets are defined based on an internal corporate IT convention to prevent namespace collisions between various internal subnets. Check your internal subnet namespace scheme for availability of internal subnet addresses for use within the I-Fabric. Enter these subnets as internal subnets during installation.
- **External subnets** are assigned by an outside entity to a corporate network when I-Fabric CPU devices require connectivity outside the corporate network. If your I-Fabric is connected to an external router and you want the CPU devices in a farm to access the Internet, check your external subnet namespace scheme for availability of external subnet addresses for use within an I-Fabric. Enter these subnets as external subnets during installation.

If you choose to use a different IP addressing structure, make note of the IP address assignments for each component. You are prompted for the IP addresses of the components during installation.

The following tables provide suggested IP address assignments for the N1 Provisioning Server and optional separate N1 image server, and the chassis components. The subnet addressing scheme *10.5.141.xx* is only used as an example in the following tables.

- Refer to the *Solaris 8 Administration Guide* for the procedure for setting server IP addresses.
- Refer to the Sun Fire B1600 Blade System Chassis Switch Administration Guides for the procedure for setting chassis component IP addresses.

TABLE 3–3 Control Plane Switch and N1 Provisioning and Image Server IP Address Assignments

Machine	IP Assignment
Cisco control plane switch	10.5.141.10
Combined N1 Provisioning Server and Image Server (control plane server)	Port `eri0`: 10.5.141.18
Stand-alone N1 Provisioning Server (control plane server)	Port `eri0`: 10.5.141.18
Stand-alone N1 Image Server	Port `eri0`: 10.5.141.20
	Port `eri1`: 10.5.141.22

The SSC login and password for each chassis system switch and system controller must be identical for all SSCs in all chassis. For procedures describing how to set the SSC switch and controller logins and passwords, see the *Sun Fire™ B1600 Blade System Chassis Administration Guide*

TABLE 3–4 Blade System Chassis Component IP Address Assignments

Component	Chassis 1	Chassis 2	Chassis 3	Chassis N
Virtual IP (VIP)	10.5.141.50	10.5.141.55	10.5.141.60	Prior Chassis VIP address +5
System Controller 0 (SSC0)	10.5.141.51	10.5.141.56	10.5.141.61	Prior Chassis SSC0 address +5
System Controller 1 (SSC1)	10.5.141.52	10.5.141.57	10.5.141.62	Prior Chassis SSC1 address +5
Switch 0 (SW0)	10.5.141.53	10.5.141.58	10.5.141.63	Prior Chassis SW0 address +5
Switch 1 (SW1)	10.5.141.54	10.5.141.59	10.5.141.64	Prior Chassis SW1 address +5

Set the IP address, netmask, and gateway for each chassis SSC switch according to your control subnet as described in the following procedure.

▼ To Manually Set an SSC IP Address, Netmask, and Gateway

Steps

1. **Use telnet to access the chassis SSC.**
2. **To set up the SSC, type `setupsc`.**

   The following messages appear.

   ```
   Entering Interactive setup mode.
   Use Ctrl-z to exit & save. Use Ctrl-c to abort
   Do you want to configure the enabled interfaces [y]?
   ```

3. **Type `y` to configure the SSC.**

   You are prompted in succession for each SSC configuration value. The default values are shown in brackets (`[]`).

   The default values for the SSC IP address, netmask, and gateway are as follows.

   ```
   Enter the SC IP address [10.5.132.65]:
   Enter the SC IP netmask [255.255.255.0]:
   Enter the SC IP gateway [10.5.132.1]:
   ```

   Type the address if your chosen address is different, or press Enter to accept the default.

Installing the N1 Provisioning Server Database

The N1 Provisioning Server 3.1, Blades Edition software enables you to use either the Oracle 8i database, version 8.1.7, or the PostgreSQL database, version 7.4. During installation, you are given the choice to use either the Postgres or the Oracle database.

- The PostgreSQL database is included on the installation DVD-ROM. If you choose to use PostgreSQL, skip this section. The PostgreSQL database is installed during N1 Provisioning Software installation.
- If you choose to use Oracle, you must purchase and install the 32–bit version of the Oracle 8.1.7 database before you can install the N1 Provisioning Server software as described by this section.

You must obtain the Oracle software and a license for the software which covers at least the number of connections that you will use. The N1 Provisioning Server software requires a number of concurrent connections to the Oracle database instance running on the N1 Provisioning Server. However, the number of connections that any particular organization might require is generally difficult to determine. Consequently, you should obtain a CPU license from Oracle, either perpetual or on a yearly basis.

You need to install the 32-bit version of the Oracle 8i database. If you do not have this version, you can download Oracle 8i from the Oracle Web site. Before you start the Oracle installation, you need to create the following user and group names, which are required during the Oracle installation:

- User name – `oracle`
- Group name – `dba`

Install Oracle 8i according to the Oracle 8i installation instructions. Follow the steps for a typical installation. The N1 Provisioning Server installation process creates separate control plane and control center databases. You can remove the Oracle database after a successful Provisioning Server installation if you require more disk space.

Be sure to note the full path of the Oracle installation directory, `ORACLE_HOME`. The `ORACLE_HOME` environment variable is required for the N1 Provisioning Server software installation, and must be set on the control plane server.

CHAPTER 4

Installing Provisioning Server Software

This chapter describes the process of installing and setting up the N1 Provisioning Server software for the first time. This chapter includes the following topics:

Installation Worksheets

This section provides a list of tasks that must be done before you install N1 Provisioning Server software, and a worksheet that lists the information you need to provide to the installation process.

Prerequisites

The following prerequisites must be met before you install the N1 Provisioning software:

- ❒ The server, chassis, and switch hardware have been connected, as described in "Connecting the Chassis to the Control Plane Server and Switches" on page 56.
- ❒ IP addresses have been assigned, as described by "Assigning IP Addresses in the Control Plane" on page 68.
- ❒ All server, chassis, server blade, and switch hardware has been procured and firmware updated to the required versions, as described in Chapter 2.
- ❒ Gigabit-capable Ethernet network cards have been installed in the control plane server and if separate, the image server, as described in "Installing Gigabit Ethernet Network Interface Cards" on page 50

- ❒ The Solaris 8 2/02 operating environment has been installed in the control plane server and if separate, the Image server, as described in "Installing the Solaris Operating System, version 8 2/02" on page 52.
- ❒ Required system and gigabit Ethernet network card patches have been installed, as described in "Installing Required Patches" on page 54
- ❒ If you have chosen to use the Oracle Relational database for the Infrastructure Database, Oracle 8i, version 8.1.7 must be installed on the control plane server, as described in "Installing the N1 Provisioning Server Database" on page 70.

Installation Worksheet

During installation, you are asked for specific information. Use the following table to record the values before you install N1 Provisioning Server.

TABLE 4–1 Information Required by the Installation Process

Description	Value
IP Address of the external DNS server to which unknown queries are forwarded. If you do not want to forward unknown queries, leave this blank. Example: `201.10.51.155`	_____
Provide the 24-bit Image Copy subnet IP address netmask. The IP address is reserved for use by image copy processes only. Example: `192.0.0.0/24`	_____
Provide the total number of server blades in all B1600 chassis.	_____
Provide the name of the database software to use [Oracle | Postgres]	_____
If you are using the Oracle database, provide the following information:	
The name of the directory where Oracle is installed. Example: `/opt/oracle/OraHome1`	_____
The name of the Oracle database data directory. The directory must be empty or installation fails. Example: `/oracle_data1`	_____

TABLE 4–1 Information Required by the Installation Process *(Continued)*

Description	Value
The database primary logs directory name. The directory must be empty or installation fails. Example: `/oracle_data2`	_____
The database secondary logs directory name. The directory must be empty or installation fails. Example: `/oracle_data3`	_____
If you are using the Postgres database, provide the following information:	
The name of the Postgres home directory. Example: `/postgres_data`	_____
The name of the Postgres database logs directory. Example: `/postgres_log`	_____
The database administrator server user name if different than the default name `admin`.	_____
The database user name if different than the default name `system`.	_____
The Control Center database user name if it is different than the default name `tcc`.	_____
If you enable database email notification, provide the following information:	
The name of a valid user account from which Oracle notification messages are to be sent.	_____
The name of a valid user account to which Oracle notification messages are to be sent.	_____
The name of your SMTP mail server.	_____
The fully qualified DNS domain name for the N1 Provisioning server. Example: `n1ps.sun.com`	_____
Provide the range or ranges of virtual local area network (VLAN) numbers from 11 through 255 that are to be allocated to the Resource Layer VLANs for your farms. Example: `11-24, 25, 26-35`	_____

TABLE 4–1 Information Required by the Installation Process *(Continued)*

Description	Value
Provide the IP addresses, mask length, and subnet type (internal or external) for all Resource Layer subnets. The IP addresses must be unique, and cannot be the same as the control subnet or the image subnet.	_____ _____ _____ _____
Internal subnets are non-routable addresses that are used internally to communicate with farm devices. Example: `10.8.0.0/24/i`, `192.168.16.0/24/i`	
External subnets are externally routable addresses. Example: `220.240.255.0/24/e`, `204.16.18 /24/e`	
Provide the following information for each blade system chassis and switch network:	
Blade system controller IP address. Example: `10.5.144.50`	_____
SSC0 switch IP address. Example: `10.5.144.53`	_____
SSC1 switch address. Example: `10.5.144.54`	_____
Note – The SSC1 switch address must be specified even if the chassis has only one SSC. The IP address is reserved for possible addition of a second SSC.	
SSC default gateway IP address. Example: `10.5.144.1`	_____
Chassis netmask. Example: `255.255.255.0`	_____
Note – All chassis have the same default gateway and netmask.	
Chassis SSC user login name.	_____
Note – The SSC login and password must be the same for all chassis during the initial installation or installation fails.	

Installing the N1 Provisioning Server Software

You can install the N1 Provisioning Server and N1 image server software on the same machine, or on separate machines.

Note – The installation process aliases the control plane server as `idb`, and modifies the `/etc/hosts` file accordingly.

Installing the N1 provisioning software can take two and a half hours or more depending on the number of chassis and server blades. Validating the server blade configuration takes approximately 25 minutes for each chassis.

▼ To Install the Provisioning Server and Image Server Software

Before You Begin

All tasks described by Chapter 3 must be completed successfully before you can proceed with this task.

Steps

1. **Log in as root (su - root) on the control plane server.**
2. **If you are going to use the Postgres database, create the Postgres database group and user accounts.**
   a. **Type `groupadd dba` to create the database administration group for the Postgres database.**
   b. **Type `useradd -g dba postgres` to add the Postgres user account.**
3. **Insert the N1 Provisioning Server installation DVD-ROM into the DVD-ROM drive.**
4. **Type `./cdrom/cdrom0/install` to run the N1 Provisioning Server installation script.**

   The following messages appear.

```
/cdrom/cdrom is removable, relocating to /tmp ...
Installer for N1 Provisioning Server Software version 3.1.3.2.


Enter the roles to install.
```

```
PS: Provisioning Server Only
PS IS: Provisioning Server and Image Server on a single system
Press enter to install both roles on a single system. [PS IS]:
```

5. **Choose whether to install both the Provisioning Server and the Image Server software.**

   - If you are installing both the Provisioning Server and the image server software on a the control plane server, press Enter. The following messages appear.

     ```
     Installing Roles: PS IS
     Continue (y/N):
     ```

   - If you are installing only the Provisioning Server software on the control plane server, and installing the image server on a separate machine, type **`PS`**. The following messages appear.

     You will be prompted near the end of the installation process for information about the separate image server machine.

     ```
     Installing Roles: PS
     Continue (y/N):
     ```

   Type **`y`** to continue.

   You are notified that configuration of the Provisioning Server software is in progress. After configuration completes, the install process checks for the type of gigabit Ethernet card that is installed.

6. **If needed, reboot the system.**

   - If the SysKonnect gigabit ethernet card is installed on the control plane server, the following messages appear.

     ```
     The syskonnect configuration file has been updated to support vlans. A
     reboot is required to enable the new configuration to take effect.
     ```

     Reboot the system. When the system finishes booting, repeat steps 1 through 4. When prompted to continue, type **`y`**.

     The installation process backs up the system state and stops all provisioning server services.

   - If the Sun GigaSwift gigabit ethernet card is installed, no messages are displayed. A system reboot is not needed.

     The installation process backs up the system state and stops all provisioning server services.

   The installation process then checks whether JRE 1.4.1 is installed.

7. **If needed, accept the JRE 1.4.1 license.**

   - If JRE 1.4.1 is not already installed, the JRE 1.4.1 license agreement appears. Read the license agreement. You are prompted whether to accept the license.

     Type **`yes`** to agree to the license terms and install JRE 1.4.1 and continue the installation process.

Type **no** if you disagree with the license terms. The installation process exits to the system prompt.

- If JRE 1.4.1 is already installed, you are not prompted to agree to the JRE license.

The install process installs the Provisioning Server packages. Informational messages about the configuration and each package appear. For a list of the packages installed and descriptions of each package, see Appendix B.

The following menu appears when package installation has completed.

```
N1 Provisioning Server Install Main Menu

  1.  IP Address of external DNS server to forward unknown queries:
  2.  Image Copy Subnet:
  3.  Number of Sun Blades to be managed:
  4.  Database software: Postgres
      4.1.   Infrastructure Database parameters ->
      4.2.   Control Center Application Server and Database parameters ->
  5.  Datacenter DNS Domain Name for this N1 Provisioning Server:
  6.  Resource Layer VLANs: <list>
  7.  Resource Layer Subnets:
  8.  Sun Blade System Chassis Information for discovery ->
  9.  Flash snapshot permission:
 10.  Directory where images will be stored:


Please select an item by entering the index value preceding it ('x' to
   exit, 'help' for usage information) :
```

Tip – To display an explanation of installation menu navigation. type **help** at the prompt.

For a detailed description of the menu items, see Appendix A

Note – Each time you enter the requested values, the Provisioning Server Install Main Menu is redisplayed with the values you specified listed.

---

8. **Type `1` to specify the IP address to which to forward unknown queries.**

   The following prompt appears.

   ```
   Enter DNS Forwarder IP (<ENTER> for none) :
   ```

   Type the IP address to which unknown queries are to be forwarded.

   If you do not have an external IP address, press Enter to leave this field blank. An incorrect entry causes installation to fail.

   The Install Main Menu reappears with the IP address displayed for item 1.

9. **Type `2` to specify the IP address of the Image Copy subnet.**

   The following prompt appears.

   ```
   Enter Image Copy Subnet (example: 10.42.42.0/24):
   ```

   Type the IP address for the Image Copy subnet.

   The Install Main Menu reappears with the IP address displayed for item 2.

10. **Type `3` to specify the number of server blades that are to be managed.**

    The following prompt appears.

    ```
    Enter the number of blades to be managed:
    ```

    Type the total number of server blades contained in all of the chassis that are to be managed by the N1 Provisioning Server.

11. **Type `4` to specify the database software.**

    The following prompt appears.

    ```
    Enter the Database software to use [Oracle|Postgres]:
    ```

12. **Type the name of the database to use exactly as shown by the prompt.**

    The installation Main Menu reappears.

13. **Type `4.1` to specify the Database Parameters.**

    - If you specified Oracle in Step 12, go to Step 14.

Caution – The Oracle database must already be installed on the control plane server. See "Installing the N1 Provisioning Server Database" on page 70. If you specify Oracle, and have not installed the Oracle database, installation will fail.

    - If you specified Postgres in Step 12, go to Step 16.

14. **Specify the Oracle database parameters.**

    The Infrastructure Database parameters menu appears.

    ```
    Infrastructure Database parameters

      1.  The directory where Oracle is installed:
      2.  Database Data Directory:
      3.  Database Log Directory 1:
      4.  Database Log Directory 2:
    ```

Note – The Oracle Data and Log directories must be empty or installation fails. If the directory names you specify do not exist, the installation software creates the directories.

a. Type `1` to provide the name of the Oracle home directory.

The following prompt appears.

```
Enter the oracle home directory [/opt/oracle/OraHome1]:
```

If you installed Oracle in the above default directory, press Enter. If you installed Oracle in a different location, type the full path of the `Orahome1` directory.

b. Type `2` to provide the database data directory name.

The following prompt appears.

```
Enter the directory name to use for the database data [/oracle_data1]:
```

Press Enter to accept the default, or type the full path of the directory you want to use for database data.

c. Type `3` to provide the database primary logs directory.

The following prompt appears.

```
Enter the primary directory name to use for the database logs
[/oracle_data2]:
```

Press Enter to accept the default, or type the full path of the directory you want to use for as the primary directory for storing database logs.

d. Type `4` to provide the database secondary logs directory.

The following prompt appears.

```
Enter the secondary directory name to use for the database logs
[/oracle_data3]:
```

Press Enter to accept the default, or type the full path of the directory you want to use as the secondary directory for storing database logs.

Type **`x`** to return to the Installation Main Menu.

15. Type `4.2` to specify the Oracle Control Center application server and Database parameters.

The following submenu appears.

```
Control Center Application Server and Database parameters

  1.  Admin Server user name:
  2.  Admin Server password:
  3.  Oracle database administrator user (see help for details):
  4.  Oracle database administrator password:
  5.  Oracle database user:
  6.  Oracle database password:
  7.  Enable Mail Notification:
```

a. Type `1` to provide the administrator server user name.

The following prompt appears.

```
Enter Admin Server user name [admin]:
```

Press enter to accept the default, or type the administration server user name if it is different.

Note – The database submenu is redisplayed with the values you provided for each submenu item.

---

b. Type 2 to provide the administrator server password.

The following prompt appears.

```
Enter admin server Password:
```

Type the administration server password. The password must be at least 8 characters. You are prompted to confirm the password. Type the password again.

c. Type 3 to provide the database administration user.

The following prompt appears.

```
Enter DBA user [system]:
```

Press enter to accept the default, or type the database administration user name if it is different.

This is the *Oracle* user account that is used to create the control center database. The account must have full Oracle DBA administrative privileges. This account is the DBA account created within the Oracle database during database installation. It is not a UNIX user account called `oracle`. Refer to the Oracle documentation for further information.

d. Type 4 to provide the database administration password.

The following prompt appears.

```
Enter Oracle DBA Password:
```

Type the database administration user password. You are prompted to confirm the password. Type the password again.

e. Type 5 to provide the Control Center database user name.

The following prompt appears.

```
Enter user name for the control center database [tcc]:
```

Press enter to accept the default, or type the Control Center database user name if it is different.

f. Type 6 to provide the Control Center database user password.

The following prompt appears.

```
Enter Oracle database user Password:
```

Type the database user password. You are prompted to confirm the password. Type the password again.

g. Type `7` to enable or disable email notification.

The following prompt appears.

```
Do you want to enable email notification? ([n]/y)
```

- To enable email notification, type **`y`**.

  The email specifications menu appears. Go to Step 17

- To disable email notification, type **`n`** and then type **`x`** to return to the Installation Main Menu.

  Go to Step 18

16. Specify the Postgres Control Center application server database parameters.

The following submenu appears.

```
Infrastructure Database parameters

  1.  Database Data Directory:
  2.  Database Log Directory 1:
```

a. Type `1` to provide the name of the Postgres home directory.

The following prompt appears.

```
Enter the directory name to use for the database data [/postgres_data]:
```

Press Enter to install Postgres in the default directory `/postgres_data`. If you want to install Postgres in a different directory, type the full path of the directory.

b. Type `2` to provide the name of the database logs directory.

The following prompt appears.

```
Enter the primary directory name to use for the database logs
 [/postgres_log]:
```

Press Enter to use `/postgres_log` as the directory in which to store the database logs. If you want to store the logs in a different directory, type the full path of the directory.

The following submenu appears.

```
Control Center Application Server and Database parameters

  1.  Admin Server user name:
  2.  Admin Server password:
  3.  Database user:
  4.  Database password:
  5.  Enable Mail Notification:
```

c. Type `1` to provide the administration server user name.

The following prompt appears.

```
Enter Admin Server user name [admin]:
```

Press enter to accept the default, or type the administration server user name if it is different.

Note – The password must be at least 8 characters. You are prompted to confirm your password by typing the password again.

---

d. Type `2` to provide the administration server password.

The following prompt appears.

```
Enter admin server Password:
```

Type the administration server password. You are prompted to confirm the password. Type the password again.

e. Type `3` to provide the Control Center database user name.

The following prompt appears.

```
Enter user name for the control center database [tcc]:
```

Press enter to accept the default, or type the Control Center database user name if it is different.

f. Type `4` to provide the Control Center database user password.

The following prompt appears.

```
Enter Database user Password:
```

Type the database user password You are prompted to confirm the password. Type the password again.

g. Type `5`to choose whether to enable email notification.

The following prompt appears.

```
Do you want to enable email notification? ([n]/y)
```

- To disable email notification, type **`n`** and then type **`x`** to return to the Installation Main Menu.

  Go to Step 18

- To enable email notification, type **`y`**.

  The email specifications submenu appears.

17. Specify database email notification values.

When you enable email notification, the following submenu appears.

```
7.1 Mail From:
 7.2 Mail To:
 7.3 SMTP host name:
```

a. Type `1`.

Provide the name of a valid user account for sending mail. The mail submenu reappears.

b. Type `2`.

Provide the name of a valid user account for receiving mail. The mail submenu appears.

c. Type `3`.

Provide the host name of the SMTP mail server on your intranet.

d. Type `x` to return to the Installation Main Menu.

18. Type `5` to provide the DNS Domain Name for the Provisioning Server.

The following prompt appears.

```
Enter the fully qualified dns domain name:
```

Type the fully qualified DNS domain name for the Provisioning Server. For example; `n1ps01.companyname.com`.

19. Type `6` to allocate the virtual local area networks (VLANs) for your farms.

The following prompt appears.

```
Resource Layer VLANs

  1. 10-255

  These are the VLANs that will be allocated to your farms. Each Resource
  VLAN must be a valid integer range such as '11-23' or '25'

  Choose an operation to perform on the list.
  a - add item       d - delete item
  i - insert item    x - exit
  [a|d|i|x]:
```

Type **`a`** to add a VLAN range. The following prompt appears.

```
Add Item to List
  Enter a VLAN range (example: '11-23'):
```

Type a range of VLANs to allocate for a farm, for example, **`10-22`**. The Resource Layer VLAN menu is redisplayed.

Repeat this step until you have allocated all VLANs. When you have completed adding VLAN ranges for the farms, type **`x`** to exit the VLAN menu.

The Install Main Menu appears.

20. Type `7` to provide the Resource Layer Subnets IP addresses

The following prompt appears.

```
Resource Layer Subnets

  <Empty List>
```

```
These are the subnets that are allocated to your farms. Each resource
subnet must be of the form '<subnet address>/<i|e>' where <subnet
address> is of the form '<subnet ip>/<masklen>' and the final 'i' or 'e'
indicates whether this is an internal subnet or an external subnet. For
example: '10.8.0.0/24/i' and '220.240.255.0/24/e' are valid values.

Choose an operation to perform on the list.
a - add item       d - delete item
i - insert item    x - exit
[a|d|i|x]:
Add Item to List
Enter Resource Subnet (example: 10.8.0.0/24/i):
```

Type **a** to add a Resource Layer subnet. The following prompt appears.

```
Add Item to List
  Enter Resource Subnet (example: 10.8.0.0/24/i):
```

Type a valid subnet value. The Resource Layer Subnets menu is redisplayed.

Repeat this step until you have entered all Resource Layer subnets. When you have completed adding subnet values for the farms, type **x** to exit the VLAN menu.

The Installation Main Menu appears.

21. Type `8` to provide the blade system chassis information for discovery.

The following menu appears.

```
Sun Blade System Chassis Information for discovery

  1.  Blade System Chassis IP Addresses and Switch Network Configuration:
  2.  Blade System Controller and Switch User Login (Note: The System
      Controllers and Switches for ALL the Blade System Chassis MUST have
      the same login):
  3.  Blade System Controller and Switch Password (Note: The System
      Controllers and Switches for ALL the Blade System Chassis MUST have
      the same password):


  Please select an item by entering the index value preceding it ('x' to
  exit, 'help' for usage information) :
```

a. Type `1` to provide the chassis IP addresses and switch network configuration.

The following menu appears.

```
Blade System Chassis IP Addresses and Switch Network Configuration

  sc_ip         sw1_ip      sw2_ip       default_gw    netmask
  ------------------------------------------------------------------
  <empty list> <empty list> <empty list> <empty list> <empty list>

  These are the IP Addresses of the SunFire Blade System Chassis in your
  I-Fabric. Each Blade System Controller IP Address must be accompanied by
  network configuration data for the Switches on that Blade System Chassis.
  The install program uses the SC IP Address to connect to the SunFire
  Blade System Controller and uses the rest of the information for
```

```
*configuring** the switches on that blade system chassis. Note that the
installer will destroy any existing switch configurations and replace it
with the supplied information.

You *must* supply 2 IP addresses for the switches even if only one switch
is present in a shelf. The installer will ignore the unused address but
you should keep it reserved  for possible addition of a second switch.

Choose an operation to perform on the list.
a - add item         d - delete item
i - insert item    x - exit
[a|d|i|x]:
```

Note – A switch address must be specified for `SSC1` (a second SSC) even if the chassis has only one SSC. The IP address is reserved for possible addition of a second SSC.

- **Add the chassis information.**

  Type **a**. The following prompt appears.

  ```
  Add Item to List
    Enter Blade System Controller IP Address:
  ```

  Type the chassis system controller IP address, for example, `10.5.144.50`. The installation process pings the address to ensure it exist. If it exists, the following message appears:

  ```
  Pinging 10.5.144.50 ...success!
  ```

  The following prompt appears.

  ```
  Enter First Switch IP Address:
  ```

- **Type the first switch IP address.**

  The following prompt appears.

  ```
  Enter Second Switch IP Address:
  ```

- **Type the second switch IP address.**

  The following prompt appears.

  ```
  Enter Blade Switch Default Gateway:
  ```

- **Type the switch default gateway IP address.**

  The following prompt appears.

  ```
  Enter Blade Switch netmask:
  ```

- Type the netmask value.

  The values for the chassis appear. For example:

  ```
  Blade System Chassis IP Addresses and Switch Network Configuration
  ```

```
sc_ip        sw1_ip       sw2_ip       default_gw   netmask
-----------------------------------------------------------------
10.5.144.50  10.5.144.53  10.5.144.54  10.5.144.1   255.255.255.0
```

Repeat this step until you have entered the values for all of the chassis. When you have completed entering the values, type **x** to exit the Blade System Chassis IP Addresses and Switch Network Configuration menu. The blade system chassis menu reappears.

```
Sun Blade System Chassis Information for discovery

  1.  Blade System Chassis IP Addresses and Switch Network Configuration:
  2.  Blade System Controller and Switch User Login (Note: The System
      Controllers and Switches for ALL the Blade System Chassis MUST have
      the same login):
  3.  Blade System Controller and Switch Password (Note: The System
      Controllers and Switches for ALL the Blade System Chassis MUST have
      the same password):


  Please select an item by entering the index value preceding it ('x' to
  exit, 'help' for usage information) :
```

b. Type `2` to provide the chassis SSC user login.

The following prompt appears.

```
Enter Blade System Controller and Switch user login:
```

Type a user name. The blade system chassis menu reappears.

c. Type `3` to provide the chassis SSC user password.

The following prompt appears.

```
Enter Blade System Controller and Switch user Password:
```

Type the password. You are prompted to confirm the password:

```
Confirm Blade System Controller and Switch user Password:
```

Type the password again, and then type **x** to return to the Installation Main Menu.

22. Type `9` to choose whether to enable Flash snapshot permission.

The following prompt appears.

```
Enter new value [enabled|disabled]:
```

Type **`enabled`** to enable snapshot permission, or type **`disabled`** to disable snapshot permission.

If you want to specify different values for any of the menu items, type the menu item number to edit the values for that item.

23. Type `10` to specify the directory in which images are to be stored.

The following prompt appears.

```
Enter new value [/images]:
```

Press Enter to accept the default value `/images`, or type the name of a different directory.

The following prompt appears.

```
(optional) Make a backup of these settings to a file?? ([n]/y)
```

24. Choose whether to save the settings to a file.

- Type **`n`** to continue without saving the settings. Go to Step 25
- Type **`y`** to save the settings. The following messages appear.

```
Settings saved. File is /var/tmp/Profile.pl
Continue with installation??
```

  - Type **`y`** to continue the installation process. Go to Step 25.
  - Type **`n`** to exit the installation process and return to the system prompt.

    You can resume the installation process later by typing the following command from the root login prompt:

    `/cdrom/cdrom0/install -n -s /var/tmp/Profile.pl`

    When you resume the installation process, informational messages are displayed, and the installation process continues as described in the following steps.

The following prompt appears.

```
Continue with installation?? (n/[y])
```

25. Continue the installation process.

Type **`y`** to continue.

The following messages appear.

```
Done with user input.

Disabling (finger/talk/uucp/printer) / Enabling (tftp) services ...done!
Configuring DNS ...done!
Preparing the system for IDB ...done!
```

- If you selected Oracle as your database, the following messages appear.

```
The database will be created in the following directories.
    - Data Directory => /export/oracle-data1
    - Log Dirs => [/export/oracle-data2,
                   /export/oracle-data3/oracle-data3
]


  If you want to mount a second disk or an nfs share onto
  these directories, do so now. Ensure that the filesystems
  on these directories are created and empty

  If these directories do not exist after this, they will be
  created on the / filesystem
```

```
Press Enter to continue.
```

- If you selected Postgres as your database, the following messages appear.

```
The database will be created in the following directory.
     - Data Directory => /export/postgres_data

   If you want to mount a second disk or an nfs share onto
   these directories, do so now. Ensure that the filesystems
   on these directories are created and empty

   If these directories do not exist after this, they will be
   created on the / filesystem

 Press Enter to continue.
```

Press Enter to continue.

The installation process then performs setup and configuration tasks, including creation of the control plane database, DNS setup, chassis switch setup and configuration, and chassis server blade setup and configuration. After setup and configuration completes, the installation process runs discovery and starts the provisioning server services, copies required files to the control plane server, configures provisioning server settings, and sets up the ignition operating system.

The setup process then checks whether you have installed a combined Provisioning Server and Image Server.

- If you chose to install the Provisioning Server and Image Server on a single machine, the following messages appear.

```
Installation of N1 Combined Provisioning and Image Server software
 setup completed successfully.
```

  Go to Step 28

- If you chose to install the Provisioning Server software only, the following messages appear.

```
Setting up separate Image Server ...
Creating new image server 47001
Allocated ip address 10.23.44.2
Now you will need to manually set up the Image Server as follows:

1. Plumb the interface which is connected to VLAN 8

2. Configure the interface using the template:
   ifconfig ifname  inet 10.23.44.2 netmask 255.255.255.0 broadcast + up
   Make sure the interface is automatically configured during reboot

3. Create a filesystem on /images of at least 6000MB

4. Export the filesystem as:
      share -F nfs -o anon=0,rw=@10.23.44.0/24 /images
   Make sure the export is automatically shared upon reboot
```

```
When the Image Server machine configuration is complete, come back to
this machine to finish the image server setup


Press Enter  only AFTER you have set up the Image Server:
```

Caution – Do not press Enter until you have completed all of Step 26.

26. Set up the image server.

Log in as root (**`su - root`**) on the image server machine.

a. Plumb the interface connected to the data plane switch (VLAN 8).

Type the command **`ifconfig`** *ifname* **`plumb`** where *ifname* is the name of the gigabit Ethernet card interface.

b. Configure the interface.

Type the command **`ifconfig`** *ifname* **`inet 10.23.44.2 netmask 255.255.255.0 broadcast + up`** where *ifname* is the name of the gigabit Ethernet card interface.

c. Create a filesystem on `/images` that has at least 6000 Mbytes free space.

If you intend to use a partition other than `/images`, mount the partition on `/images`.

If your images directory is part of the image server root file system (`/`), skip this step.

Type the following commands to mount the partition on `/images`.

```
# mkdir /images
# newfs /dev/rdsk/partition
# mount /dev/dsk/partition /images
```

where *partition* is the partition disk location. Ensure that the partition contains at least 6000 Mbytes free space.

d. Ensure the `/image` partition is available over the network

Add the following line to the `/etc/dfs/dfstab` file.

```
share -F nfs -o anon=0,rw=@10.23.44.0/24 /images
```

e. Preserve the mount point across reboots.

Edit the `/etc/vfstab` file to preserve the mount point across reboots. See the manual page `vfstab(4)` for further information.

f. Reboot the image server machine.

When the image server has completed booting, return to the installation session on the control plane server.

27. Complete image server setup.

Press Enter. The following message appears.

```
Are you sure you have set up the Image Server? If yes, press Enter to
continue or x to exit:
```

Press Enter to continue. The installation process checks whether the image server is accessible using `ping`.

Messages similar to the following appear.

```
Checking if Image Server is pingable ...Done.
Image Server Size = 33812 Mbytes
Image Server setup completed
```

28. Complete Installation.

The installation process now imports the operating system images from the installation DVD-ROM into the image repository, and creates the server images. After server image creation completes, the installation process configures and starts the control center, and then tests the server blades. The status of each test is displayed. When server blade testing completes, the following message appears.

```
Installation of N1 Provisioning Server software completed successfully.
```

See Also To complete your N1 Provisioning Server system, perform the following tasks:

- Validate the N1 Provisioning Server installation. See "Validating the N1 Provisioning Server Installation" on page 103
- Apply role-based access control. See "Applying Role-Based Access Control" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

Installing Sun SNMP Management Agent on the N1 Provisioning Server

If you are going to use an SNMP-based monitoring and management tool such as Sun Management Center, to manage and control your blade system chassis and blades, you must install the Sun SNMP Management Agent on the control plane server. Refer to *Sun SNMP Management Agent Guide* for the Sun Fire B1600 for installation and configuration details.

Depending on the platform type, you can employ the following agents:

- A domain agent, running on Sun Fire B10n, B100s, B100x, and B200x server blades for domain hardware monitoring.

The software is installed locally on the server being monitored and only that server can be monitored. In the case of the Sun Fire B1600, each server blade is monitored separately.

The scope of domain hardware monitoring for the Sun Fire B100s blade is limited to the hardware of the blade only. The scope does not include other Sun Fire B1600 components such as the service indicators, power supply units (PSUs), SSCs and the identity of the Blade System Chassis itself.

- A platform agent, proxied through a system controller (platform hardware monitoring).

  The software is installed on the control plane server, which functions as the platform agent server to access chassis instrumentation through the system controller. This setup enables you to monitor all the hardware managed by the system controller.

  The scope of platform hardware monitoring for a Sun Fire B1600 includes the Blade System Chassis, its identity, service indicators, and all its field replaceable units (FRUs). In addition, some hardware information, specifically voltage monitoring, about the Sun Fire B100s blades is available that is not available using domain hardware monitoring.

For N1 provisioning, install the platform agent on the control plane server. After you install the platform agent packages, you need to configure both the control plane server and the B1600 chassis to use the platform agent. See *Sun SNMP Management Agent Guide for the Sun Fire™ B1600* for details.

When you install and configure the Sun SNMP Management Agent according to the instructions in *Sun SNMP Management Agent Guide for the Sun Fire™ B1600*, be sure to perform the following tasks:

- Where installation instructions say to make sure that you have installed Java 1.4. Note that for N1 Provisioning, JRE 1.4.1_01 has already been installed on the N1 Provisioning Server and the server blades. Consequently, you need to modify the Sun SNMP Management Agent startup scripts. Follow the instructions in Appendix A, Editing the Startup Scripts of *Sun SNMP Management Agent Guide for the Sun Fire™ B1600*.
- Step 5 in Installing Software for Domain Hardware Monitoring, Chapter 10 of *Sun SNMP Management Agent Guide for the Sun Fire B1600* says to see Chapter 11 to configure the software. To accommodate N1 Provisioning while editing the General, Mediator, and Master Agent Configuration files, use `cp` for the manager variable name.
- Step 5 in Installing Software for Platform Hardware Monitoring, Chapter 10 of *Sun SNMP Management Agent Guide for the Sun Fire B1600* says to see Chapter 11 to configure the software. If you have not done so already, you need to install the following Solaris packages on the N1 Provisioning Server before you install any Sun SNMP Management Agent packages:
  - `SUNWmibii`
  - `SUNWsacom`

- SUNWsadmi
- SUNWsasnm

- The N1 SNMP Trap Listener and Receiver by default listens for traps on port 162, which is also the port used by the Solstice Enterprise Agents™ master agent, snmpdx. If you install the Sun SNMP Management Agent, the N1 Provisioning SNMP Trap Listener and Receiver ports need to be changed by allocating two free open ports, one for listening and one for sending traps by adding the following lines in the /etc/opt/terraspring/tspr.properties file:

  com.terraspring.mlg.SnmpConf.SnmpTrapReceivePort=*Port for Receiving Traps*
  com.terraspring.mlg.SnmpConf.SnmpTrapSendPort=*Port for Sending Traps*

  After you add these lines, restart the SNMP Trap Receiver on the N1 Provisioning Server by executing the following commands:

  ```
  /opt/terraspring/sbin/snmpd stop
  /opt/terraspring/sbin/snmpd start
  ```

- The communication between the server blades and the N1 Provisioning Server is blocked by IP Filter. Consequently, ports 161 and 162 need to be opened on the N1 Provisioning Server to allow the Sun SNMP Management Agent software to communicate. To open these ports on the N1 Provisioning Server for Sun SNMP Management Agent, you need to add the following lines to the /etc/opt/ipf/ipf.conf file:

  ```
  pass in quick proto udp from any to any port = 162 # allow SNMP Trap
  pass in quick proto udp from any to any port = 161 # allow SNMP commands
  ```

  Also, because you must change the N1 Provisioning SNMP Trap Listener and Receiver ports, addressed in the previous item, you need to add the following lines to the /etc/opt/ipf/ipf.conf file as well:

  pass in quick proto udp from any to any port=*Port Number for Receiving Traps*
  pass in quick proto udp from any to any port=*Port Number for Sending Traps*

  After you have added these lines, restart the ipf daemon by using the following command:

  ```
  /etc/rc2.d/S65ipfboot reload
  ```

CHAPTER 5

Upgrading to N1 Provisioning Server 3.1

This chapter provides the procedure for upgrading N1 Provisioning Server, Blades Edition version 3.0 to version 3.1.

The upgrade process is applicable to installations with a combined Provisioning Server and Image server machine, and to installations with separate Provisioning Server and Image Server machines.

Upgrading to N1 Provisioning Server Version 3.1

You can perform an upgrade of the N1 Provisioning Server software on an I-Fabric that contains live farms. The Provisioning Server software cannot be patched or upgraded when the Provisioning Server services are handling farm modification requests. Farm modification requests include farm activation, moving a farm to standby, farm snapshots, DHCP synchronization, and so on. If any requests are in progress when you start the upgrade, the upgrade process exits. You are prompted to wait for the requests to complete or to stop any requests before running the upgrade. Any requests in that are in the queue before the upgrade, may fail once the request is processed after the upgrade. Therefore, all queued requests should be deleted before upgrading.

Upgrading from N1 Provisioning Server version 3.0 to N1 Provisioning Server 3.1 requires that you perform the following tasks in sequence:

- Upgrade the Provisioning Server software as directed by "To Upgrade from N1 Provisioning Server Version 3.0 to Version 3.1" on page 96
- Synchronize the chassis state and databases as directed by "To Synchronize a Chassis's Physical State and Its Information in the Database" on page 98

- Update the Control Center Application Server as directed by "To Update the Control Center Application Server" on page 101
- Import the N1 Provisioning Server version 3.1 operating system images as directed by "To Import Operating System Images" on page 102
- Delete all queued and queued-blocked requests as directed by "To Delete Queued Requests" on page 96.

Refer to the release notes to get detailed information about the upgrade, such as the list of packages that are newer than the last release, or the list of new packages and any special instructions for the upgrade.

▼ To Delete Queued Requests

Upgrades can only be performed while no requests are in progress or queued. The upgrade process verifies that no requests are in progress before starting the upgrade. However, for queued requests no such check is performed. You must check if there are any queued requests before starting the upgrade as described below. If you update N1 Provisioning Server software without deleting the queued and queued-blocked requests from the system, some of these requests may appear as failed or in error after the upgrade. You can delete the failed requests or choose to ignore them. For each request that was deleted before the upgrade or which appears as failed after the upgrade, you must reissue the request from the control center.

Steps

1. **Login in as root `(su - root)` on the control plane server.**
2. **List queued and queued-blocked requests.**

   Type **`opt/terraspring/sbin/request -l`** to list all queued and in-progress requests.
3. **Delete queued and queued-blocked requests.**

   If there are any queued or queued-blocked requests. type the command **`/opt/terraspring/sbin/request -d`** *request_id* where *request_id* is the ID of the request. This must be done for each request listed by the `request -l` command.

▼ To Upgrade from N1 Provisioning Server Version 3.0 to Version 3.1

Before You Begin

Make certain you have performed the following tasks before you start the upgrade process:

❒ Updated chassis component firmware See "Blade System Chassis Firmware Requirements" on page 42.

- ❒ Applied operating system security modifications. See “Disabling Remote Logins From Root Accounts” on page 53.
- ❒ Installed operating system and chassis patches. See “Installing Required Patches” on page 54.
- ❒ Delete all queued and queued-blocked requests as directed by “To Delete Queued Requests” on page 96.

Steps

1. **Login in as root (`su - root`) on the control plane server.**
2. **Insert the N1 Provisioning Server, Blades Edition version 3.1 DVD-ROM into the DVD-ROM drive.**
3. **Type the command `/cdrom/crom0/install` to start the upgrade.**

   The following messages appear.

   ```
   N1 Provisioning Server Software version 3.0 is already installed on
   this system.
   Continuing will upgrade to version 3.1.

   Continue (y/N):
   ```

   Type **`y`** and press Return.

   - If you are upgrading a combined Provisioning Server and Image Server machine, the following messages appear.

     ```
     Upgrading Roles: PS IS
     Continue (y/N):
     ```

   - If you are upgrading a Provisioning Server only machine, the following messages appear.

     ```
     Upgrading Roles: PS
     Continue (y/N):
     ```

   Type **`y`** and press Return.
4. **You are prompted for the database administrator user name.**

   ```
   Enter database administrator user [system]:
   ```

   Type the name of the database administrator user, or press Enter to accept the default `system`.
5. **You are prompted for the database administration password.**

   ```
   Enter database administrator Password:
   ```

   Type the database administrator password. You are prompted to confirm the database administrator password. Retype the password.
6. **You are asked whether to enable flash permission.**

   ```
   Do you want flash permission enabled?[y/n]
   ```

   To enable flash permission, type **`y`**. To disable flash permission, type **`n`**.

Messages similar to the following appear.

```
removing TSPRblibl package.
Parsing /tmp/Upgrade_24373__WML__ ...done!

Encrypting passwords ...done!Check for pending requests in progress ...done!
Configuration of Combined Provisioning and Image Server software and setup
in progress (Please wait) ...
Determining packages to upgrade/install ...removing TSPRblibl package.
Parsing /tmp/Upgrade_24373__WML__ ...done!
```

The upgrade process then stops all Provisioning Server services, backs up the control center database, and then stops the domain. The upgrade process then removes old packages and upgrades the Provisioning Server packages, updates the control plane database and state, updates the control center database, and starts the Provisioning Server services.

When the Provisioning Server services have started, the upgrade process configures the Provisioning Server settings, sets up the ignition operating system, and starts the control center. After the control center has started, the upgrade process tests each server blade.

See Also When the server blade validation tests have completed, the upgrade process exits to the system prompt. You must now synchronize each chassis with the I-Fabric as directed by the next procedure, "To Synchronize a Chassis's Physical State and Its Information in the Database" on page 98.

▼ To Synchronize a Chassis's Physical State and Its Information in the Database

Before You Begin Make certain you have upgraded the Provisioning Server software as directed by "To Upgrade from N1 Provisioning Server Version 3.0 to Version 3.1" on page 96

Note – You must synchronize each chassis in your installation. When you complete synchronizing a chassis, you are given the option to synchronize another chassis.

Steps

1. **Login in as root `(su - root)` on the control plane server.**
2. **To start the synchronization process, type the command `opt/terraspring/sbin/shelfsync`.**

   You are prompted to enter the IP address or device ID of the chassis.
3. **Provide the IP address or device ID of the chassis you want to synchronize.**

   Type the IP address or the device ID of the chassis.

   The upgrade process queries the database for the chassis, checks the chassis network connectivity, and runs discovery on the chassis. You are then prompted

for the chassis management interface user name.

4. **Provide the chassis management interface user name.**

   Type the chassis user name. You are then prompted for the chassis user name password.

   Note – The default chassis user name is `admin`.

   ---

5. **Provide the chassis user name password.**

   Type the chassis user name password. The following prompt appears:

   ```
   Are the switch user name and password the same as the management user
   name and password?
   [yY/nN]
   ```

6. **Verify that the switch user name and password are the same as the management user name and password.**

   - Type **`y`** if the user name and password are the same for the switch and chassis management.

     Note – The chassis switch user name and password and the chassis management user name and password must be the same only when discovering devices during installation. The user names and passwords do not have to be the same when you have modified a chassis or added a new chassis and are subsequently running `shelfsync`. For more information about `shelfsync`, see "Adding, Moving, and Deleting Chassis Components" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.

   - Type **`n`** if the user name and password are not the same.

   The following prompt appears.

   ```
   Is there any new switch added to the shelf that you want to bench configure?
    [yY/nN]
   ```

7. **Configure new chassis switch and system controllers.**

   - Type **`y`** if any chassis contains a new SSC.

     You are prompted in sequence for the default gateway IP address, the netmask address, the VLAN ranges, the IP address of the switch, and the SSC number of the switch. When you have provided the information required by each prompt, the upgrade process configures the new SSC. The upgrade process then runs discovery on the chassis as described below.

   - Type **`n`** if no new switches are present in any chassis.

The upgrade process runs discovery on the chassis, writes WML output for the chassis to `/var/tmp`, and retrieves the database state.

A list of recommended actions then appears. For example:

```
Recommended actions:
                Recommended
#  Cause        Action     Identification       Conflicting IDs
-- -----------  ------- ---------------------- ---------------
0  Discovered   ADD     50211 00:03:BA:26:91:AD
1  Discovered   ADD     50251 sw_50251_SSC1

* = action has been run, entering -y will suppress acknowledgement prompts

enter line number(s) from above or q for quit:
```

8. **Resolve the listed problems or continue the upgrade process.**

   - To resolve a problem, type the line number of the problem. For example, to add the device `50211` shown in the previous step, you would type **`0`** to add the device, and then provide the information for which you are prompted.
   - To continue the upgrade process, type **`q`**.

     You are given the opportunity to resynchronize the current chassis, synchronize another chassis, or exit the upgrade process.

9. **Select an action.**

```
What do you want to do next:
#1. Re-sync the current SFB1600 device with its saved state.
#2. Synchronize another SFB1600 device with its saved state.
#3. Exit.
Make selection (1-3):
```

   - To resynchronize the current chassis, type **`1`**.
   - To synchronize another chassis, type **`2`**.
   - To exit to the system prompt, type **`3`**.

Caution – You must synchronize each chassis in your installation. If you have more than one chassis, type **`2`** to synchronize the next chassis. You are prompted to provide the IP address or device ID of the chassis you want to synchronize. Go to Step 3.

See Also When you have completed chassis synchronization, update the control center application server as directed by the next procedure, "To Update the Control Center Application Server" on page 101.

▼ To Update the Control Center Application Server

Before You Begin

Make certain you have performed the following tasks before you update the control center application server:

- Upgraded the Provisioning Server software as directed by "To Upgrade from N1 Provisioning Server Version 3.0 to Version 3.1" on page 96
- Synchronized the chassis state and databases as directed by "To Synchronize a Chassis's Physical State and Its Information in the Database" on page 98

Steps

1. **Login in as root (`su - root`) on the control plane server.**

2. **Stop the Provisioning Server and the Application Server.**

   Type the command **`/opt/terraspring/sunone/bin/appserv stop`**. The following messages appear.

   ```
   Stopping admin server instance...
   Instance admin-server stopped
   Stopping server server_gw...
   Instance server_gw stopped
   ```

   - If the administrator server fails to stop, type the following command :

     `/opt/terraspring/sunone/domain_gw/admin-server/bin/stopserv`

   - If the application server fails to stop, type the following command:

     `/opt/terraspring/sunone/domain_gw/server_gw/bin/stopserv`

3. **Update the Control Center application server.**

   Type **`/opt/terraspring/sunone/bin/setup7.sh -silent -upgrade`**.

   The `setup7.sh` process copies files required for the update, updates the server and security database, and generates the required database and security keys. The update process exits to the system prompt when it has completed the update.

4. **Restart the application server.**

   Type the command **`/opt/terraspring/sunone/bin/appserv start`**. The following messages appear.

   ```
   Starting admin server instance...
   Instance admin-server started
   Starting server server_gw...
   Instance server_gw started
   ```

   - If the administrator server fails to start, type the following command :

     `/opt/terraspring/sunone/domain_gw/admin-server/bin/startserv`

   - If the application server fails to start, type the following command:

     `/opt/terraspring/sunone/domain_gw/server_gw/bin/startpserv`

   When the administrator server and application server have started, import the operating system images as directed by the next procedure, "To Import Operating

System Images" on page 102.

▼ To Import Operating System Images

Before You Begin

Make certain you have performed the following tasks before you import the N1 Provisioning Server version 3.1 operating system images:

- Upgraded the Provisioning Server software as directed by "To Upgrade from N1 Provisioning Server Version 3.0 to Version 3.1" on page 96
- Synchronized the chassis state and databases as directed by "To Synchronize a Chassis's Physical State and Its Information in the Database" on page 98
- Update the Control Center Application Server as directed by "To Update the Control Center Application Server" on page 101

Steps

1. **Log in as root (`su - root`) on the image server machine.**

2. **Type the command `ps -ef | grep mountd` to check whether the network file system (NFS) daemon is running.**

   If the NFS daemon is not running, type **`/etc/init.d/nfs.server start`** to start the NFS daemon.

3. **Import the operating system images.**

   On the control plane server, type the command **`/opt/terraspring/sbin/imagewizard -n -i /cdrom/cdrom0/Images`**. The Solaris images on the N1 Provisioning Server installation DVD-ROM are imported to the image server.

See Also

When the images have been imported, you must perform the following tasks.

- Secure the Provisioning Server. See "N1 Provisioning Server Security" on page 32
- Validate the N1 Provisioning Server installation. See "Validating the N1 Provisioning Server Installation" on page 103
- Apply role-based access control. See "Applying Role-Based Access Control" in *N1 Provisioning Server 3.1, Blades Edition, System Administration Guide*.
- If you also plan to use the Postgres as your control plane database (CPDB), migrate your data from the Oracle CPDB to Postgres. See "Migrating From Oracle to PostgreSQL" on page 112

CHAPTER 6

Post-Installation Tasks

This chapter provides the procedures for tasks that are performed after the N1 Provisioning Server software has been installed. The following topics are discussed:

Validating the N1 Provisioning Server Installation

N1 Provisioning Server validation consists of two tasks:

- Checking that all N1 Provisioning Server packages have been correctly installed on the control plane server
- Creating and activating a farm

  You can either import and then activate a default farm configuration, or you can manually create and activate a farm. Procedures for both methods are provided.

▼ To Validate Package Installation on the Control Plane Server

Steps

1. **Log in as root (`su - root`) on the control plane server.**
2. **Type the command `/opt/terraspring/sbin/check_rel` to list the installed packages and their installation states.**

   The output should be similar to the following.

```
root# /opt/terraspring/sbin/check_rel
Manifest is for Terraspring Release 3.1.1.4
Checked system for roles: SP, IDB, CC

Package      Manifest   System     Installation State
-------------------------------------------------------------------------------
NcFTPc:      3.1.5      3.1.5      completely installed
TSPRbli:     3.1.2      3.1.2      completely installed
TSPRblibs:   3.1.2      3.1.2      completely installed
    .
    .
    .
TSPRsuna:    3.1.2      3.1.2      completely installed
TSPRtools:   3.1.4      3.1.4      completely installed
root@idbqe1.qe1:~/etc/seq11017-1#
```

▼ To Validate Installation by Creating and Activating a Farm

Before You Begin

- The N1 Provisioning Server software must be installed successfully. Chapter 4.
- A PC running Internet Explorer 6.0 or later must be connected and configured to the network. See Table 2–3.

Steps

1. **Log in to the Control Center Management PC as administrator and start Internet Explorer.**

2. **Type the URL of the N1 Provisioning Server in the address field of the Internet Explorer browser.**

   The URL is the location where the Control Center software is installed, for example http://*machine_name.domain_name* where *machine_name* is the name of the control plane server, and *domain_name*is the corporate domain name.

   The Control Center login page is displayed.

3. **Click on Login Page.**

   The login screen is displayed.

4. **Type `demo` for the username and for the password.**

   The first time that you log in as an administrator, the default username is demo with password demo for the user account. You should change this information immediately after you log in for the first time. An administrator account has also been provided. The username for this account is root with password root. For further information, See "Managing Accounts" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*.

5. **Click Log In to access the Control Center Administration Screen.**

   The Administration Welcome screen is displayed.

Caution – The Internet Explorer navigation controls are intentionally disabled by the Control Center. Do not navigate by using the keyboard shortcuts such as control-K and F5. Using Internet Explorer navigation controls within the Control Center causes unpredictable behavior.

The first time that you log in, the Administration screen shows that an initial account has already been created for you. The name of this account is demo. This account is already highlighted under Accounts in the upper left corner of the screen. This initial account enables you to quickly validate the N1 Provisioning Server installation.

6. **From the Editor menu, choose Edit new farm.**
   The Editor screen is displayed with the Create New Design dialog displayed.
7. **In the Name field, type a name for your farm.**
8. **In the I-Fabric field, choose Initial I-Fabric.**
9. **Click Import Options and type a file name to import.**
   See "Importing and Exporting Farms" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide* for further information.
10. **Click OK to close the Create New Design dialog box.**
    The Editor screen appears.
11. **From the Elements box on the left, drag and drop the External Subnet element icon (displayed as a subnet with a cloud) to the Editor work area.**
12. **From the Elements box on the left, drag and drop the Server Group element icon (third element down on the left column) to the Editor work area to a position about two inches below the External Subnet element.**
13. **Click a connection point (port) on the External Subnet element. Do not hold the mouse button 3 down.**
14. **Move the cursor to the Server Group element.**
    A connection line is displayed in red.
15. **Click the Server Group element Eth0 interface node.**
    Your Control Center screen should look similar to the following screen.

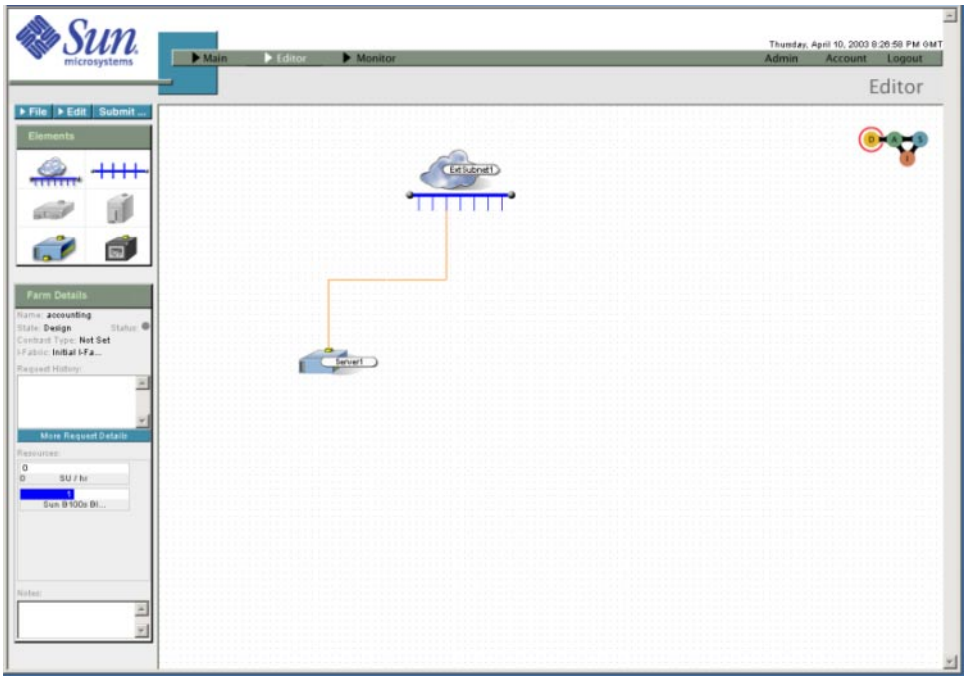

FIGURE 6–1 Initial Create I-Fabric Screen

16. **Double-click the Server Group element.**

    The Configure Server window on the screen is displayed.

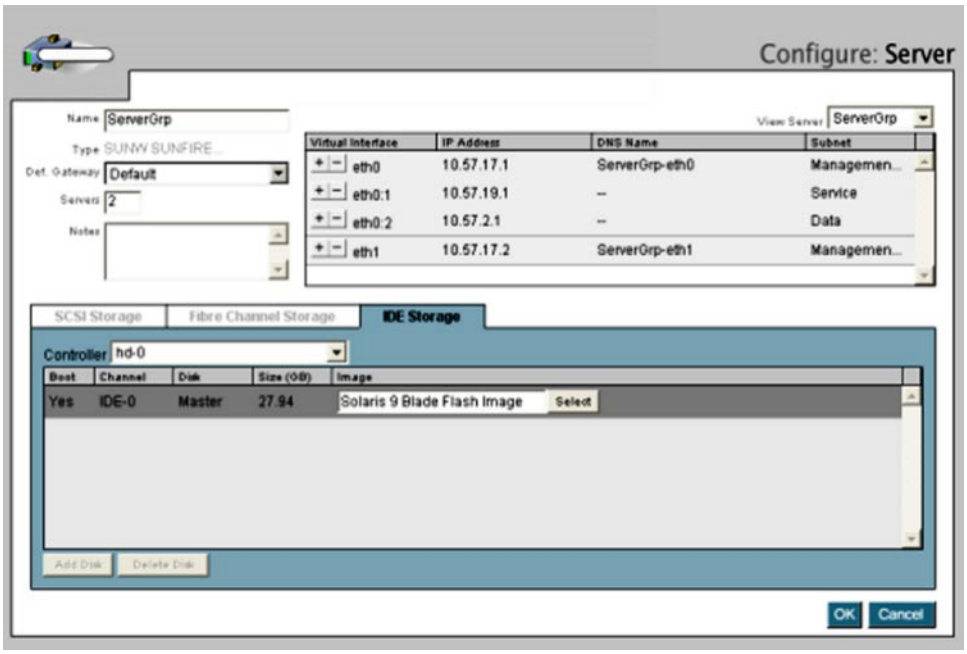

FIGURE 6–2 Configure Server Window

17. **Click Select an Image.**

    The Select Disk Image dialog is displayed. The name of the Disk Image is already highlighted.

18. **Click OK to select this disk image.**

    The Configure Server window is displayed with the name of the Disk Image displayed in the Image field.

19. **Click OK to select the Disk Image.**

20. **In the upper left of the Editor screen, click the Submit button.**

    The Farm Activation dialog box is displayed.

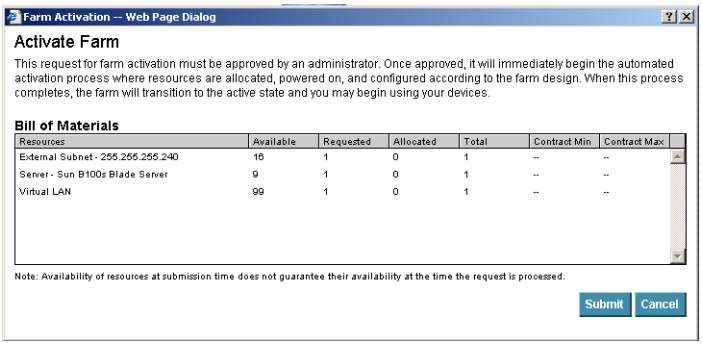

FIGURE 6–3 Control Center Farm Activation Dialog Box

21. Click the Submit button.

The Control Center Main screen is displayed.

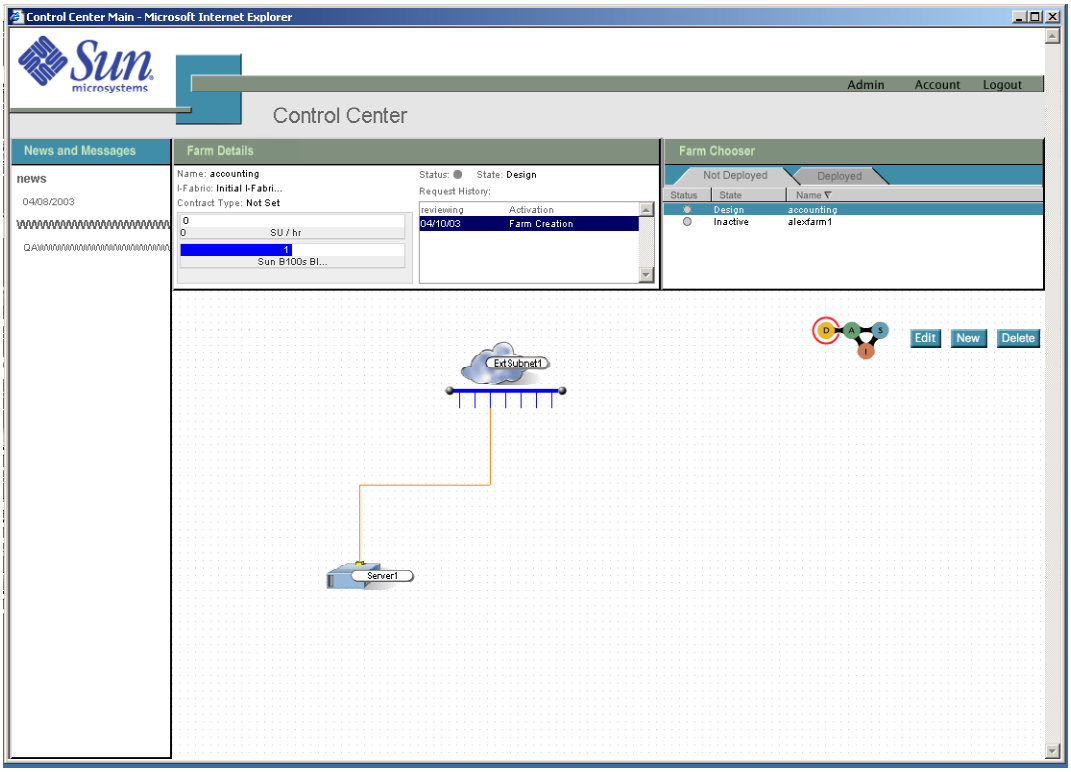

FIGURE 6–4 Control Center Main Screen

22. Click the Admin link at the upper right of the screen.

The Administration screen is displayed.

23. **Under Farm Management Tools on the left of the Administration screen, click the Pending Requests button**

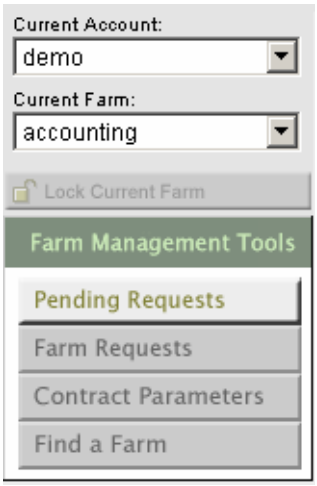

FIGURE 6–5 Select Pending Requests Button

The Pending Request screen displays.

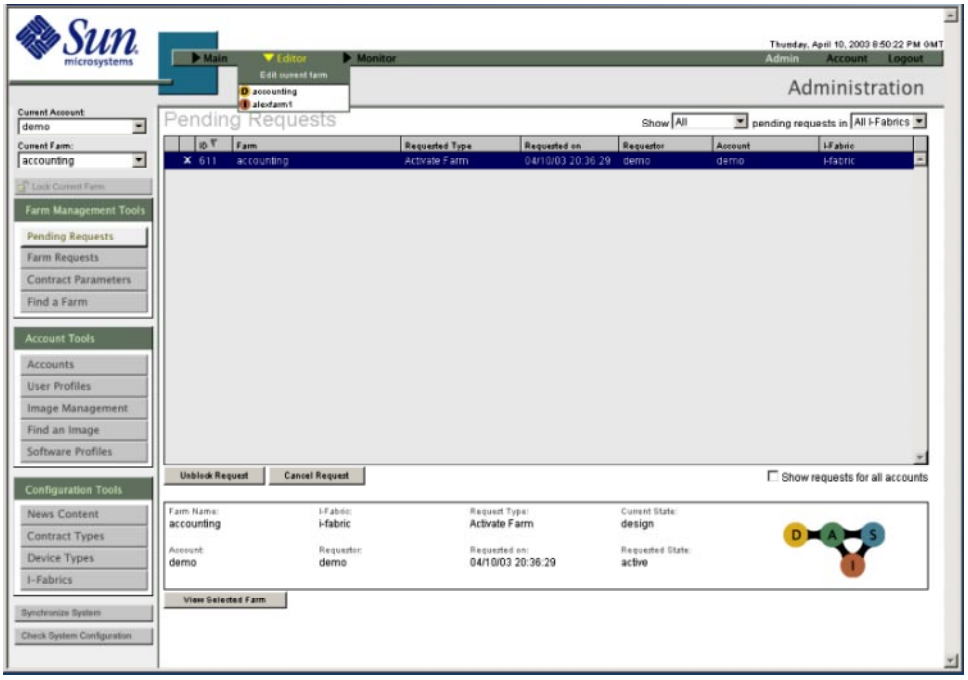

FIGURE 6–6 Pending Request Screen

24. **Click Unblock Request to initiate farm activation.**

    A confirmation dialog box is displayed.

25. **Click OK.**

26. **Under Farm Management Tools on the left of the Administration screen, click the Farm Requests button.**

    The Farm Requests screen is displayed.

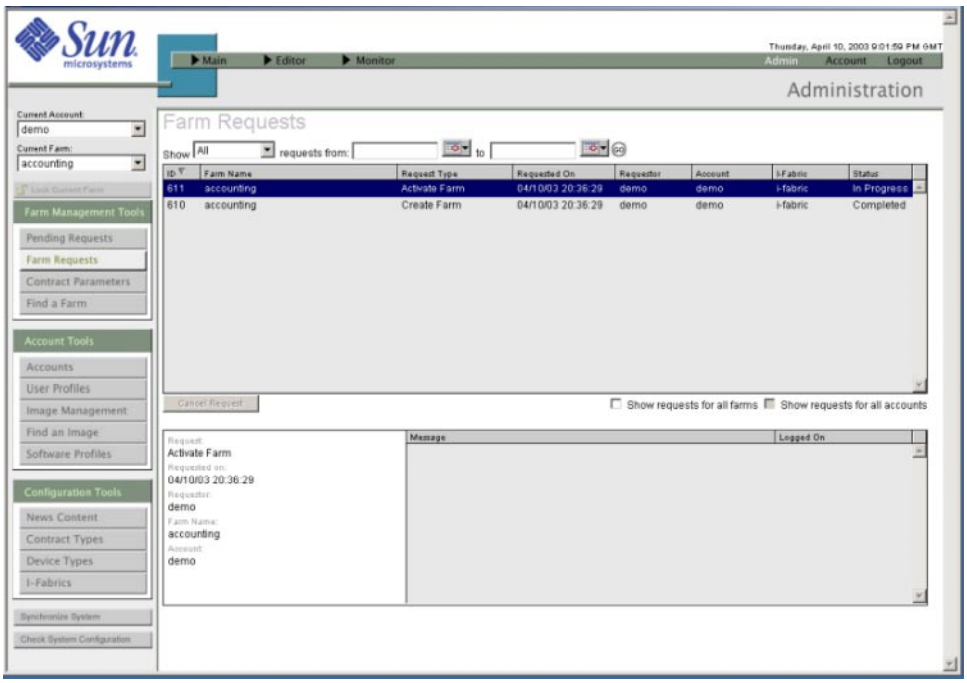

FIGURE 6–7 Farm Requests Screen

27. **Monitor the message panel in the lower right corner.**

    It might take up to an hour before you see the status field show Completed as illustrated in the following figure.

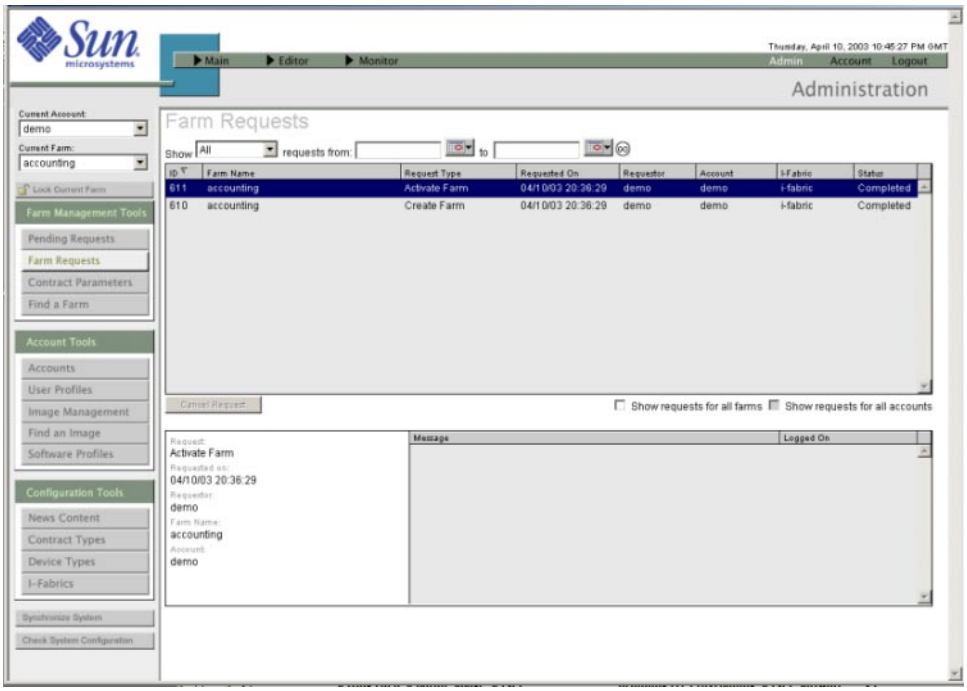

FIGURE 6–8 Farm Request Completed Screen

- If no failed messages appear in the message panel, the successful activation of this simple farm validates the N1 Provisioning Server Installation. You can now create your server blade farms. Follow the instructions in Chapter 4, "Building, Updating, and Monitoring Server Farms" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*.
- If you see failed messages in the message panel, you need to correct the problem and resubmit the farm by returning to step 14. See Chapter 6, "Troubleshooting" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide* for information on troubleshooting problems.

See Also "How To Import a Farm" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*

"How To Design a New Farm" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*

"How To Download Sample Farms" in *N1 Provisioning Server 3.1, Blades Edition, Control Center Management Guide*

Migrating From Oracle to PostgreSQL

You must upgrade from N1 Provisioning Server, Blades Edition version 3.0 to version 3.1 before you can migrate your N1 Provisioning Server 3.0 database data from Oracle to PostgreSQL (Postgres).

▼ To Migrate N1 Provisioning Server 3.0 Data from Oracle to Postgres

Steps

1. **Log in as root (`su - root`) on the control plane server.**
2. **Verify that the database administration group exists by typing `grep dba /etc/group`.**
   - If the `dba` group exits, the response `dba::100:` is displayed. Go to the next step.
   - If the `dba` group does not exist, only the prompt is displayed. Type **`groupadd dba`** to create the database administration group.
3. **Type `useradd -g dba postgres` to add the Postgres user account.**
4. **Change the database port.**
   a. **Log onto the control center as `administrator` using a Control Center management PC.**
      The Control Center main screen is displayed.
   b. **Click Admin in the menu bar.**
      The Administration Screen is displayed.
   c. **Click I-Fabric in the Configuration Tools panel.**
      The I-Fabrics screen is displayed.
   d. **Replace the displayed port number with the Postgres port number `5432`.**
   e. **Click Commit Changes.**
   f. **Click Logout to log out of the Control Center.**
5. **Type `/opt/terraspring/sunone/bin/appserv stop` to stop the control center application server.**
6. **Back up the control plane database.**

Type the command `/opt/terraspring/sbin/backupdb -o ${Oracle_Home}` *backup_file*

where *backup_file* is the name you have chosen for the backup file.

7. **Back up the Control Center database by typing `/opt/terraspring/gwdb/bin/backupDB.sh`.**

   The Control Center database is backed up to the file `/var/opt/terraspring/gwdb/backup/tsprgwdb.backup`.

8. **Update the database properties file to point to the Postgres database and port.**

Note – The following single-line examples have been split across two lines for display purposes.

---

   a. **In the file `/etc/opt/terraspring/tspr.properties`, change the following `DBConnection` text string.**

      ```
      com.terraspring.core.sys.GridOS.DBConnection=
              com.terraspring.db.oracle.OracleCpdbConnection
      ```

      to

      ```
      com.terraspring.core.sys.GridOS.DBConnection=
              com.terraspring.db.postgres.PostgresCpdbConnection
      ```

   b. **Change to port number in the `CpdbConnection` text string from `1521` to `5432`.**

      ```
      com.terraspring.db.CpdbConnection.port=1521
      ```

      For example:

      ```
      com.terraspring.db.CpdbConnection.port=5432
      ```

   c. **Save and close the file.**

9. **Install the Postgres database.**

   a. **Insert the N1 Provisioning Server 3.1 Installation DVD-ROM in the control plane server DVD-ROM drive.**

   b. **Install the Postgres package by typing `pkgadd -d /cdrom/cdrom0/Products/SUNWn1pg.pkg`**

10. **Create the Postgres database.**

    Type the command **`/opt/terraspring/lib/postgres/createdb -i -H localhost -o /opt/postgres -n tsprdb -f`** *postgres_data postgres_log*
    where *postgres_data* is the full path of the directory in which the database is created, and *postgres_log* is the full path name of the directory in which the database logs are saved.

11. Restore the control plane database data to Postgres.

Type the command `/opt/terraspring/sbin/restoredb` *restore_file*

where *restore_file* is the name of the control plane database backup file you created in Step 6.

12. Configure the database by typing `/opt/terraspring/gwdb/bin/configure.sh`.

You are prompted for configuration information. The following list shows the prompts and the required responses. Responses are case-sensitive and must be typed exactly as shown with no leading and no trailing spaces unless otherwise noted.

- DB_TYPE: **`Postgres`**
- DB Admin User: **`postgres`**
- DB Admin Password: **`postgres`**
- DB User: **`tcc`**
- DB User Password: **`tcc`**
- DB Host Name: **`localhost`**
- DB Instance Name: **`tsprdb`**
- DB Instance Listening Port: **`5432`**
- DB Backup Directory [/var/opt/terraspring/gwdb/backup]:

  Press Enter.
- DB Backup Filename [tsprgwdb.backup]:

  Press Enter.

13. Initialize the Postgres database by typing `/opt/terraspring/gwdb/bin/createDB.sh -y`.

14. Restore the database Web configuration information by typing `/opt/terraspring/gwdb/bin/restoreDB.sh`.

The following messages appear:

```
WARNING: That will destroy the current Control Center database.
Do you want to continue anyway(y/n)? [n]:
```

Type **`y`** to continue.

15. Reconfigure the Control Center for Postgres.

a. Change the database type and port.

In the file `/var/opt/terraspring/gw/gw.sunone.state`, change the following text string

```
DB_TYPE=Oracle
```

to

```
DB_TYPE=Postgres
```

Change the following text string

```
DB_PORT=1521
```

to

```
DB_PORT=5432
```

b. Save and close the file.

16. Stop and reconfigure the Control Center application server by typing `/opt/terraspring/sunone/bin/setup7.sh -silent`.

The `setup7.sh` script stops and then reconfigures the Control Center (CC) application server using the files you have updated in the previous steps.

17. Type the following commands in sequence to stop and restart the monitoring manager:

```
/opt/terraspring/sbin/snmpd stop
/opt/terraspring/sbin/snmpd start
```

18. Type the following commands in sequence to stop and restart the segment manager.

```
/etc/rc3.d/S97sm stop
/etc/rc3.d/S97sm start
```

19. Type the following commands in sequence to stop and restart the monitoring manager:

```
/opt/terraspring/sbin/mmd stop
/opt/terraspring/sbin/mmd start
```

20. Restart the CC application server by typing `/opt/terraspring/sunone/bin/appserv start`

CHAPTER 7

Uninstalling N1 Provisioning Server, Blades Edition Software

This chapter provides the procedure for uninstalling N1 Provisioning Server software.

Uninstalling N1 Provisioning Server Software

You might need to uninstall N1 Provisioning Server software in the following situations:

- When you encounter an installation problem and you need to begin the installation again. You can uninstall an incorrect installation or a partial installation where a problem has occurred.
- If you want to uninstall your current version.

You can uninstall the software on an I-Fabric that contains live server farms. However, if you have pending farm modification requests, you are prompted to confirm if you want to proceed with the uninstall process.

Farm modification requests include the following actions:

- Moving a server farm to standby
- Snapshot
- Synchronizing DHCP
- Activation
- Update
- Deactivation
- Failover

Caution – If you proceed, all farm modification requests are terminated and all associated data is lost, including all information about active farms.

▼ To Uninstall the N1 Provisioning Server Before the Installation or Upgrade Completes

Before You Begin

To prevent new farm modification requests from being submitted while you are uninstalling N1 Provisioning Server, make certain all N1 Provisioning Server users are logged off before uninstalling N1 Provisioning Server software.

Steps

1. **Login as root (`su – root`) on the control plane server.**
   - If you are uninstalling N1 Provisioning Server, Blades Edition version 3.0, insert the N1 Provisioning Server 3.0 Update 1 CD-ROM 1 of 2 into the DVD/CD-ROM drive.
   - If you are uninstalling N1 Provisioning Server, Blades Edition version 3.1, insert the N1 Provisioning Server 3.1 DVD-ROM into the DVD/CD-ROM drive.
2. **Type `/cdrom/cdrom/uninstall_PS` to start the uninstall process.**
   The following message is displayed.

   ```
   Do you want to uninstall the N1 software [y/n]?
   ```

3. **Type `y` to uninstall the N1 Provisioning software.**
   The following messages are displayed.

   ```
   Beginning uninstall process...
   Checking for pending requests in progress ...done!

   Stopping all Provisioning Server services ...done!
   ```

   - If the installation or upgrade process was not near completion when it exited, the following message might be displayed:

     ```
     Do you want to revert blades to factory settings [y/n]?
     ```

     Type **`y`** to revert to factory settings or type **`n`** to retain the current settings.

     – If you type **`y`** to revert the server blades to the factory setting, the message `Unconfiguring hardware...done!` is displayed.

     – If you type **`n`** , the server blades are not reverted to factory settings, and the message is not displayed.

     The following messages are then displayed:

```
Stopping database...done!

Removing N1 PS software packages...done!


Restoring system state...done!

Please check the following files to restore any changes made by N1 PS
software:

/etc/nsswitch.conf
/etc/resolv.conf
/etc/defaultdomain
/etc/system
/etc/dfs/dfstab
/etc/inetd.conf

Unconfiguring Network Interface cards....done!
Deleting FTP account...done!


Deleting additional files/directories used by PS/IS software...
Do you want to delete the images directory - '/images' [y/n]?
```

Go to Step 5.

- If the installation or upgrade process was near completion when it exited, the following messages might be displayed.

```
You may retrieve the pre-PS-install version of the following files
from /var/tmp/SystemState_before_PS_install.tar If the archive does
not contain some file, it implies that the file was created during
PS software installation.

/etc/nsswitch.conf
/etc/resolv.conf
/etc/defaultdomain
/etc/system
/etc/dfs/dfstab
/etc/inetd.conf

Unconfiguring Network Interface cards....done!
Deleting FTP account...done!


Deleting additional files/directories used by PS/IS software...
Do you want to delete the images directory - '/images' [y/n]?
```

4. **Type `y` to delete the `/images` directory containing the Solaris operating system image and disk snapshots. Type `n` to retain the directory.**

   The following messages are displayed.

```
The following files/directories will be deleted.
/etc/opt/terraspring
/etc/opt/ipf
```

```
/etc/named.conf
/opt/terraspring
/var/opt/terraspring
/tftpboot/terraspring
/etc/rc3.d/S60tsprdb
```

- If your Infrastructure Database is Oracle, the following messages are displayed:

  ```
  /oracle_data1
  /oracle_data2
  /oracle_data3
  ```

- If your Infrastructure Database is Postgres, the following messages are displayed:

  ```
  /postgres_data
  /postgres_log
  ```

You are prompted to confirm deletion of the files:

```
Is it okay to delete[y/n]? y
```

5. **Type `y` to delete the listed directories or type `n` to retain the listed directories.**

   If you type `n`, the following message is displayed.

   ```
   WARNING:You may have to manually delete the PS/IS
   related directories/files before reinstalling the software.
   ```

   Uninstall then finishes and the following messages are displayed.

   ```
   done!


   PS/IS logs are backed up in /var/tmp/N1PS_backup directory.
   ```

▼ To Uninstall the N1 Provisioning Server After the Installation or Upgrade Completes

Steps

1. **Login as root (`su – root`) on the control plane server.**

2. **Type `/opt/terraspring/sbin/uninstall_PS`**

   The following message is displayed.

   ```
   Do you want to uninstall the N1 software [y/n]?
   ```

3. **Type `y` to uninstall the Provisioning Server software.**

   The following messages are displayed.

   ```
   Beginning uninstall process...
   Checking for pending requests in progress ...done!

   Stopping all Provisioning Server services ...done!
   ```

```
Do you want to revert blades to factory settings [y/n]?
```

4. **Type `y` to revert to factory settings or `n` to retain the current settings.**
   - If you type **`y`** to revert the server blades to the factory setting, the message `Unconfiguring hardware...done!` is displayed.
   - If you type **`n`** , the server blades are not reverted to factory settings, and the message is not displayed.

   The following messages are displayed.

```
Stopping database...done!

Removing N1 PS software packages...done!


Restoring system state...done!

You may retrieve the pre-PS-install version of the following files
from /var/tmp/SystemState_before_PS_install.tar If the archive does
not contain some file, it implies that the file was created during
PS software installation.

/etc/nsswitch.conf
/etc/resolv.conf
/etc/defaultdomain
/etc/system
/etc/inetd.conf
/kernel/drv/skge.conf

Unconfiguring Network Interface cards....
```

5. **If interface devices are configured, you are prompted to authorize the removal of these interface devices. For example:**

```
Is it okay to unplumb interface skge1000 [y/n]
```

6. **If you are uninstalling an PS/IS combined server and ftp was selected as the image server protocol, the following message is displayed.**

```
Deleting FTP account...done!
```

   The following messages are then displayed.

```
Deleting additional files/directories used by PS/IS software...
Do you want to delete the images directory - '/images' [y/n]?
```

7. **Type `y` to delete the `/images` directory containing the Solaris Operating System image and disk snapshots. Type `n` to retain the directory.**

   The following messages are displayed.

```
The following files/directories will be deleted.
/etc/opt/terraspring
/etc/opt/ipf
/etc/named.conf
```

```
/opt/terraspring
/var/opt/terraspring
/tftpboot/terraspring
/var/tmp/n1_install_lock
/etc/rc3.d/S60tsprdb
/oracle_data1
/oracle_data2
/oracle_data3
Is it okay to delete[y/n]? y
```

8. **Type `y` to delete the listed directories or `n` to retain the listed directories.**

   If you type **`n`** to retain the listed directories, the following message is displayed.

   ```
   WARNING:You may have to manually delete the PS/IS
   related directories/files before reinstalling the software.
   ```

   Uninstall then finishes and the following messages are displayed.

   ```
   PS/IS logs are backed up in /var/tmp/N1PS_backup directory.

   Please delete the following empty directory - /opt/terraspring

   done!
   ```

APPENDIX **A**

Installation Main Menu Description

This appendix provides a summary about the following N1 Provisioning Install menu items.

```
N1 Provisioning Server Install Main Menu

  1.  IP Address of external DNS server to forward unknown queries:
  2.  Image Copy Subnet:
  3.  Number of Sun Blades to be managed:
  4.  Database software: Postgres
      4.1.   Infrastructure Database parameters ->
      4.2.   Control Center Application Server and Database parameters ->
  5.  Datacenter DNS Domain Name for this N1 Provisioning Server:
  6.  Resource Layer VLANs: <list>
  7.  Resource Layer Subnets:
  8.  Sun Blade System Chassis Information for discovery ->
  9.  Flash snapshot permission:
 10.  Directory where images will be stored:
```

1. IP Address of external DNS server to forward unknown queries:

If you need this function, then enter the IP Address of the external DNS Server to which unknown DNS queries are forwarded. Otherwise, press Enter if you do not require queries to be forwarded.

2. Image Copy Subnet:

This is the subnet in which resource layer servers will be configured during disk copy operations. The Image Subnet resides on a Secure VLAN (image VLAN) and enables a secure copy operation.

3. Number of Sun Blades to be managed:

Total number of server blades. Add the number of server blades installed in each B1600 Blade System Chassis.

Note – If the image server does not contain adequate disk space for the listed number of server blades, a message similar to the following message appears.

```
Space needed: 68000 MB, Space available: 16567 MB. You may not
have enough space to support future snapshot images for all your
blades. Do you wish to continue anyway? [y/N] y
```

4. Database software: Postgres

This menu selection enables you to specify which database software you want to use: Postgres, the default, or Oracle. If you choose Postgres, the Postgres database is installed for you during the N1 Provisioning Server installation process. If you choose Oracle, you must install the Oracle database before you install the N1 Provisioning Server software as described by "Installing the N1 Provisioning Server Database" on page 70.

4.1 Infrastructure Database parameters ->

This menu enables you to enter information relating to the Infrastructure Database. This information includes the directories where the database will be created and the directory where the database software is installed.

- If you chose Oracle as your database, the following menu items appear.

  1. **The directory where Oracle is installed:**

     The directory where Oracle has been installed on this machine, for example `/opt/oracle/OraHome1`. Database creation will fail if the correct information is not provided for this item.

  2. **Database Data Directory:** `/oracle_data1`

     The directory where the infrastructure database data files are created. You can create this directory and mount secondary disks, external disks, or NFS file systems onto this directory if you want. This directory is created by the install program if the directory does not exist. `/oracle_data1` is a sample directory name supplied by default. You can change this value.

  3. **Database Log Directory 1:** `/oracle_data2`

     The directory where the infrastructure database primary log files are created. You can create this directory and mount secondary disks/external disks/NFS file systems onto this directory if you want. This directory will be created by the install program if the directory does not exist. `/oracle_data2` is a sample directory name supplied by default. You can change this value.

  4. **Database Log Directory 2:** `/oracle_data3`

     The directory where the infrastructure database primary log files are created. You can create this directory and mount secondary disks/external disks/NFS file systems onto this directory if you want. This directory will be created by the install program if the directory does not exist. `/oracle_data2` is a sample

directory name supplied by default. You can change this value.

Note – The Oracle data and log directories must be empty or installation will fail.

- If you chose Postgres as your database, the following menu items appear.

  1. Database Data Directory:

     The directory where the Postgres database is to be installed on this machine, for example `/postgres_data`. Database creation will fail if the correct information is not provided for this item.

  2. Database Log Directory 1:

     The directory where the infrastructure database primary log files are created. You can create this directory and mount secondary disks/external disks/NFS file systems onto this directory if you want. This directory will be created by the install program if the directory does not exist. `/postgres_log` is a sample directory name supplied by default. You can change this value.

4.2 Control Center Application Server and Database parameters ->

This menu enables you to enter information related to the control center application server and the database. Information includes administrator user and password, database user and password, and mail notification details.

1. Admin Server user name:

This name is the name of the user account who is going to manage the Sun ONE Application Server.

2. Admin Server password:

This password is the password for the Sun One administration user account. The password must be at least 8 characters in length.

– If you chose Oracle as your database, the following menu items are displayed.

3. Oracle database administrator user:

This is the database administrator user name that is used to administer and maintain the control center database.

4. Oracle database administrator password:

This is the password for the database administrator user account. The password must be at least 8 characters in length.

5. Oracle database user:

This user name is the user name that is used to create and access the control center database.

6. Oracle database password:

This is the password for the control center database user account. The password must be at least 8 characters in length.

– If you chose Postgres as your database, the following menu items are displayed.

3. Database user:

This user name is the user name that is used to create and access the control center database.

4. Database password:

This is the password for the control center database user account. The password must be at least 8 characters in length.

The last item in the Control Center Application Server and Database parameters menu is **Enable Email Notification: no**. In the Oracle submenu, this is item 7. In the Postgres submenu, this is item 5.

This parameter is used to decide whether email notifications will be sent by the control center. The default is set to `no`.

If you choose yes, the following Mail Notification menu items are displayed, where *x* is 7 if you have chosen Oracle as your database, and 5 if you have chosen Postgres as your database.

x.1 **Mail From:**

This email address is the email address from which the email notifications will be sent.

x.2 **Mail To:**

This email address is the email address to which the email notifications will be sent.

x.3 **SMTP host name:**

This host name is the SMTP host name from which the email notifications will be sent.

5. Datacenter DNS domain name for this N1 Provisioning Server:

This name is the Fully Qualified DNS domain name that is assigned to this Provisioning Server.

6. Resource Layer VLANs:

This list is the list of resource layer VLANS that will be added in the infrastructure database. VLANs for farms will be allocated from this list. Each item in the list must be a range of numbers. For example, '11-15' is a valid entry for this list.

Note – Resource layer VLANS 1, 2, 4, 8, and 9 are already used by N1 Provisioning Server software. 10 is the minimum value allowed. 255 is the maximum value allowed.

By default, this list is set to 10-255.

7. Resource Layer Subnets:

This list is the list of resource layer subnets that will be added to the database. Subnets for farms will be allocated from this list. Each item in the list must be a subnet address followed by an 'i' or 'e' to indicate if this address is an internal subnet address or external subnet address. For example '10.10.0.0/24/i' and '220.240.255.0/24/e' are valid entries for this list.

The exact subnets that you enter depend on you site's particular network configuration.

Internal subnets are used to create IP address namespaces for I-Fabric N1 Provisioning Servers which do not require network connectivity outside the corporate network by using an external router such as the Internet. Internal subnets are defined based on internal corporate IT conventions to prevent namespace collisions between various private subnets. You need to check with your administrator to determine what internal subnet addresses are available for use with your I-Fabric. Then, enter these subnets as internal subnets during installation.

Note – Internal subnet is required. Any subnet that is entered in this list must not be the same as the Image copy subnet.

External subnets are typically assigned by an outside entity to a corporate IT network when cpu devices require connectivity outside the corporate network such as the Internet. If your I-Fabric is connected to an external router, and you want the cpu devices in a farm to access the Internet, you need to ask your administrator what external subnet address are available for your I-Fabric. Then, enter the subnet as external subnets during installation.

8. Blade System Chassis Information for discovery ->

This menu requests information about the Blade System Chassis in your I-Fabric. The Blade System Chassis System Controller and Switches must be configured in your I-Fabric network. The Blade System Chassis System Controller and Switches must be accessible from this provisioning server machine by using telnet. The user name and password must be configured to be the same for all Blade System Chassis System Controllers and Switches.

The following menu items are displayed when you choose `8. Blade System Chassis Information for discovery`.

1. **Blade System Chassis IP Addresses and Switch Network Configuration:**

   These addresses are the IP Addresses for all the Blade System Chassis in your I-Fabric. Each IP Address must be accessible from this machine to be considered valid. You will also need to provide the network configuration data for the switches on each Blade System Chassis. The install program will use this data to configure the switches in each Blade System Chassis.

   Blade System Chassis IP Addresses and Switch Network Configuration

```
sc_ip            switch_ip        default_gw       netmask
-------------------------------------------------------------
<empty list>     <empty list>     <empty list>     <empty list>
```

These addresses are the IP Addresses of the Blade System Chassis in your I-Fabric. Each Blade System Chassis SC IP Address must be accompanied by network configuration data for the switch on that Blade System Chassis. The install program uses the Blade System Chassis SC IP Address to connect to the Blade System Chassis. The install program uses the remaining information for configuring the switch on that Blade System Chassis.

Note – The install program will destroy any existing configuration and replace the configuration with the supplied information.

```
Choose an operation to perform on the list.
a - add item                 d - delete item
i - insert item                x - exit
[a|d|i|x]
```

2. **Blade System Chassis switch and system controller (SSC) user login and password:**

   This name is the user name that is used by telnet and SNMP to access the blade system chassis SSCs.

Caution – All blade system chassis SSCs must have the same user name and password to access, else installation will fail.

Note – The install program will destroy any existing configuration and replace the configuration with the supplied information.

---

3. **Blade System Chassis switch and system controller Password:**

Caution – All blade system chassis SSCs must have the same user name and password to access, else installation will fail.

This is the password that is be used by telnet and SNMP to access the blade system chassis SSCs.

Note – The install program will destroy any existing configuration and replace the configuration with the supplied information.

9. Flash snapshot permission:

This menu item is used to choose whether to enable or disable flash snapshot permission for operating system images.

10. Directory where images will be stored:

This is the directory in which operating system images are stored. The default is `/images`.

If you intend to use a filesystem other than `/images`, you must mount the filesystem on `/images` on the image server machine, and make the `/images` available over the network using network file system (NFS) mounting. The filesystem must have at least 6 gigabytes of free space,

APPENDIX **B**

N1 Provisioning Server Packages

This appendix provides a list of the N1 Provisioning Server, Blades Edition packages and descriptions.

Package Name	Description
SUNWn1pg	Sun Microsystems Postgres Database
TSPRaglnx	Sun Microsystems Infrastructure Agent for Linux
	Note – TSPRaglnx is a Linux RPM and not a package.
TSPRagsol	Sun Microsystems Infrastructure Agent for Solaris
	Note – The TSPRagsol package is installed on the Solaris master image supplied with the software. All other packages are installed on the control plane server unless otherwise noted.
TSPRbli	Sun Microsystems core Boot Loader Images components
TSPRblibs	Terraspring Boot Loader Images for Sun SPARC blades architecture
TSPRblibx	Terraspring Boot Loader Images for x86 sun blades architecture
TSPRcore	Sun Microsystems core control plane components.
TSPRcs	Sun Microsystems compute services.
TSPRdb	Sun Microsystems Infrastructure database components.
TSPRdhcp	Sun Microsystems dhcp daemon from ISC.
TSPRdns	Sun Microsystems dns daemon from ISC.
TSPRdrvrs	Sun Microsystems device driver components.
TSPRgm	Sun Microsystems Global Manager
TSPRgw	Sun Microsystems N1 Virtualization Control Center - Sun ONE Version

Package Name	Description
TSPRgwcom	Sun Microsystems N1 Virtualization Control Center Common Components
TSPRgwdb	Sun Microsystems N1 Virtualization Control Center Database Components
TSPRhal	Sun Microsystems hardware abstraction layer components.
TSPRipf	Sun Microsystems IP Filter
TSPRmlg	Sun Microsystems Infrastructure logging package
TSPRmon	Sun Microsystems Infrastructure monitoring
TSPRnetcf	Sun Microsystems network configuration components.
TSPRpdc	Sun Microsystems N1 Virtualization Pseudo Data Center
TSPRrel	Sun Microsystems Infrastructure release info tools
TSPRstmc	Sun Microsystems Storage Manager Client
TSPRsuna	Sun Microsystems N1 Virtualization App Server - 3.1.2
TSPRtools	Sun Microsystems Infrastructure support tools

Glossary

account — A method of controlling access to the Control Center and server farms. An account may have *user* or *account manager* login roles assigned to it.

account image — Account images are assigned to specific accounts or farms and are managed by users. Account images consist of user-specific customizations of global images, and application and data images. See also *global image*.

account manager — An account manager has all the Control Center access privileges of a *user* and can edit account information including creation and removal of other users in the account. See also *user* and *administrator*.

administrator — An administrator has the highest level of Control Center access privileges and operates an overall I-Fabric.

agent — See *N1 Provisioning Server agent*.

automated provisioning — The capability of building unique, complex, and secure computing environments in near real time without manual intervention. Automated provisioning includes powering up and configuring resource pool servers, and configuring load balancers and network topologies.

backhaul — See *unmanaged devices*.

blades — Individual server blades located in the chassis. See also *server blades*.

blade system chassis — Also known as the Sun Fire Blade Platform or the Sun Fire B1600 Intelligent Shelf. Individual server blades are located in the chassis. See also *chassis*.

chassis — Also known as the Sun Fire Blade Platform or the Sun Fire B1600 Intelligent Shelf. Individual server blades are located in the chassis. See also *blade system chassis*.

chassis switch	An Ethernet switch that is part of the switch and system controller (SSC) unit. The chassis switch controls access to server blades. See also *system controller*.
chargeable events	Events that occur within the N1 Provisioning Server environment for which you can bill customers.
Control Center (CC)	Control Center software
Control Center database	The Control Center database.
Control Center Management PC	The PC used to access the Control Center graphical user interface (GUI).
Control Center GUI	The Control Center graphical user interface.
Control Center dialog box	Used in the Control Center to denote a dialog. There are four types of dialogs: ■ Standard dialog. The user may leave that dialog open while opening another one. ■ Modal dialog. The user must provide a response before being able to click outside this dialog. ■ Alert dialog. A message generated by the software for the user's benefit. ■ Confirmation dialog. The user may choose to click OK or Cancel.
control plane (CP)	All N1 Provisioning Server software and hardware, 3rd-party software and hardware, and the Oracle or Postgres database, but not resource pool servers and fabric layer.
control plane database (CPDB)	The Control Plane database.
control plane server (CP server)	Server hardware that hosts the N1 Provisioning Server software.
control plane switch	Network switch and fabric that manages the transfer of instructions, such as commands, from the Control Planer server to other I-Fabric components. See also *fabric layer*.
data plane	Network hardware, such as switches, used for transferring data within an I-Fabric. See also *fabric layer*.
Data plane switch	Manages the data transfer, such as images, within an I-Fabric. See also *fabric layer*
data VLAN	VLAN on which the virtual IPs reside.
disk size	The size of the resource pool server disk onto which to copy a global or account image.
deployable image	An image in the image repository that has been validated for deployment to a resource pool server.

device identification number (DEVID) A unique identifier assigned to a piece of equipment in an I-Fabric.

disk controller type The disk controller type used for the disk, such as IDE or SCSI. This information is used when working with the `image` command.

fabric layer The fabric layer consists of networking fabrics and switches within and I-Fabric that are controlled and managed by the control plane.

failover The process of automatically switching to a redundant or standby server, system, or network upon failure or abnormal termination of the currently active server, system, or network.

farm A collection of resource pool servers that are assigned to a particular account. See also *server farm* and *logical server farm*.

farm elements Graphical representations of I-Fabric components in the Control Center GUI.

Farm Export Markup Language An XML-based language that is used to import and export logical server farms.

farm life cycle A farm life cycle includes the design, provisioning, use, and eventual return of a device to the resource pool. These life cycle events are tracked in the Control Center or on the command line by various farm states. The following list shows example of possible farm states:

- Design. A new farm has been created, but not yet submitted.
- Pending. The user has submitted a farm for approval and activation.
- Active. The farm has been activated and is running.
- Standby. All farm elements are in the process of being returned to the resource pool.
- Inactive. The farm is inactive and all hardware resources are returned to the resource pool.

farm manager A process that monitors and manages activities related to server farms.

Farm Markup Language (FML) An XML-based language that is used to provide a logical description of a farm.

farm state A farm life cycle is defined by various states. A farm's state is displayed graphically in the State Diagram icon in the Control Center GUI. See also *farm life cycle*.

FEML See *Farm Export Markup Language*.

Flexing Making any kind of change to an active server farm. Changes can include the following:

- Editing the configuration
- Adding new elements

- Resizing a server or server group
- Adding or deleting a server or server group

FML	See *Farm Markup Language*.
global image	An image that consists of the operating system (including patches and service packs), integrated N1 Provisioning Server agents, and certain customizations. A global image is considered the master image and may be duplicated for use in other resource pool servers within an I-Fabric. Global images may also include applications.
Hardware Abstraction Layer (HAL)	An application programming interface (API) to a hardware device.
image	An archive of operating system, N1 Provisioning Server agent software, and optional application software and data combinations. See also *deployable image* and *non-deployable image*.
image architecture	The architecture type of an image. N1 Provisioning Server supports two architectures: Sun SPARC and x86.
image archive type	The archive type of an image. N1 Provisioning Server supports three image archive types: disk, flash, and JumpStart.
image attributes	Meta information about a specific image, such as image name, image ID, image configuration file, and image description.
image operating system (image OS)	The operating system on which an image is based.
image repository	A collection of images within the N1 Provisioning Server environment.
image server	Software or hardware (if the image server runs on a separate host) on which the image repository resides.
image size	The size of the image to be copied onto a resource pool server. The image size must always be less than the disk size. See also *disk size.*
image type	N1 Provisioning Server supports two types of images: global images and account images. See also *global images* and *account images*.
image wizard	A command-line user interface within the N1 Provisioning Server used for creating, upgrading, listing, importing, updating, and deleting images.
Infrastructure Fabric (I-Fabric)	All components of the control plane, the resource pool, and the fabric layer.
life cycle	See *farm life cycle.*
lockout	Users are locked out of the Control Center access if their login attempts fail a configurable number of times within a configurable number of minutes.

logical server farm A collection of resource pool servers that are assigned to a particular farm or account. See also *server farm* and *farm*.

load balancer A server blade that performs load balancing tasks within a server farm. Also referred to as a *load balancing blade*.

management VLAN VLAN on which resource pool servers are load balanced.

messaging A message routing framework provided by the N1 Provisioning Server software for directing farm- and monitoring-related messages to a central repository on the CPDB or to an external NMS. Three types of messages are generated:

- Informational messages
- Farm messages
- Billing messages

message repository A collection of messages within an N1 Provisioning Server environment. The monitoring manager forwards messages to the message repository.

MML See *Monitoring Markup Language*.

Monitoring Markup Language (MML) An XML-based language that is used to provide a logical description of the monitoring parameters of any logical server farm.

monitoring manager A process that monitors the health and performance of devices in the control plane.

N1 Provisioning Server All product software and hardware, including the Control Center and Control Plane software and hardware.

N1 Provisioning Server agent A process that performs device interface configurations within an I-Fabric.

network virtualization A concept that allows for the creation of a digital map of the physical I-Fabric network using XML-based markup languages. See also *FML, FEML, MML, and WML*.

non-deployable image An image in the image repository that has not been validated for deployment to a resource pool server.

power controller A network device that provides and manages power for the servers in the resource pool.

preconfigured image An operating system image with basic configurations and software packages that is included in the N1 Provisioning Server software package.

provisioning The ability to add or delete capacity on a logical server farm using the N1 Provisioning Server software.

queuing mechanism Processes all farm-related requests, such as farm activation and update.

resource pool	A supply of unused devices that are available for provisioning to server farms.
resource pool server	A hardware server in the resource pool.
resource virtualization	A concept that allows for the creation of a digital map of the physical resources within an I-Fabric using XML-based markup languages. See also *FML, FEML, MML, and WML*.
scrubbing	The process of overwriting a memory device with 1s or 0s so that the data formerly stored on the device cannot be recovered. Resource pool servers are scrubbed by N1 Provisioning Server software before they are returned to the resource pool.
segment manager	A process that controls and coordinates activities for an I-Fabric.
server blades	Refers to the individual servers blades located in the chassis. See also *Blades*.
server farm	A collection of resource pool servers that are assigned to a particular farm or account. See also *farm* and *logical server farm*.
server group	A unique logical structure that enables rapid flexing of multiple servers by associating a predefined role or image for all servers within a group.
service unit	A way to abstract any individual device to enable a utility-like computing service.
service VLAN	The VLAN on which traffic flows from the load balancer to the resource pool server.
snapshot	An image of the contents of a disk.
SSC	See *switch and system controller.*
state	The condition of a server or server farm in terms of its variable attributes, configuration, or content. See also *farm life cycle*.
storage manager client (STMC)	The interface required by the farm manager for accessing storage functionality.
Sun Fire Blade Platform	Also known as the Sun Fire B1600 Intelligent Shelf. See also *chassis*.
switch and system controller (SSC)	A component of the chassis that comprises the chassis switch and the system controller. The chassis switch controls access to server blades. The system controller monitors the operational status of all devices in the chassis and provides a command-line interface (CLI) to the chassis configuration software. See also *chassis switch* and *system controller*.
system controller	An interface that is part of the switch and system controller (SSC) unit. The system controller monitors the operational status of all devices in the chassis and provides a command-line interface (CLI) to the chassis configuration software. See also *chassis switch*.

terminal server	A network device that provides a serial connection to servers in the resource pool.
unmanaged devices	Ethernet-capable devices that are not officially supported by the N1 Provisioning Server software, but that are visible to other Ethernet devices within an I-Fabric. Such devices can include routers and network-attached storage (NAS) devices.
user	Lowest account login level at the Control Center GUI.
user groups	A Control Center feature that allows for grouping users for automatic messaging.
Wiring Markup Language (WML)	An XML-based language that is used to provide a logical description of the physical wiring and configuration of an I-Fabric.
WML	See *Wiring Markup Language*.

Index

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

V

W