Chapter 8 Managing Appliance Operations

Managing the operations of a NIOS appliance involves defining system parameters such as time, security, and port settings. It also includes configuring operations such as scheduling tasks, defining approval workflows, managing licenses, managing extensible attributes, and configuring access control for supported operations.

The tasks covered in this chapter include:

- **5800278**
  - Administrative Permissions
  - Operations that Support Access Control
  - Defining Named ACLs
  - Managing Named ACLs
  - Applying Access Control to Operations
- **Managing Time Settings**
  - Changing Time and Date Settings
  - Changing Time Zone Settings
  - Monitoring Time Services
- **Using NTP for Time Settings**
  - Authenticating NTP
  - NIOS Appliances as NTP Clients
  - Configuring the Grid to Use NTP
  - Configuring Grid Members to Use NTP
  - NIOS Appliances as NTP Servers
  - Configuring a NIOS Appliance as an NTP Server
  - Monitoring NTP
- **About Extensible Attributes**
  - Adding Extensible Attributes
  - Configuring Inheritable Extensible Attributes
  - Using Extensible Attributes
  - Viewing Extensible Attributes
  - Modifying Extensible Attributes
  - Deleting Extensible Attributes
  - Configuration Examples for Inheritable Extensible Attributes
- **Managing Security Operations**
  - Restricting Remote Console Access
  - Restricting GUI/API Access
  - Enabling HTTP Redirection
  - Modifying the Session Timeout Setting
  - Disabling the LCD Input Buttons
  - Configuring Security Features
  - Enabling and Disabling Remote Console and Infoblox Technical Support Access
- **Configuring Proxy Servers**
- **Configuring Members and Interfaces for Automatic Updates**
- **Configuring Ethernet Ports**
  - Enabling GUI and API Access on the MGMT and LAN1/VIP Ports
  - About Virtual LANs
  - Implementing Quality of Service Using DSCP
  - Ethernet Port Usage
  - Modifying Ethernet Port Settings
  - Using the LAN2 Port
  - About Port Redundancy
  - Configuring the LAN2 Port
  - Enabling DHCP on LAN2
  - Enabling DNS on LAN2
- **Using the MGMT Port**
  - Appliance Management
  - Grid Communications
  - DNS Services
- **About Lights Out Management**
  - Enabling LOM
  - Adding LOM User Accounts
  - Configuring the IPMI Network Interface
  - Modifying LOM Settings
  - Viewing LOM Users
  - IPMI Commands and Examples
- **Setting Static Routes**
- **Enabling DNS Resolution**
- **Managing Licenses**
  - License Types
  - Managing Static Licenses
  - Managing Dynamic Licenses
  - Managing Grid-wide Licenses
  - Adding Permanent or Subscription Licenses
  - Adding Temporary Licenses
  - Viewing Licenses
  - Backing Up Licenses
  - Removing Licenses
- **About IB-FLEX**
Configuring Access Control

To effectively manage your core network services, you can grant legitimate hosts access to specific tasks and operations using an access control list (ACL) or anonymous access control entries (ACEs). Depending on your admin permissions, you can configure a named ACL, and then apply it to multiple operations, such as file distribution and DNS zone transfers. For information about admin permissions, see About Administrative Permissions.

When you define a named ACL, you add access control types such as IPv4 and IPv6 addresses, IPv4 and IPv6 networks, nested named ACLs, and TSIG key based ACEs to a list, and then grant each entry in the list the Allow or Deny permission. For information about named ACLs and how to configure them, see Defining Named ACLs. Note that each operation supports specific access control types. You cannot apply a named ACL to an operation that does not support the access control types contained in the named ACL. For more information about which NIOS operations support access control and which access control types each operation supports, see Operations that Support Access Control.

When you add or modify a named ACL, or when you import named ACLs and ACEs to an existing named ACL through CSV import, the appliance does not automatically validate the ACEs in the list. For more information about how to import named ACLs and ACEs, refer to the Infoblox CSV Import Reference.

To avoid conflicts and unexpected results, you must perform validations for all named ACLs before you use them for access control. When the appliance detects a conflict or an optimized issue about a specific ACE during the validation process, it displays detailed information in a CSV file. For more information about ACL validation, see Validating Named ACLs.