Managing Resource Records

DNS resource records provide information about objects and hosts. DNS servers use these records to respond to queries for hosts and objects. The appliance supports IDNs for all DNS resource records. For information about IDNs, see Support for Internationalized Domain Names. Note that the appliance does not decode the IDN of a resource record to punycode. In other words, a record that contains a domain name in punycode is displayed in punycode and a record that contains an IDN is displayed in its native characters.

You can manage the following types of DNS resource records:

- **A (IPv4 Address)**—For information, see Managing A Records.
- **NS (Name server)**—For information, see Managing NS Records.
- **AAAA (IPv6 Address)**—For information, see Managing AAAA Records.
- **PTR (Pointer)**—For information, see Managing PTR Records.
- **MX (Mail exchanger)**—For information, see Managing MX Records.
- **SRV (Service location)**—For information, see Managing SRV Records.
- **TXT (Text)**—For information, see Managing TXT Records.
- **TLSA (Transport Layer Security)**—For information, see Managing TLSA Records.
- **CNAME (Canonical name)**—For information, see Managing CNAME Records.
- **DNAME**—For information, see Managing DNAME Records.

Managing A Records

An A (address) record is a DNS resource record that maps a domain name to an IPv4 address. To define a specific name-to-address mapping, you can add an A record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the A record is in the corpxyz.com zone, which is associated with 10.1.0.0/16 network, then the IP addresses of the A record must belong to the 10.1.0.0/16 network. For information about associating zones and networks, see Associating Networks with Zones.

The appliance also supports wildcard A records. For example, you can use a wildcard A record in the corpxyz.com domain to map queries for names such as www1.corpxyz.com, ftp.corpxyz.com, main.corpxyz.com, and so on to the IP address of a public-facing web server. Note that wildcard names only apply when the domain name being queried does not match any resource record.

NIOS allows superusers to add A records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record to add A records with a blank name. You can assign global permission for specific admin groups and roles to allow limited-access users to add blank A records. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

Note: If an A record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Name field displays the record name in UTF-8 encoded format. For example, an A record with the domain name .test.com added through DDNS updates displays "229:183:165:228:189:156:231:171:153.test.com in the Name field.

Adding A Records

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add A Record.
2. In the Add A Record wizard, do the following:
   - **Name**: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the host record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com. Ensure that the domain name you enter complies with the hostname restriction policy defined for the zone. To create a wildcard A record, enter an asterisk (*) in this field.
   - **DNS View**: This field displays the DNS view to which the DNS zone belongs.
   - **Shared Record Group**: This field appears only when you are creating a shared record. Click Select Shared Record Group. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the Shared Record Group Selector dialog box. You can use filters or the Go to function to narrow down the list.
   - **Hostname Policy**: Displays the hostname policy of the zone.
   - In the IP addresses section, click the Add icon and do one of the following:
     - Select Add Address to enter the IPv4 address to which you want the domain name to map. or
     - Select Next Available IPv4 to retrieve the next available IP address in a network.
   - If the A record is in zone that has associated networks, the Network Selector dialog box lists the associated networks. If the zone has no network associations, the Network Selector dialog box lists the available networks. When you select a network, Grid Manager retrieves the next available IP address in that network.
   - **Comment**: Optionally, enter additional information about the A record.
   - **Create associated PTR record**: Select this option to automatically generate a PTR record that maps the specified IPv4 address to the hostname. To create the PTR record, the reverse-mapping zone must be in the database.
   - **Disable**: Select this check box to disable the record. Clear the check box to enable it.
3. Click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Save the configuration and click Restart if it appears at the top of the screen.

Modifying A Records

When you modify an A record, you can do the following:
• In the **General** tab, you can change the information you previously entered through the wizard, as described in Adding A Records.

• The **Discovered Data** tab displays discovered data, if any, for the record. For information, see Viewing Discovered Data.

You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

### Managing NS Records

An NS record identifies an authoritative DNS server for a domain. Each authoritative DNS server must have an NS record. Grid Manager automatically creates NS records when you assign a Grid member as the primary server for a zone or when you assign an NS group to a zone. Grid Manager generates two NS records; an authoritative NS record for the current zone; and a delegation NS record for the parent zone for each name server available in the NS group. You cannot edit an automatically generated NS record. Note that when you delete a name server from an NS group, the NS record associated with the name server is deleted. For information about using NS Groups, see Importing Zone Data. You can manually create NS records for other zones. NS records associated with one or more IP addresses are used for related A record and PTR record generation. You can configure an NS record for anycast IP addresses on the appliance. For more information about anycast, see About Anycast Addressing for DNS.

### Adding NS Records

To add an NS record:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add NS Record**.
2. In the **Add NS Record** wizard, complete the following fields:
   - **Zone**: The displayed zone name can either be the last selected zone or the zone from which you are adding the NS record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**.
   - **DNS View**: Displays the DNS view to which the selected zone belongs.
   - **Name Server**: Enter the host name that you want to configure as the name server for the zone. IDN is not supported in this field. You can use the punycode representation of an IDN in this field.
3. Click **Next** to enter IP addresses for the name server.
4. In the **Name Server Addresses** panel, click the Add icon and complete the following fields:
   - **Address**: Enter the IP address of the name server.
   - **Add PTR Record**: This field displays Yes by default, enabling the automatic generation of a PTR record for the IP address. You can select **No** to disable the generation of the PTR record.
5. Click **Next** to define extensible attributes, or save the configuration and click **Restart** if it appears at the top of the screen.

### Modifying and Deleting NS Records

When you modify an NS record, you can change the following information:

- In the **General** tab, you can change the name server name.
- In the **Addresses** tab, you can do the following:
  - Delete an address by selecting it and clicking the Delete icon.
  - Add an address by clicking the Add icon, and then entering the IP address and completing the **Add PTR Record** field.

### Managing AAAA Records

An AAAA (quad A address) record maps a domain name to an IPv6 address. To define a specific name-to-address mapping, add an AAAA record to a previously defined authoritative forward-mapping zone. If the zone is associated with one or more networks, the IP address must belong to one of the associated networks. For example, if the AAAA record is in the corpxyz.com zone, which is associated with the 1111:0001/32 network, then the IP addresses of the A record must belong to that network. For information about associating zones and networks, see Associating Networks with Zones.

**Note:** If an AAAA record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Name** field displays the record name in UTF-8 encoded format. For example, an AAAA record with the domain name .test.com added through DDNS updates displays `229.183.165.228;189.156.231;171.153.test.com` in the **Name** field.

NIOS allows superusers to add AAAA records with a blank name. Limited-access users must have read/write permission to Adding a blank A/AAAA record to add AAAA records with a blank name. You can assign global permission for specific admin groups and roles to allow limited-access users to add blank AAAA records. For more information, see Administrative Permissions for Adding Blank A or AAAA Records.

### Adding AAAA Records

To create an AAAA record:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add AAAA Record**.
2. In the **Add AAAA Record** wizard, complete the following:
• **Name**: If Grid Manager displays a zone name, enter the hostname that you want to map to an IP address. The displayed zone name can either be the last selected zone or the zone from which you are adding the AAAA record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the hostname. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the host. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com.
• **DNS View**: Displays the DNS view to which the selected DNS zone belongs.
• **Shared Record Group**: This field appears only when you are creating a shared record. Click **Select Shared Record Group**. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the Go to function to narrow down the list.
• **Hostname Policy**: Displays the hostname policy of the zone.
• **IP Address**: Enter the IPv6 address to which you want the domain name to map. When you enter an IPv6 address, you can use double colons to compress a contiguous sequence of zeros. You can also omit any leading zeros in a four-hexadecimal group. For example, the complete IPv6 address 2006:0000:0000:123:4567:89ab:0000:cdef can be shortened to 2006::123:4567:89ab::cdef. Note that if there are multiple noncontiguous groups of zeros, the double colon can only be used for one group to avoid ambiguity. The NIOS appliance displays an IPv6 address in its shorted form, regardless of its form when it was entered.
• **Comment**: Optionally, enter additional information about this record.
• **Create associated PTR record**: Select this option to automatically generate a PTR record that maps the specified IP address to the hostname. To create the PTR record, the reverse-mapping zone must be in the database.
• **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Click **Next** to define extensible attributes. For information, see **Using Extensible Attributes**.
4. Save the configuration and click **Restart** if it appears at the top of the screen.

### Modifying AAAA Records

When you modify an AAAA record, you can do the following:

- In the **General** tab, you can change the information you previously entered through the wizard.
- In the **Discovered Data** tab, you can view discovered data, if any, for the record. For information, see **Viewing Discovered Data**.

You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see **Modifying, Disabling, and Deleting Host and Resource Records**.

### Managing PTR Records

In a reverse-mapping zone, a PTR (pointer) record maps an IP address to a hostname. Before adding a PTR record to a reverse-mapping zone, you must first create the zone. You can also add PTR records to forward-mapping zones to support zeroconf (zero configuration networking), such as wide-area Bonjour. For information about the Bonjour protocol, refer to [http://www.apple.com/support/bonjour](http://www.apple.com/support/bonjour). Though adding PTR records to forward-mapping zones supports some of the use cases in RFC 1101, it does not support the network name mapping use case described in the RFC. For more information, refer to [http://tools.ietf.org/html/rfc1101](http://tools.ietf.org/html/rfc1101).

**Note**: If a PTR record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Name** and **Domain Name** fields display the record name in UTF-8 encoded format. For example, a PTR record with the domain name .test.com added through DDNS updates displays `/229\183\165\228\189\156\231\171\153.test.com in the Name and Domain Name fields.

### Adding PTR Records

To add a PTR record:

1. From the **Data Management** tab, select the DNS tab, expand the Toolbar and click **Add -> Record -> Add PTR Record**.
2. In the Add PTR Record wizard, do the following:
   - **Name or IP Address**: From the drop-down list, select Name or IP Address. When you select Name, click **Select Zone** to select a zone, and then enter a value for the PTR record. When you are adding a PTR record to a reverse-mapping zone, you can enter a value from 0 to 255 in the **Name or IP Address** field. Note that when you launch this wizard from the IPAM tab, you can only select a reverse-mapping zone. When you launch this from a reverse-mapping zone, the IP address field is populated with the prefix that corresponds to the selected zone. When you launch this from a forward-mapping zone, you can only specify the host name, not an IP address.
   - When you select IP Address, enter the IPv4 or IPv6 address that you want to map to the domain name.
   - **DNS View**: If you entered an IPv6 address, select the DNS view of the PTR record. If you entered a name, this field displays the DNS view of the selected zone.
   - **Domain Name**: Enter the domain name to which you want the PTR record to point. For example, you can enter corpxyz.com.
   - **Comment**: Optionally, enter information about the PTR record.
   - **Disable**: Select this check box to disable the record. Clear the check box to enable it.
3. Save the configuration, or click **Next** to define extensible attributes. For information, see **Using Extensible Attributes**.
4. Click **Restart** if it appears at the top of the screen.

To schedule this task, click the Schedule icon at the top of the wizard. In the Schedule Change panel, click **Later**, and then specify a date, time, and time zone.

**Note**: When you add a PTR record to a forward-mapping zone, a message may appear on the top of the wizard if a Grid member is configured to ignore DNS queries for PTR records in forward-mapping zones. Contact Infoblox Technical Support for more information about this message.
Modifying PTR Records

Do the following to modify a PTR record:

- In the **General** tab, you can change the information you previously entered through the wizard. Note that you cannot change an IPv4 address to an IPv6 address or move a PTR record from a forward-mapping zone to a reverse-mapping zone and vice versa. When you modify a PTR record that belongs to a forward-mapping zone, you can only modify the name since there is no IP address for such record. For information, see Adding PTR Records.
- In the **Discovered Data** tab, you can view discovered data, if any, for the record. For information, see Viewing Discovered Data.

You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing MX Records

An MX (mail exchanger) record maps a domain name to a mail exchanger. A mail exchanger is a server that either delivers or forwards mail. You can specify one or more mail exchangers for a zone, as well as the preference for using each mail exchanger. A standard MX record applies to a particular domain or subdomain.

You can use a wildcard MX record to forward mail to one mail exchanger. For example, you can use a wildcard MX record in the corpxyz.com domain to forward mail for eng.corpxyz.com and sales.corpxyz.com to the same mail exchange, as long as the domain names do not have any matching resource record. Wildcards only apply when the domain name being queried does not match any record.

**Note:** If an MX record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Mail Destination** and **Mail Exchanger** fields display the record name in UTF-8 encoded format. For example, an MX record with the domain name .test.com added through DDNS updates displays \229\183\165\228\189\156\231\171\153.test.com in the **Mail Destination** and **Mail Exchanger** fields.

See Figure 20.1.

**Figure 20.1 MX Records**

The following MX records ... ... direct queries for one or more domains ... ... to the same mail exchanger:

An MX record for the mail exchanger that answers queries for just the corpxyz.com domain (and its corresponding A record):

corpxyz.com IN MX 0 mail1.corpxyz.com
mail1.corpxyz.com IN A 10.2.2.10

An MX record for just site1.corpxyz.com, a subdomain of corpxyz.com:
site1.corpxyz.com IN MX 0 mail1.corpxyz.com
mail1.corpxyz.com

A wildcard MX record for the corpxyz.com domain:

*.corpxyz.com IN MX 0 mail1.corpxyz.com

**Note:** You must also create an A record for the host defined as a mail exchanger in an MX record.

Adding MX Records

To add an MX record from the Tasks Dashboard, see Add MX Record. You can also add MX records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add MX Record from the Toolbar.

Modifying and Deleting MX Records
When you modify an MX record, you can change the information you previously entered in the **General** tab. You can also enter or edit information in the **TTL**, **Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see *Modifying, Disabling, and Deleting Host and Resource Records*.

## Managing SRV Records

An SRV (service location) record directs queries to hosts that provide specific services. For example, if you have an FTP server, then you might create an SRV record that specifies the host which provides the service. You can specify more than one SRV record for a host. For more information about SRV records, see [RFC 2052: A DNS RR for specifying the location of services (DNS SRV)].

**Note:** If an SRV record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Name** and **SRV Target** fields display the domain name in UTF-8 encoded format. For example, an SRV record with the domain name .test.com added through DDNS updates displays 231/148/181/232/132:145.test.com in the **Name** and **SRV Target** fields.

## Adding SRV Records

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add SRV Record**.
2. In the **Add SRV Record** wizard, complete the following fields:
   - **Display input as**: Select the format in which you want the SRV record to be displayed. When you select RFC 2782 format, the appliance follows the _service_._protocol._name format as defined in RFC 2782. When you select Free format, enter the entire name in the Domain field.
   - **Service**: Specify the service that the host provides. You can either select a service from the list or type in a service, if it is not on the list. For example, if you are creating a record for a host that provides FTP service, select _ftp_. To distinguish the service name labels from the domain name, the service name is prefixed with an underscore. If the name of the service is defined at [http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml](http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml), use that name. Otherwise, you can use a locally-defined name.
   - **Protocol**: Specify the protocol that the host uses. You can either select a protocol from the list or type in a protocol, if it is not on the list. For example, if it uses TCP, select _tcp_. To distinguish the protocol name labels from the domain name, the protocol name is prefixed with an underscore.
   - **Domain**: If Grid Manager displays a zone name, enter the name here to define an SRV record for a host or subdomain. The displayed zone name can either be the last selected zone or the zone from which you are adding the SRV record. If no zone name is displayed or if you want to specify a different zone, click **Select Zone**. When there are multiple zones, Grid Manager displays the **Zone Selector** dialog box. Click a zone name in the dialog box, and then enter the name to define the SRV record. The NIOS appliance prefixes the name you enter to the domain name of the selected zone. For example, if you want to create an SRV record for a web server whose host name is www2.corpxyz.com and you define the SRV record in the corpxyz.com zone, enter www2 in this field. To define an SRV record for a domain whose name matches the selected zone, leave this field blank. The NIOS appliance automatically adds the domain name (the same as the zone name) to the SRV record. For example, if you want to create an SRV record for the corpxyz.com domain and you selected the corpxyz.com zone, leave this field blank.
   - **Preview**: After you have entered all the information, this field displays the FQDN, which is the concatenation of the Service, Protocol, and Domain fields.
   - **Shared Record Group**: This field appears only when you are creating a shared record. Click **Select Shared Record Group**. If you have only one shared record group, the appliance displays the name of the shared record group here. If you have multiple shared record groups, select the shared record group in the **Shared Record Group Selector** dialog box. You can use filters or the **Go** function to narrow down the list.
   - **Priority**: Select or enter an integer from 0 to 65535. The priority determines the order in which a client attempts to contact the target host; the domain name host with the lowest number has the highest priority and is queried first. Target hosts with the same priority are attempted in the order defined in the **Weight** field.
   - **Weight**: Select or enter an integer from 0 to 65535. The weight allows you to distribute the load between target hosts. The higher the number, the more that host handles the load (compared to other target hosts). Larger weights give a target host a proportionately higher probability of being selected.
   - **Port**: Specify the appropriate port number for the service running on the target host. You can use standard or nonstandard port numbers, depending on the requirements of your network. You can select a port number from the list or enter an integer from 0 to 65535.
   - **Target**: Enter the canonical domain name of the host (not an alias); for example, www2.corpxyz.com

   **Note:** In addition, you need to define an A record mapping the canonical name of the host to its IP address.

   - **Comment**: Enter a descriptive comment for the record.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.

3. Save the configuration, or click **Next** to define extensible attributes. For information, see *Using Extensible Attributes*.
4. Click **Restart** if it appears at the top of the screen.

## Modifying and Deleting SRV Records

Do the following to modify an SRV record:

- In the **General** tab, the **Display input as** field displays the format in which the SRV record was configured. For RFC 2782 format, the appliance matches the _service_._protocol._name_ format and displays the corresponding information in the Service and Protocol fields. If the appliance cannot match the service and protocol, it displays the entire name in the Domain field. For Free format, the entire name is displayed in the Domain field. For more information about the other fields, see *Adding SRV Records*. 

Note: The appliance does not match the service and protocol names to exactly how they appear in the drop-down lists. It only checks whether the first two parts of the names start with an underscore. If the first two parts do not start with an underscore, the appliance assumes it is a free format. For example, _abc._xyz.name is considered as RFC 2782 format even though _abc is not in the Service drop-down list, and _xyz is not in the Protocol drop-down list. Grid Manager displays _abc in the Service field and _xyz in the Protocol field. On the other hand, “abc.xzy.name” is considered as a free format because the first two parts do not start with underscores, and Grid Manager displays this in its entirety in the Domain field.

You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing TXT Records

A TXT (text record) record contains supplemental information for a host. For example, if you have a sales server that serves only North America, you can create a text record stating this fact. You can create more than one text record for a domain name.

Note: If a TXT record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Name field displays the domain name in UTF-8 encoded format. For example, a TXT record with the domain name .test.com added through DDNS updates displays ‘2311:1481:132:132:151:13:5:141:15451:145.test.com in the Name field.

Using TXT Records for SPF

SPF (Sender Policy Framework) is an anti-forgery mechanism designed to identify spam e-mail. SPF fights e-mail address forgery and makes it easier to identify spam, worms, and viruses. Domain owners identify sending mail servers in DNS. SMTP receivers verify the envelope sender address against this information, and can distinguish legitimate mail from spam before any message data is transmitted. SPF makes it easy for a domain to say, “I only send mail from these machines. If any other machine claims that I'm sending mail from there, they’re not valid.” For example, when an AOL user sends mail to you, an email server that belongs to AOL connects to an email server that belongs to you. AOL uses SPF to publish the addresses of its email servers. When the message comes in, your email servers can tell if the server that sent the email belongs to AOL or not.

You can use TXT records to store SPF data that identifies what machines send mail from a domain. You can think of these specialized TXT records as reverse MX records that e-mail servers can use to verify if a machine is a legitimate sender of an e-mail.

SPF Record Examples

corpxyz.com. IN TXT "v=spf1 mx -all"  
corpxyz.net. IN TXT "v=spf1 a:corpxyz.com -all"  
corpxyz.com. IN TXT "v=spf1 include:corpxyz.com -all"  
corpxyz.net. IN TXT "v=spf1 mx -all exp=getlost.corpxyz.com"  
corpxyz.com. IN TXT "v=spf1 include:corpxyz.com -all"

Adding TXT Records

To add an TXT record from the Tasks Dashboard, see Add TXT Record. You can also add TXT records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add TXT Record from the Toolbar.

Modifying and Deleting TXT Records

When you modify a TXT record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

Managing TLSA Records

A TLSA record is used to associate a TLS (Transport Layer Security) server certificate or a public key with a domain name. For example, you can define whether a certificate or a public key must be associated with a domain name when you define a TLSA resource record through Grid Manager. When you define your own TLSA record, you do not have to depend on an external Certificate Authority to issue a digitally signed TLS certificate for your domain name. When a client queries the domain name, TLSA records are matched to authenticate associated TLS certificates.

Using TLSA Records for DANE

Infoblox supports DANE (DNS-based Authentication of Named Entities) protocol to secure information about domain names. DANE uses DNSSEC to sign certificates and keys that are used by the TLS and distributes secure information about the domain name using DNS. With DANE, you can make an authoritative binding between the domain name and a certificate or a public key, whichever is used by a host for the respective domain. You can define what kind of certificates or public keys must be associated with a domain name to prevent vulnerability attacks and to reduce or prevent the interaction of third party Certification Authorities to issue PKIX certificates. For detailed information about the TLSA record format and certificate usage, refer to RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA.

Note: You can add a TLSA record to a DNSSEC signed zone only. You cannot unsign a zone that contains a TLSA record.
Adding TLSA Records

To add a TLSA record:

1. From the *Data Management* tab, select the *DNS* tab, expand the Toolbar and click *Add -> Record -> TLSA Record*.
2. In the *Add TLSA Record wizard*, complete the following fields:
   - **Display input as:** Select either *Strict format (_port.*_protocol.*domain)* or *Free format*. Grid Manager selects *Strict format* by default. In this format, you can choose port and protocol values from the list. When you select *Free format*, you cannot specify these values.
   - **Port:** Select a value from the drop-down list to indicate the port on which the TLS-based service is active.
   - The values in the drop-down list are:
     - 21 (FTP)
     - 22 (SSH)
     - 23 (Telnet)
     - 25 (SMTP)
     - 80 (HTTP)
     - 88 (Kerberos)
     - 389 (LDAP)
     - 443 (HTTPS)
     - 464 (KPASSWD)
     - 3268 (GC)
   - **Protocol:** Select a value from the drop-down list to indicate the protocol that is used for secure communication. The values in the drop-down list are:
     - _msdcs
     - _sites
     - _tcp
     - _udp

   **Note:** When you select *Strict format*, *Port* and *Protocol* values are set to 443 (HTTPS) and _tcp, by default. You can change these values. When you select *Free format*, you cannot edit the mentioned values.

- **Name:** Enter a name for the TLSA resource record. You can specify a name only when you select *Free format*.
- **Select Zone:** Click to select a zone. You can only select signed zones to associate with a TLSA resource record. For more information, see *Signing a Zone*. Click *Clear* to clear the *Name* that you have entered.
- **FQDN:** This is displayed by default. You cannot modify the value. TLSA resource records are stored using the domain name that you select. When you select *Free format*, name.domain is displayed as the FQDN. Example: abc.example.com. When you select *Strict format* at _port._protocol.domain is displayed as the FQDN, where:
  - _port* indicates the port on which the TLS-based service is active.
- **protocol** indicates the name of the transport protocol that you have selected.

Consider an example where you are the owner of the domain www.example.com and you have set the *Port* to 443(HTTPS) and *Protocol* to _tcp, which indicates that the HTTP server is running TLS on port 443. To request TLSA record for [www.example.com](http://www.example.com), you must use _443._tcp. [www.example.com](http://www.example.com). Similarly, to request a TLSA resource record for an SMTP server running the STARTTLS protocol on port 25 at mail.example.com, you must use _25._tcp.mail.example.com.

- **DNS View:** The DNS View associated with the selected DNS zone is displayed.
- **Certificate Usage:** Select a value from the drop-down list to indicate how the certificate or the public key associated with the domain name is matched when the client queries for the domain name on the TLS server. The values in the drop-down list are: **PKIX-TA, PKIX-EE, DANE-TA, and DANE-EE**.
  - **With PKIX-TA and PKIX-EE,** you need additional Trust Anchors to validate peer certificate chains. These Trust Anchors must be mutually trusted by both the TLS server and the client. For more information, refer to *RFC 6898 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*.
  - **When you select DANE-TA and DANE-EE,** the TLSA records that you define using Grid Manager are sufficient to verify the client's certificate chain and additional Trust Anchors are not required to authenticate the public key or certificate data. For more information, refer to *RFC 6898 The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*.

- **Selector:** Select a value from the drop-down list to indicate whether you are associating an entire certificate or only the public key with the domain. When you select a value, it indicates which part of the TLS certificate presented by the server is matched with the associated data. The values in the drop-down list are: **Full certificate** and **Subject Public Key Info**. NIOS builds an hexadecimal format for the entire certificate when you select **Full certificate**. If you select **Subject Public Key Info**, NIOS extracts the public key and builds a hexadecimal format for it.

- **Matched Type:** Select a value from the drop-down list to indicate how a TLSA certificate or the public key of the domain received from the client must be matched with the certificate or the key that you have specified for the respective domain in the TLS server. You can select to match the entire content or only the hash of the selector. The values in the drop-down list are: **No hash**, **SHA 256 bit**, and **SHA 512 bit**. If you select **No hash**, the TLS server performs an exact match on the selected content. When you select either **SHA 256 bit** or **SHA 512 bit**, only the hash of the selected content is matched by the TLS server.

  - **Certificate Data:** Enter the certificate data that must be matched for authentication. You can either paste the full certificate or the corresponding public key when the **Matched Type** is set to **No hash**. Based on the values that you select for the *Selector* and the **Matched Type**, the server builds a hexadecimal format for the TLSA record. If you set the **Matched Type** to **SHA 256 bit** or **SHA 512 bit**, you must specify only the hash of the full certificate or the public key.

- **Get From File:** Click this to upload the certificate or the public key to the server.

  - **When you select **Strict format**, you must provide either the certificate or public key or hash of any of them. The value must be based on the *Selector* and **Matched Type** field values.
  - **When you select **Free format**, you must upload the certificate in DER format. The server builds an appropriate hexadecimal format for the TLSA record based on the *Selector* value.

- **Comment:** Optionally, enter a descriptive comment for the TLSA record.
- **Disable:** Clear the check box to enable the record. Select the check box to disable it.
**Note:** You cannot add TLSA resource records during a scheduled full upgrade from an earlier NIOS version to 8.0 and later. Grid Manager will not convert a TLSA resource record that is stored in `bind_resource_record` during an upgrade. You must do it manually after an upgrade.

You can also do the following:

- Use **Global Search** to search for TLSA records. For information, see [Global Search](#).
- Use **Copy Records** to copy TLSA records between DNS zones. For information, see [Copying Zone Records](#).
- Define global permission for **All TLSA records** with read-only, read/write or deny access. You can also define object level permission for TLSA records. For information, see [Defining Global Permissions](#) and [Defining Global Permissions](#).
- Import and export records in CSV format. For information, see [About CSV Import](#).
- View audit log entries for the TLSA record. For information, see [Viewing the Audit Log](#).

### Modifying and Deleting TLSA Records

When you modify a TLSA record, you can change the information you previously entered in the **General** tab. You can also enter or edit information in the **TL Extensible Attributes** and **Permissions** tabs. For information on modifying and deleting resource records, see [Modifying, Disabling, and Deleting Host and Resource Records](#).

### Managing CNAME Records

A CNAME record maps an alias to a canonical name. You can use CNAME records in both forward- and IPv4 reverse-mapping zones to serve two different purposes. (At this time, you cannot use CNAME records with IPv6 reverse-mapping zones.)

**Note:** If a CNAME record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the **Alias** and **Canonical Name** fields display the domain name in UTF-8 encoded format. For example, a CNAME record with the domain name `.test.com` added through DDNS updates displays `\x{231}`\x{148}`\x{181}`\x{232}`\x{132}`\x{145}.test.com` in the **Canonical Name** and **Alias** fields.

### CNAME Records in Forward-Mapping Zones

In a forward-mapping zone, a CNAME record maps an alias to a canonical (or official) name. CNAME records are often more convenient to use than canonical names because they can be shorter or more descriptive. For example, you can add a CNAME record that maps the alias `qa.engr` to the canonical name `qa.engr.corpxyz.com`.

**Note:** A CNAME record does not have to be in the same zone as the canonical name to which it maps. In addition, a CNAME record cannot have the same name as any other record in that zone.

To add a CNAME record to a forward-mapping zone from the Tasks Dashboard, see [Add CNAME Record](#). You can also add CNAME records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add CNAME Record from the Toolbar.

### CNAME Records in IPv4 Reverse-Mapping Zones
You can add CNAME records to an IPv4 reverse-mapping zone to create aliases to addresses maintained by a different name server when the reverse-mapping zone on the server is a delegated child zone with fewer than 256 addresses. This technique allows you to delegate responsibility for a reverse-mapping zone with an address space of fewer than 256 addresses to another authoritative name server. See RFC 2317, Classless IN-ADDR.ARPA delegation.

Figure 20.2 CNAME Records in a Reverse-Mapping Zone

You add CNAME records in the parent zone on your name server. The aliases defined in those CNAME records point to the addresses in PTR records in the child zone delegated to the other server.

When you define a reverse-mapping zone that has a netmask from /25 (255.255.255.128) to /31 (255.255.255.254), you must include an RFC 2317 prefix. This prefix can be anything, from the address range (examples: 0-127, 0/127) to descriptions (examples: first-network, customer1). On a NIOS appliance, creating such a reverse-mapping zone automatically generates all the necessary CNAME records. However, if you need to add them manually to a parent zone that has a child zone with fewer than 255 addresses.

You add CNAME records in the parent zone on your name server. The aliases defined in those CNAME records point to the addresses in PTR records in the child zone delegated to the other server.

When you define a reverse-mapping zone that has a netmask from /25 (255.255.255.128) to /31 (255.255.255.254), you must include an RFC 2317 prefix. This prefix can be anything, from the address range (examples: 0-127, 0/127) to descriptions (examples: first-network, customer1). On a NIOS appliance, creating such a reverse-mapping zone automatically generates all the necessary CNAME records. However, if you need to add them manually to a parent zone that has a child zone with fewer than 255 addresses.

Adding CNAME Records

To add a CNAME record to a forward-mapping or reverse-mapping zone from the Tasks Dashboard, see Add CNAME Record. You can also add CNAME records from the Data Management tab -> DNS tab by clicking Add -> Record -> Add CNAME Record from the Toolbar.

Modifying and Deleting CNAME Records

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.
Managing DNAME Records

A DNAME record maps all the names in one domain to those in another domain, essentially substituting one domain name suffix with the other (see RFC 2672, Non-Terminal DNS Name Redirection). For example, adding a DNAME record to the corpxyz.com domain mapping "corpxyz.com" to "corp200.com" maps name-x.corpxyz.com to name-x corp200.com.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Target Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1.corpxyz.com</td>
<td>server1.corp200.com</td>
</tr>
<tr>
<td>server2.corpxyz.com</td>
<td>server2.corp200.com</td>
</tr>
<tr>
<td>server3.corpxyz.com</td>
<td>server3.corp200.com</td>
</tr>
<tr>
<td>....corpxyz.com</td>
<td>....corp200.com</td>
</tr>
</tbody>
</table>

Note: If a DNAME record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Alias and Target fields display the domain name in UTF-8 encoded format. For example, a DNAME record with the domain name .test.com added through DDNS updates displays `\231\148\181\232\132\145.test.com` in the Alias and Target fields.

When a request arrives for a domain name to which a DNAME record applies, the NIOS appliance responds with a CNAME record that it dynamically creates based on the DNAME definition. For example, if there is a DNAME record

```
corpxyz.com          DNAME corp200.com
```

and a request arrives for server1.corpxyz.com, the NIOS appliance responds with the following CNAME record:

```
server1.corpxyz.com   CNAME server1.corp200.com
```

If responding to a name server running BIND 9.0.0 or later, the NIOS appliance also includes the DNAME record in its response, so that name server can also create its own CNAME records based on the cached DNAME definition.

The following are two common scenarios for using DNAME records:

- One company buys another and wants people using both the old and new name spaces to reach the same hosts.
- A virtual Web hosting operation offers different "vanity" domain names that point to the same server or servers.
- You cannot have a CNAME record and a DNAME record for the same subdomain.
- You cannot use a DNAME record for a domain or subdomain that contains any subdomains. You can only map the lowest level subdomains (those that do not have any subdomains below them). For an example of using DNAME records in a multi-tiered domain structure, see Figure 20.3.

Figure 20.3 Adding DNAME Records for the Lowest Level Subdomains
In the case of a domain structure consisting of a single domain (no subdomains), adding a DNAME record redirects queries for every name in the domain to the target domain, as shown in Figure 20.4.

Figure 20.4 Adding a DNAME Record for a Single Domain

Corp200 buys corp2xz and wants to redirect all queries for corp2xz.com to corp200.com. To accomplish this, you add a single DNAME record to corp2xz.com.

When using a DNAME record, you must copy the resource records for the source domain to the zone containing the target domain, so that the DNS server providing service for the target domain can respond to the redirected queries.

<table>
<thead>
<tr>
<th>Copy from corp2xz.com</th>
<th>to corp2xz.corp200.com</th>
</tr>
</thead>
<tbody>
<tr>
<td>www1 IN A 10.1.1.10</td>
<td>www1 IN A 10.1.1.10</td>
</tr>
<tr>
<td>www2 IN A 10.1.1.11</td>
<td>www2 IN A 10.1.1.11</td>
</tr>
<tr>
<td>ftp1 IN A 10.1.1.20</td>
<td>ftp1 IN A 10.1.1.20</td>
</tr>
<tr>
<td>mail1 IN A 10.1.1.30</td>
<td>mail1 IN A 10.1.1.30</td>
</tr>
</tbody>
</table>
After copying these records to the zone containing the `corpxyz.corp200.com` domain, delete them from the zone containing the `corpxyz.com` domain. If DNS service for the source and target domain names is on different name servers, you can import the zone data from the NIOS appliance hosting the source domain to the appliance hosting the target domain. For information about this procedure, see `Importing Zone Data`. If DNS service for the source and target domain names is on the same name server and the parent for the target domain is on a different server, you can delegate DNS services for the target domain name to the name server that provided—and continues to provide—DNS service for the source domain name (see `Figure 20.5`). By doing this, you can continue to maintain resource records on the same server, potentially simplifying the continuation of DNS administration.

*Figure 20.5 Making the Target Zone a Delegated Zone*

![Diagram of domain name mapping and delegation](image.png)

*Note:* This is a conceptual representation of domain name mapping and depicts the resulting hierarchical relationship of `corpxyz.corp200.com` as the parent zone for `corpxyz.corp200.com`. The hosts are not physically relocated.

The following tasks walk you through configuring the two appliances in `Figure 20.5` to redirect queries for `corpxyz.com` to `corpxyz.corp200.com` using a DNAME record:

2. Copy all the resource records for the domain or subdomain to which the DNAME record is going to apply from `corpxyz.com` to `corpxyz.corp200.com`. Because you can only specify the records by type, not individually, you might have to copy some records that you do not want and then delete them from the `corpxyz.corp200.com` zone.

*Note:* Because you can only specify the records by type, not individually, you might have to copy some records that you do not want and then delete them from the `corpxyz.corp200.com` zone.

3. In the `corpxyz.com` zone, delete all the resource records for the domain or subdomain to which the DNAME record is going to apply.
4. Add a DNAME record to the `corpxyz.com` zone specifying "`corpxyz.com`" as the domain and "`corpxyz.corp200.com`" as the target domain. Adding a DNAME record is explained in the next section.
5. On the `ns1.corp200.com` name server, add `corpxyz.corp200.com` as a delegated zone and specify `ns1.corpxyz.com` as the name server for it. See `Configuring a Delegation`.

**DNAME Records for Forward-Mapping Zones**

To add a DNAME record to a forward-mapping zone:

1. From the **Data Management** tab, select the **DNS** tab, expand the Toolbar and click **Add -> Record -> Add DNAME Record**.
2. In the **Add DNAME Record** wizard, complete the following fields:
DNAME Records for Reverse-Mapping Zones

You can use DNAME records to redirect reverse lookups from one reverse-mapping zone to another. You can use DNAME records for reverse-mapping zones to simplify the management of subzones for classless address spaces larger than a class C subnet (a subnet with a 24-bit netmask).

RFC 2672, *Non-Terminal DNS Name Direction*, includes an example showing the delegation of a subzone for an address space with a 22-bit netmask inside a zone for a larger space with a 16-bit netmask:

```
$ORIGIN 0.192.in-addr.arpa.
8/22 NS ns.slash-22-holder.example.
8 DNAME 8.8/22
9 DNAME 9.8/22
10 DNAME 10.8/22
11 DNAME 11.8/22
```

The reverse-mapping zone 0.192.in-addr.arpa. applies to the address space 192.0.0.0/16. Within this zone is a subzone and subdomain with the abbreviated name 8/22 (its full name is 8/22.0.192.in-addr.arpa). This subdomain contains its own subdomains corresponding to the 1024 addresses in the 192.0.8.0/22 subnet:

- Subdomain 8/22 (8/22.0.192.in-addr.arpa)
  - Subdomain 8.8/22 for addresses 192.0.8.0 – 192.0.8.255 (or 192.0.8.0/24)
  - Subdomain 9.8/22 for addresses 192.0.9.0 – 192.0.9.255 (or 192.0.9.0/24)
  - Subdomain 10.8/22 for addresses 192.0.10.0 – 192.0.10.255 (or 192.0.10.0/24)
  - Subdomain 11.8/22 for addresses 192.0.11.0 – 192.0.11.255 (or 192.0.11.0/24)

The NS record delegates authority for the reverse-mapping subzone 8/22 to the DNS server ns.slash-22-holder.example. Finally, the DNAME records provide aliases mapping domain names that correspond to the 192.0.8.0/24, 192.0.9.0/24, 192.0.10.0/24, and 192.0.11.0/24 subnets to the respective subdomains 8.8/22, 9.8/22, 10.8/22, and 11.8/22 in the 8/22.0.192.in-addr.arpa subzone.

**Note:** NIOS appliances support DNAME records in reverse-mapping zones that map addresses to target zones with a classless address space larger than a class C subnet. However, NIOS appliances do not support such target zones.

You might also use DNAME records if you have a number of multihomed appliances whose IP addresses must be mapped to a single set of domain names. An example of this is shown in *Figure 20.6: Figure 20.6 DNAME Records to Simplify DNS for Multihomed Appliances*
To add a DNAME record to a reverse-mapping zone:

1. From the Data Management tab, select the DNS tab, expand the Toolbar and click Add -> Record -> Add DNAME Record.
2. In the Add DNAME Record wizard, complete the following fields:

   - **Alias**: If Grid Manager displays a zone name, enter the name of a subdomain here. If you are adding a DNAME record for the entire zone, leave this field empty. This field is for adding a DNAME record for a subdomain within the selected zone. The displayed zone name can either be the last selected zone or the zone from which you are adding the DNAME record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Click a zone name in the dialog box, and then enter the name of a subdomain.
   - **Target**: Type the name of the reverse-mapping zone to which you want to map all the addresses specified in the Domain Name field.
   - **Comments**: Enter identifying text for this record, such as a meaningful note or reminder.
   - **Disable**: Clear the check box to enable the record. Select the check box to disable it.
3. Save the configuration, or click Next to define extensible attributes. For information, see Using Extensible Attributes.
4. Click Restart if it appears at the top of the screen.

### Modifying and Deleting DNAME Records

When you modify a CNAME record, you can change the information you previously entered in the General tab. You can also enter or edit information in the TTL, Extensible Attributes and Permissions tabs. For information on modifying and deleting resource records, see Modifying, Disabling, and Deleting Host and Resource Records.

### Managing NAPTR Records
A NAPTR (Name Authority Pointer) record specifies a rule that uses a substitution expression to rewrite a string into a domain name or URI (Uniform Resource Identifier). A URI is either a URL (Uniform Resource Locator) or URN (Uniform Resource Name) that identifies a resource on the Internet. NAPTR records are usually used to map E.164 numbers to URIs or IP addresses. An E.164 number is a telephone number, 1-555-123-4567 for example, in a format that begins with a country code, followed by a national destination code and a subscriber number. (E.164 is an international telephone numbering system recommended by the International Telecommunication Union.) Thus, NAPTR records allow us to use telephone numbers to reach devices, such as fax machines and VoIP phones, on the Internet.

To map an E.164 to a URI, the E.164 number must first be transformed into a domain name. ENUM (E.164 Number Mapping) specifies a method for converting E.164 numbers to domain names. For example, using the method specified by ENUM, the telephone number 1-555-123-4567 becomes the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. For details about ENUM, refer to RFC 3761, The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM). After the E.164 number is converted to a domain name, a DNS client can then perform a DNS lookup for the NAPTR records of the domain name. The following example illustrates how a DNS client processes NAPTR records.

In this example, the telephone number 1-555-123-4567 is converted to the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. The DNS client then sends a query to the Infoblox DNS server for the NAPTR records associated with 7.6.5.4.3.2.1.5.5.5.1.e164.arpa. The Infoblox DNS server returns the following NAPTR record:

```
$ORIGIN 7.6.5.4.3.2.1.5.5.5.1.e164.arpa
IN NAPTR 100 "U "sip + E2U" "!^.*$!sip:jdoe@corpxyz.com!" .
```

The DNS client then examines the fields in the NAPTR record as follows:

- If a DNS client receives multiple NAPTR records for a domain name, the value in the Order field determines which record is processed first. It processes the record with the lowest value first.
- The DNS client uses the Preference value when the Order values are the same. Similar to the Preference field in MX records, this value indicates which NAPTR record the DNS client should process first when the records have the same Order value. It processes the record with the lowest value first.
- The Flag field indicates whether the current lookup is terminal; that is, the current NAPTR record is the last NAPTR record for the lookup. It also provides information about the next step in the lookup process. The flags that are currently used are:
  - \textbf{U}: Indicates that the output maps to a URI (Uniform Record Identifier).
  - \textbf{S}: Indicates that the output is a domain name that has at least one SRV record. The DNS client must then send a query for the SRV record of the resulting domain name.
  - \textbf{A}: Indicates that the output is a domain name that has at least one A or AAAA record. The DNS client must then send a query for the A or AAAA record of the resulting domain name.
  - \textbf{P}: Indicates that the protocol specified in the Service field defines the next step or phase.

- If the Flag field is blank, this indicates that the client must use the resulting domain name to look up other NAPTR records.
- The Service field specifies the service and protocol that are used to communicate with the host at the domain name. In the example, the service field specifies that SIP (Session Initiation Protocol) is used to contact the telephone service.
- The regular expression specifies the substitution expression that is applied to the original string of the client. In the example, the regular expression \texttt{!^.*$!sip:jdoe@corpxyz.com!} specifies that the domain name 7.6.5.4.3.2.1.5.5.5.1.e164.arpa is replaced with \texttt{sip:jdoe@corpxyz.com}. The regular expression in a NAPTR record is always applied to the original string of the client. It must not be applied to a domain name that resulted from a previous NAPTR rewrite.
- The Replacement field specifies the FQDN for the next lookup, if it was not specified in the regular expression.

\textbf{Note:} If a NAPTR record with the domain name in its native characters is added to the Infoblox Grid through DDNS updates, the Domain and Replacement fields display the domain name in UTF-8 encoded format. For example, a NAPTR record with the domain name .test.com added through DDNS updates displays `\texttt{231\148\181:232\132\145.test.com}` in the Domain and Replacement fields.

### Adding NAPTR Records

To add a NAPTR record:

1. From the \textbf{Data Management} tab, select the DNS tab, expand the Toolbar and click \textbf{Add} \to \textbf{Record} \to \textbf{Add NAPTR Record}.
2. In the Add NAPTR Record wizard, complete the following fields:
   - **Domain**: If Grid Manager displays a zone name, enter the domain name to which this resource record refers. The displayed zone name can either be the last selected zone or the zone from which you are adding the NAPTR record. If no zone name is displayed or if you want to specify a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Select dialog box. Click a zone name in the dialog box, and then enter a domain name for the record. The name you enter is prefixed to the DNS zone name that is displayed, and the complete name becomes the FQDN (fully qualified domain name) of the record. For example, if the zone name displayed is corpxyz.com and you enter admin, then the FQDN becomes admin.corpxyz.com. This field is not displayed when you configure a NAPTR record for a DTC server.
   - **DNS View**: Displays the DNS view of the selected zone.
   - **Service**: Specifies the service and protocol used to reach the domain name that results from applying the regular expression or replacement. You can enter a service or select a service from the list.
   - **Flags**: The flag indicates whether the resulting domain name is the endpoint URI or if it points to another record. Select one of the following:
     - U: Indicates that the output maps to a URI.
     - S: Indicates that the resulting domain name has at least one SRV record.
     - A: Indicates that the resulting domain name has at least one A or AAAA record.
     - P: Indicates that this record contains information specific to another application.
   - **Order**: Select an Integer from 10 to 100, or enter a value from 0 to 65535. This value indicates the order in which the NAPTR records must be processed. The record with the lowest value is processed first.
   - **Preference**: Select an Integer from 10 to 100, or enter a value from 0 to 65535. Similar to the Preference field in MX records, this value indicates which NAPTR record should be processed first when the records have the same Order value. The record with the lowest value is processed first.
   - **RExEX**: The regular expression that is used to rewrite the original string from the client into a domain name. RFC 2915 specifies the syntax of the regular expression. Note that the appliance validates the regular expression syntax between the first and second delimiter against the Python re module, which is not 100% compatible with POSIX Extended Regular Expression as specified in the RFC. For information about the Python re module, refer to http://docs.python.org/release/2.5.1/lib/module-re.html.
   - **Replacement**: This specifies the domain name for the next lookup. The default is a dot (.), which indicates that the regular expression in the REXEX field provides the replacement value. Alternatively, you can enter the replacement value in FQDN format.
   - **Comment**: Optionally, enter a descriptive comment for this record.
   - **Disabled**: Clear the check box to enable the record. Select the check box to disable it.
3. Click Next to define extensible attributes. For information, see Using Extensible Attributes. This is not applicable when you configure a NAPTR record for a DTC server.
4. Save the configuration and click Restart if it appears at the top of the screen.

### Managing LBDN Records

When your Grid has a DNS Traffic Control license, you can add LBDN (Load Balanced Domain Name) records to authoritative or delegated zones. You can add an LBDN even if the zone is DNSSEC signed but some restrictions apply.

To add an LBDN record when in the DNS records list view:

- On the Zones or Members/Servers tab, click the arrow next to the Add icon and select Record -> DTC LBDN. For more information, see Configuring DNS Traffic Control LBDNs.

You can also add an LBDN when in the Traffic Control tab. For more information, see the previously referenced section.

### Viewing Resource Records

You can view the configured resource records by navigating to the Data Management tab -> DNS tab -> Zones tab -> zone -> Records tab. Grid Manager displays the following information for each resource record in the zone:

- **Name**: The name of the record, if applicable. For host records, this field displays the canonical name of the host. For PTR record, this displays the PTR record name without the zone name.
- **Type**: The resource record type.
- **Data**: Data that the record contains. For host records, this field displays the IP address of the host. For PTR records, this displays the domain names.
- **Active Users**: The number of active users for the selected resource record.
- **Comment**: Comments that were entered for the resource record.
- **Site**: Values that were entered for this pre-defined attribute.

**Note**: The DNS record that is obscured by an LBDN record is indicated by a strikethrough, for example, an obscured A record appears as A Record in Grid Manager.

You can also display the following columns:

- **MSDelegationAddresses**: This column appears only if the primary server of the zone is a Microsoft server. It displays the IP addresses that are associated with an NS record.
- **TTL**: The TTL (time-to-live) value of the record.
- **Address**: The IPv4 or IPv6 address associated with the owner domain name in a reverse-mapping zone.
- **Shared**: Displays true for shared resource records. Otherwise, displays false.
- **SharedRecordGroup**: Displays the shared record group name of a shared record.
- **Disabled**: Indicates if the record is disabled.
You can do the following:

- Modify some of the data in the table. Double click a row and either modify the data in the field or select an item from a drop-down list. Click Save to save the changes. Note that some fields are read only.
- Add new DNS records by clicking the arrow next to the Add icon and selecting Host, Record, SharedRecord, and then selecting the required record type. For more information, see Managing Resource Records.
- View the DNS Traffic Control structure for an LBDN.
  - Select the LBDN record and click the Open Visualization icon. For more information, see Visualization for DNS Traffic Control Objects.
- Create a DTC server based on an existing A, AAAA, or host record by selecting a record in the table and clicking CreateDTCServer in the Toolbar or in the record's Action menu. For more information, see Configuring DNS Traffic Control Servers.
- Edit the properties of a resource record.
  - Select the resource record, and then click the Edit icon.
- Delete a resource record.
  - Select the resource record, and then click the Delete icon.
- Export the list of resource records to a .csv file.
  - Click the Export icon.
- Print the list of resource records.
  - Click the Print icon.
- Use filters and the Goto function to narrow down the list. With the autocomplete feature, you can just enter the first few characters of an object name in the Goto field and select the object from the possible matches.
- Create a quick filter to save frequently used filter criteria:

  1. In the filter section, click Show Filter and define filter criteria for the quick filter.
  2. Click Save and complete the configuration in the Save Quick Filter dialog box.

The appliance adds the quick filter to the quick filter drop-down list in the panel. Note that global filters are prefixed with [G], local filters with [L], and system filters with [S].

Modifying, Disabling, and Deleting Host and Resource Records

You can modify, disable, or delete an existing host or DNS resource record. When physical repair or relocation of a network device occurs, you can disable a record instead of deleting it. When you disable a record, the NIOS appliance does not answer queries for it, nor does it include disabled records in zone transfers and zone imports. This avoids having to delete and then add the record again. When the changes to the physical device are complete, you can simply enable the host or resource record.

To modify or disable a host or resource record:

1. Use one of the following methods to retrieve the host or resource record:
   - Perform a global search.
   - Select it from a Smart Folder.
   - From the Data Management tab, select the DNS tab - > Zones tab - > dns_view - > zone - > host_record or resource_record.
2. Select the record you want to modify and click the Modify icon.
3. In the host or resource record editor, you can do the following:
   - In the General tab, you can change most of the information, except for the read-only fields, such as the DNSView and HostNamePolicy. You can select the Disable check box to disable the record.
   - In the TTL tab, you can modify the TTL setting. The NIOS appliance also allows you to specify TTL settings for each record. If you do not specify a TTL for a record, the appliance applies the default TTL value of the zone to each record. For information, see About Time To Live Settings.
   - In the Extensible Attributes tab, you can modify the attributes. For information, see Using Extensible Attributes.
   - The Permissions tab displays if you logged in as a superuser. For information, see About Administrative Permissions.
4. Save the configuration and click Restart if it appears at the top of the screen.

When you delete host and resource records, Grid Manager moves them to the Recycle Bin. You can use the Recycle Bin to store deleted DNS configuration objects and selectively restore objects to the active configuration at a later time. You can also permanently remove the objects from the Recycle Bin.

**Note:** You cannot delete automatically-generated records, such as NS records and SOA records.

To delete host and resource record:

1. Perform a global search to retrieve the record you want to delete. 
   or 
   From the Data Management tab, select the DNS tab, click the Zones tab - > dns_view - > zone - > host_record or resource_record.
2. Select the record and click the Delete icon.
3. In the Delete Confirmation dialog box, select Yes to delete or No to cancel.
4. Optionally, if the Enable PTR record removal for A/AAAA records option is selected and if you try to delete an A or AAAA record, the appliance displays the Delete Confirmation (A or AAAA Record) dialog box to confirm whether you want to remove the corresponding PTR record that was automatically generated while creating the A or AAAA record. In the Delete Confirmation dialog box, select the Remove associated PTR resource record(s) check box and click Yes to delete the associated PTR record or click No to cancel. For information about enabling this option, see Deleting PTR Records associated with A or AAAA Records.
   or 
   You can also schedule the deletion for a later time. Click Schedule Deletion and in the Schedule Change panel, enter a date, time, and time zone. For information, see Scheduling Deletions.