Signing a Zone

When it signs a zone, the Grid Master generates new DNSKEY key pairs. As shown in 4820072, it uses the private key of the ZSK to sign the authoritative RRsets in the zone, and stores the corresponding public key in a DNSKEY record. It then uses the private key of the KSK to sign the DNSKEY records and stores the corresponding public key in another DNSKEY record. It stores the private keys in the Grid database and stores the public keys in the DNSKEY records in the database.

The Grid Master also does the following:

- It inserts NSEC or NSEC3 records. The use of NSEC or NSEC3 records depends on the NSEC type you selected for the Grid or the zone. When you select NSEC3, the Grid Master uses NSEC3 records in signed zones.
- It increments the SOA serial number and notifies the secondary servers that there is a change to its zone data. When the secondary servers check the serial number and see that it has been incremented, the secondary servers request a zone transfer.
- If the TTL of an RR in the zone exceeds the ZSK grace period, the Grid Master reduces the TTL to the ZSK grace period. (For information about the grace period, see About Key Rollovers.) Setting a TTL value that exceeds half of the rollover period is not allowed.
- If the KSK rollover period is less than the ZSK rollover period, the Grid Master sets the TTL of the DNSKEY RR to the KSK rollover period.
- The appliance sets the Grid Master as the primary server for zones, enables DNSSEC on the Grid Master, and starts DNS service on the Grid Master.

When it signs a subzone, the Grid Master automatically inserts DS records for parent zones that are hosted by Grid members. The appliance allows you to sign a single zone or multiple zones simultaneously. For example, if you have multiple zones that are due for rollover at the same time, you can select all such zones and sign them at once. Note that each operation is independent of the other. For example, if you want to sign five zones at the same time, and if one of the zones fails during this time, NIOS signs the remaining four zones. Note that the selected zones must have an associated primary server. The appliance displays an error message if the zone does not have a primary server. When the sign operation fails, the appliance displays the zone names, associated DNS views, and the error message indicating the reason for failure.

To sign a zone:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Sign Zones.
3. In the Sign Zones dialog box, the displayed zone name can either be the last selected zone or the zone from which you are signing. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays unsigned zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. Select a zone. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. After you have selected the zones, click Sign Zones.
5. When the confirmation dialog displays, click Yes.

When you sign multiple zones, the appliance displays generic error messages for the following cases:

- The value to which the resource record TTL is reduced is not displayed.
- The appliance displays a message about name server group disassociation if at least one zone is associated with a name server group. It will not list the affected zones.
- When you sign a zone or multiple zones, the appliance displays a warning message indicating that the operation might take a longer time.
The appliance displays an error message if the number of characters in the zone name, which you want to sign, exceeds 180 characters. You can sign a zone only when the name of the zone is less than 180 characters in size.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon. To view the records of the signed zone, from the Data Management tab, select the DNS tab -> Zones tab -> zone. Expand the Records section to list the RRs of the zone, as shown in Figure 22.4

Managing Signed Zones

After you sign a zone, you can do the following:

- You can add a DS RR at the delegation point for a signed subzone when the subzone is hosted on a non-Infoblox DNS server or an Infoblox server that is part of a different Grid. For information, see 4820072.
- Trust anchors can be specified as DNSKEY RRs, DS RRs, and as a BIND trusted-keys statement. You can export any of these as trust anchors. For information, see 4820072.
- You must change the KSK periodically, to ensure its security. For information, see 4820072 and 4820072.
- You can initiate ZSK rollovers manually. For information, see 4820072.
- If, for any reason, the security of the keys are compromised, you can delete a key and perform a manual rollover. For information, see 4820072.
- Note that when you re-sign a zone, the Grid Master generates new ZSK and KSK pairs. You must send the new DNSKEY of the KSK to resolvers that use it as a trust anchor and generate new DS records and send them to the parent zones.
- You can move a signed zone to the Recycle Bin, from where you can delete it permanently or restore it. For information, see 4820072.

In addition, signed zones can accept dynamic DNS updates. For information about configuring zones to accept dynamic DNS updates, see Configuring DNS Servers for DDNS.

Importing a Keyset

A keyset is a DS RRset, or a DNSKEY RRset which is used as input to generate the DS RRset. To import a keyset:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Import Keyset.
3. In the Import Keyset dialog box, the displayed zone name can either be the last selected zone or the zone from which you are importing the keyset. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select a zone.
4. Paste the KSK or DS record being imported. It must be a KSK or DS record, and must belong to an immediate subzone of the zone to which the record is being imported.
5. Click Import.

If you imported a DNSKEY RRset, the Grid Master uses the SHA-1 algorithm to generate the DS RRset, which it adds to the parent zone. If you imported a DS RRset, the Grid Master adds it to the parent zone. The Grid Master incrementally signs the DS RRset.

Exporting Trust Anchors
A trust anchor is a DNSSEC public key which is used by security-aware resolvers as the starting point for establishing authentication chains. A trust anchor can be specified as a DNSKEY RR or a DS RR, which contains the hash of a DNSKEY RR and can also be used to create a secure delegation point for a signed subzone in DNS servers.

In BIND, trust anchors are configured using the trusted-keys directive. A trusted key is a DNSKEY RR without the TTL, class and RR type. You can export the trust anchors for the selected zone in a format that can be used in a BIND trusted-keys directive. Exporting trust anchors supports multiple algorithms, which means you can export all the algorithms in a key.

To export trust anchors:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Export Trust Anchors.
3. In the Export Trust Anchors dialog box, do the following:
   - The displayed zone name can either be the last selected zone or the zone from which you are exporting trust anchors. If no zone name is displayed or if you want to select a different zone, click Select Zone. When there are multiple zones, Grid Manager displays the Zone Selector dialog box from which you can select one.
   - Select one of the following: DNSKEY records, DS records, or BIND trusted-keys statement.
4. Click Export.
5. Specify the location of the exported file and click OK.

If you exported DS records, the exported file contains DS records that use the SHA-1 and SHA-256 algorithms.

Checking Key-Signing Keys

To check which key-signing keys are overdue for a rollover or are due to roll over within a week:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Check KSK Rollover Due.
3. The KSK Rollover Due dialog box lists the key-signing keys that are due to rollover. It includes the domain name of the zone, DNS view (if there are multiple DNS views), and the number of days until the rollover.
4. You can click the Schedule icon at the top of the wizard to schedule a KSK rollover for one or more zones at a given date and time. In the Schedule Change dialog box, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
5. Click Close.

Rolling Key-Signing Keys

You can initiate a rollover before or after a rollover period, or when you need to replace the KSK for security reasons. You can initiate a KSK rollover several times simultaneously, but note that the number of keys will increase each time you perform a rollover. You can schedule the KSK rollover to occur at a later date and time.

To roll over key-signing keys:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Roll Over Key-Signing Key.
3. In the Roll Over Key-Signing Key dialog box, the displayed zone name can either be the last selected zone or the zone from which you are rolling over key-signing keys. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays signed zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule a KSK rollover for one or more zones at a given date and time. In the Schedule Change dialog box, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks. Note that you cannot schedule the KSK rollover on a recurring basis.
4. Click Roll Over.

You can export the new KSK and send it to the security-aware resolvers that use it as a trust anchor. To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon.

Rolling Zone-Signing Keys

Only an administrator can initiate ZSK rollovers either before or after a rollover period, or when you want to replace the ZSK for security reasons. You can initiate a ZSK rollover several times simultaneously, but note that the number of keys will increase each time you perform a rollover.

To roll over zone-signing keys:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Roll Over Zone-Signing Key.
3. In the Roll Over Zone-Signing Key dialog box, the displayed zone name can either be the last selected zone or the zone from which you are rolling over zone-signing keys. If no zone name is displayed or if you want to select a different zone, click the Add icon. The appliance displays unsigned zones only. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. To add multiple zones, click the Add icon and select a zone.
   You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. Click Roll Over.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon. The appliance displays warning messages when the changes take effect on the first zone or when the rollover occurs. You cannot change the zone-signing key rollover method while the previous change is still in progress. The previous change will be completed only when the zone active key, which is active when the rollover method is changing, expires and is deleted.
Best Practices for Configuring Zone Signing Keys

Infoblox recommends that you use the pre-publish option for zone signing key method for the following reasons:

- The double-signature ZSK rollover doubles the number of signatures in your zone when a rollover is in progress. The size of the zone increases due to the duplicate signature records. This is not recommended if the size of your zones are large. When you select this option, the appliance creates a new set of signatures for all the resource records. This also increases the database usage.
- When you select to pre-publish key rollover, the rollover uses a single key to sign the records at a given time and it does not sign the zone data twice. The appliance publishes the new key in the keysset even before the actual rollover. This reduces the database usage.

Unsigning a Zone

When you unsign a zone, the Grid Master permanently removes all automatically generated DNSSEC records in the zone and parent zone. It does not remove any DS records associated with a child zone. You can unsign a single zone or multiple zones at the same time.

To unsign a zone:

1. From the Data Management tab, select the DNS tab.
2. Expand the Toolbar and click DNSSEC -> Unsign Zones.
3. In the Unsign Zones dialog box, the displayed zone name can either be the last selected zone or the zone from which you are unsigning. If no zone name is displayed or if you want to select a different zone, click the Add icon. When there are multiple zones, Grid Manager displays the Zone Selector dialog box. The appliance displays signed zones only. Select a zone. To add multiple zones, click the Add icon and select a zone. You can click the Schedule icon at the top of the wizard to schedule this task. In the Schedule Change panel, either select Now and click Save or select Later and enter a date, time, and time zone. For information, see Scheduling Tasks.
4. After you have selected the zones, click Unsign Zones.
5. When the confirmation dialog displays, click Yes.

To remove a zone from the list, select the check box adjacent to the respective zone and click the Delete icon.

Deleting and Restoring Signed Zones

When you delete a signed zone, the Grid Master unsigns the zone before moving it to the Recycle Bin. Unsigning the zone effectively deletes all auto-generated DNSSEC RRs; only user-defined DS records are retained and moved to the Recycle Bin as well. The Grid Master also retains the ZSK and KSK in its database, until you permanently delete the zone from the Recycle Bin.

When you restore a signed zone, the Grid Master restores it and re-signs its data sets with the original keys, which are also restored. You can also restore the user-defined DS records. The rollover period of the ZSK and KSK starts when the zone is signed after it is restored. Note that when you restore a zone that contains rolled keys, either KSK or ZSK, the appliance removes all these rolled keys. Note that when you restore a deleted zone from recycle bin on the NIOS server, which is created and signed on the Microsoft Server 2012, then all the DNSSEC records will be deleted, except for the DNSKEY records. The DNSKEY records will only be resynchronized. The DNSSEC records are read-only and cannot be regenerated using NIOS. You must recreate the zone manually on the Microsoft Server. When you recreate the zone on the Microsoft Server, new keys will be generated. The signed zone, which is restored, and the DNSSEC keys are synced to Microsoft Server. This zone will be seen as an unsigned zone on the Microsoft Server, as NIOS does not trigger the signing zone request for the corresponding zone. For such zones, the ‘DNSSEC’ label is not displayed and the value for ‘Signed’ column is ‘No’.

To delete a signed zone:

1. From the Data Management tab, select the DNS tab -> Zones tab.
2. Click the check box of the zone you want to delete.
3. Click the Delete icon.
4. Click Yes to confirm the deletion.

To restore a signed zone:

1. In the Finder panel, expand Recycle Bin.
2. Select the zone you want to restore.
3. Click the Restore icon.

Configuring Automatic KSK Rollovers and Notifications

You can configure automatic KSK rollovers at the Grid level and override the settings at the zone level. You can also configure notifications for KSK rollovers. The appliance sends one notification, SNMP, or email, or both based on the selection, for each event. For example, if the KSK of two zones are rolled over in the same batch, the appliance sends two notifications, one for each zone. Note that the appliance sends these notifications only once, and they are not recurring. Apart from the notifications that you receive, Grid Manager also displays a banner when you log in to the Grid indicating that the KSK rollover is due within the next seven days.

These notifications are not applicable to an ZSK, as the ZSK rollover is an automated process. The appliance generates numerous notifications. To configure KSK rollover, complete the following:

1. Grid: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties.
   Zone: From the Data Management tab, select the DNS tab -> Zones tab -> zone check box, and click the Edit icon. Click Override to override the values at the zone level.
   Standalone appliance: From the Data Management tab, select the DNS tab. Expand the Toolbar and click System DNS Properties.
2. Select the DNSSEC tab and complete the following in the Basic tab:
   - KSK Notification Configuration: You can choose to receive notifications for KSK rollover events.
     - No Notifications: Select this if you do not want to receive any notifications for KSK rollover events.
     - Notifications for all KSK rollover events: Select this if you want to receive notifications for all KSK rollover events. The appliance sends notifications after the rollover.
The appliance enables notifications and automatic KSK rollover by default for NIOS 6.11.0 and later releases. Properties manual update requiring Settings From the Basic Management DNS Management DNS iterations hashing 4820072 to DNS NSEC3 DNS Notification System Grid Signing DNS SNMP Length DS. Data HSM Override Properties Management Data Zones An emergency KSK rollover involves the following: manually, see when a zone is compromised. To initiate an emergency rollover, you must first perform a manual rollover. For information about rolling over a KSK compromised key and the associated compromised data from the zone. The ability to perform emergency rollovers enable administrators to react quickly. The appliance supports emergency rollover that can be used when the keys are compromised. In an emergency operation, you must delete the rolled key.

Configuring NSEC3 Salt Length and Hashing Iterations

The salt is a random string, which is appended to the domain name before it gets hashed. The number of iterations indicates the number of additional times the hashing occurs. These serve as a protection against dictionary attacks. The appliance generates a new salt for initial signing and changes it every time a ZSK rollover occurs. Note that when you use a longer salt and higher number of iterations, DNS is more secure and the chances of dictionary attacks on NSEC3 are reduced.

You can choose the minimum and the maximum salt length at the Grid level and override them at the zone level. Note that the length of the salt has an impact on the size of the NSEC3 record, but it does not have an impact on the performance of the appliance. When the number of iterations increases, the DNS client has to validate a additional data and the cost of the DNS server to serve the zone increases. This might also reduce the performance of the system with regards to DNSSEC operations.

To define salt length and hashing iterations, complete the following:

1. Grid: From the Data Management tab, select the DNS tab. Expand the Toolbar and click Grid DNS Properties. Zone: From the Data Management tab, select the DNS tab -> Zones tab -> Zone check box, and click the Edit icon. Click Override to override the parameters.
2. Standalone appliance: From the Data Management tab, select the DNS tab. Expand the Toolbar and click System DNS Properties.
3. Select the DNSSEC tab and complete the following in the Basic tab:

   - Zone-signing Key Settings
     - NSEC3 Salt Length: Specify a minimum and maximum length for NSEC3 salt. The minimum length is one octet and the maximum length is 255 octets. The appliance sets the following default values for minimum and maximum lengths respectively: one and 15 octets.
     - Number of NSEC3 hashing iterations: The appliance uses the default value, ten, for hashing iterations. The minimum value is ten and the maximum value depends on the smallest key size, as defined in RFC 5155 as follows:
       - 150 if the key size is equal or less than 1024 bits.
       - 500 if the key size is equal or less than 2048 bits.
       - 2,500 if the key size is equal or less than 4096 bits.

Note: The above fields are displayed only when you select NSEC3 record type.

Deleting Server Keys

The appliance retains the key until the expiration of the grace period. For example, if the validity period of a KSK is two years, you can delete the rolled key after publishing the DS record to the parent zone and waiting for a period greater than its TTL.

The following rules are valid for KSK and ZSK signing using the double-signature scheme:

- You cannot delete an active key.
- When you delete a rolled key, the appliance displays a warning message indicating that it might break validation on clients.

The following rules are valid for ZSK signing using the pre-publish scheme:

- You cannot delete an active key.
- When you delete a pre-published key, the appliance generates a new pre-published key.
- You can delete a rolled key. The appliance deletes this key as it is no longer used.

When you use an HSM, the appliance does not delete the key from HSM. For more information, see About HSM Signing.

Configuring Emergency KSK Rollover

The appliance supports emergency rollover that can be used when the keys are compromised. In an emergency operation, you must delete the compromised key and the associated compromised data from the zone. The ability to perform emergency rollovers enable administrators to react quickly when a zone is compromised. To initiate an emergency rollover, you must first perform a manual rollover. For information about rolling over a KSK manually, see 4820072. After the rollover, you must delete the compromised key. For information about deleting the compromised key, see 4820072. An emergency KSK rollover involves the following:

- The administrator of the compromised zone, which is hosted on the Infoblox appliance, must initiate the emergency KSK rollover and later export the corresponding DS record.
- The administrator of the parent zone, which is hosted on an external server, must import the DS record of the child zone. This is required to maintain the chain of trust.
During this emergency procedure, the chain of trust is temporarily broken. As stated in RFC 6781, the effect depends on the order of the operations:

- You must perform the KSK rollover first. The chain of trust is broken until the administrator of the parent zone replaces the DS record. In the meantime, the zone appears bogus to a validating client.
- You must remove the compromised DS record first. The chain of trust is broken until the NIOS administrator performs the KSK rollover, communicates the new DS record to the administrator of the parent zone who then adds it. In the meantime, the zone appears insecure to validating resolvers.

Handling Error and Warning Messages for DNSSEC Operations

Grid Manager consolidates warnings from one or more DNSSEC long running operations and displays them in a single dialog box. For more information about long running tasks, see About Long Running Tasks. When the long running operations are completed with warnings, the appliance displays the message using a yellow banner at the top of Grid Manager. Click Show Warnings to view the warnings that are generated by the server for DNSSEC operations. Click Close to close the warning dialog box.

The appliance also displays a warning icon in the Execution Status column of the Task Manager. For more information about the task manager, see Viewing Tasks. When you click the icon, the appliance displays a dialog box indicating that the task is complete with warnings. Click the show task details hyperlink to view detailed information about the error or warning message. The appliance displays Scheduled Task Details wizard in which you can view the task details and error or warning messages, if any. For more information, see 4820072. The appliance clears the warning messages from the cache when you close the dialog box.

When a DNSSEC operation fails, NIOS saves the messages in the syslog. For more information about the syslog, see Using a Syslog Server.

Viewing Scheduled Tasks

You can view the status of operations that are scheduled. The appliance also displays error or warning messages, if any. For example, if you schedule the Sign Zones operation for multiple zones, there is a possibility that some operations may fail, some may succeed with warnings, and some are completed successfully. You can also view the error or warning messages that are generated for certain affected zones. To view the status:

1. From the Administration tab, select the Workflow tab -> Task Manager tab.
2. Grid Manager displays the DNSSEC operations that are scheduled. To view the details you can either click the Action icon next to the task ID and select View from the menu or select the check box adjacent to the Action icon and then click View from the Toolbar.
3. The General tab of the Scheduled Task Details wizard displays the following details:
   - Task ID: The ID associated with the task. The appliance assigns an ID to a task in chronological order. By default, the appliance sorts tasks by Task ID.
   - Action Type: The operation the appliance performs in this task.
   - Submitter: The username of the admin who scheduled or submitted the task.
   - Submitted Time: The date, time, and time zone when the task was submitted.
   - Ticket Number: For an approval workflow, this number may be entered by the submitter to associate the task with a help desk ticket number or a reference number.
   - Approver: The username of the admin who has approved this task.
   - Approver Comments: Comments entered by the approver.
   - Executed on Member: The Grid member on which the task is executed.
   - Execution Status: The execution status of the task. Possible values are Completed, Failed, Pending, and Executing.
   - Execution Time: The date, time, and time zone when the task was executed.
   - Affected Objects: The name of the object and object type.
4. The Warnings/Errors tab of the Scheduled Task Details wizard displays error or warning messages related to tasks. It also displays object execution details. This table is blank if there are no error messages or warnings. You can view the error message and the name of the zone with which the error or warning message is associated.
5. Click Close to close the dialog box.