

Oracle

*NoSQL Database
Administrator's Guide*

12c Release 1
Library Version 12.1.4.3



Legal Notice

Copyright © 2011 - 2017 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Published 17-Feb-2017

Table of Contents

Preface	x
Conventions Used in This Book	x
1. Installing Oracle NoSQL Database	1
Installation Prerequisites	1
Installation	2
Installation Configuration	3
Steps to Configure KVSTORE Installation	6
Configuring the Firewall	8
2. Plans	9
Using Plans	9
Feedback While a Plan is Running	9
Plan States	10
Reviewing Plans	10
Plan Ownership	11
3. Configuring the KVStore	12
Configuration Overview	12
Start the Administration CLI	12
The plan Commands	13
Configure and Start a Set of Storage Nodes	14
Name your KVStore	14
Create a Zone	14
Create an Administration Process on a Specific Host	16
Create a Storage Node Pool	17
Create the Remainder of your Storage Nodes	18
Create and Deploy Replication Nodes	18
Configuring Security with Remote Access	19
Configuring with Multiple Zones	20
Using a Script to Configure the Store	28
Smoke Testing the System	28
Troubleshooting	30
Where to Find Error Information	31
Service States	31
Useful Commands	32
4. Determining Your Store's Configuration	34
Steps for Changing the Store's Topology	35
Make the Topology Candidate	35
Transform the Topology Candidate	36
Increase Data Distribution	37
Increase Replication Factor	38
Balance a Non-Compliant Topology	38
Contracting a Topology	39
View the Topology Candidate	40
Validate the Topology Candidate	41
Preview the Topology Candidate	41
Deploy the Topology Candidate	42
Verify the Store's Current Topology	43

Deploying an Arbiter Node Enabled Topology	45
5. Upgrading an Existing Oracle NoSQL Database Deployment	51
Preparing to Upgrade	51
General Upgrade Notes	51
Upgrade to This Release from Release 3.0 or Later	53
Using a Script to Upgrade to Release 4	58
6. Administrative Procedures	60
Backing Up the Store	60
Taking a Snapshot	60
Snapshot Management	61
Recovering the Store	63
Using the Load Program	63
Load Program and Metadata	65
Restoring Directly from a Snapshot	67
Recovering from Data Corruption	67
Detecting Data Corruption	68
Data Corruption Recovery Procedure	68
Using the Export and Import Utilities	70
Exporting Data	70
Importing Data	72
Installing the Cloud Storage JARs	73
Managing Avro Schema	73
Adding Schema	73
Changing Schema	74
Disabling and Enabling Schema	74
Showing Schema	74
Increasing the capacity of a Storage Node	75
Managing Storage Directory Sizes	77
Replacing a Failed Storage Node	79
Replacing a Failed Disk	82
Repairing a Failed Zone by Replacing Hardware	84
Disabling Storage Node Agent Hosted Services	84
Verifying the Store	85
Monitoring the Store	89
Events	90
Other Events	90
Setting Store Parameters	91
Changing Parameters	91
Setting Store Wide Policy Parameters	92
Admin Parameters	93
Storage Node Parameters	94
Replication Node Parameters	97
Global Parameters	98
Security Parameters	98
Admin Restart	100
Replication Node Restart	101
Removing an Oracle NoSQL Database Deployment	101
Fixing Incorrect Storage Node HA Port Ranges	102
7. Failover and Switchover Operations	104

Repairing a Failed Zone	104
Performing a failover	105
Performing a Switchover	108
8. Standardized Monitoring Interfaces	112
Java Management Extensions (JMX)	112
Enabling Monitoring	112
In the Bootfile	112
By Changing Storage Node Parameters	113
Displaying the NoSQL DB MBeans	113
9. Integrating Oracle Enterprise Manager (OEM) with Oracle NoSQL Database	114
Importing and Deploying the EM Plug-in	114
Adding NoSQL Database Targets	115
Components of a NoSQL Store	118
Store Targets	119
Store Page	119
Storage Node Page	122
Shard Page	123
Replication Node Page	124
A. Installing and Configuring a Non-secure Store	127
Installation Configuration	127
B. CLI Command Reference	130
aggregate	132
aggregate kv	132
aggregate table	134
await-consistent	135
change-policy	136
configure	136
connect	137
connect admin	137
connect store	137
delete	138
delete kv	139
delete table	139
ddl	139
ddl add-schema	140
ddl enable-schema	140
ddl disable-schema	140
execute	140
exit	141
get	141
get kv	141
get table	144
help	144
hidden	145
history	145
load	145
logtail	146
page	147
ping	147

plan	148
plan add-index	149
plan add-table	150
plan register-es	152
plan deregister-es	152
plan cancel	153
plan change-parameters	153
plan change-storagedir	154
plan change-user	154
plan create-user	155
plan deploy-admin	155
plan deploy-datacenter	155
plan deploy-sn	155
plan deploy-topology	156
plan deploy-zone	156
plan drop-user	157
plan evolve-table	157
plan execute	158
plan failover	158
plan grant	159
plan interrupt	159
plan migrate-sn	160
plan remove-admin	160
plan remove-index	160
plan remove-datacenter	161
plan remove-sn	161
plan remove-table	161
plan remove-zone	161
plan repair-topology	162
plan revoke	162
plan start-service	162
plan stop-service	163
plan wait	163
pool	163
pool clone	164
pool create	164
pool join	164
pool leave	164
pool remove	164
put	164
put kv	165
put table	166
repair-admin-quorum	167
show	167
show admins	168
show datacenters	168
show events	168
show faults	169
show indexes	169

show parameters	169
show perf	169
show plans	169
show pools	170
show schemas	170
show snapshots	170
show tables	171
show topology	171
show upgrade-order	171
show users	171
show versions	171
show zones	172
snapshot	172
snapshot create	172
snapshot remove	172
table	173
table-size	173
timer	176
topology	176
topology change-repfactor	177
topology change-zone-arbiters	177
topology change-zone-type	178
topology clone	178
topology contract	178
topology create	178
topology delete	179
topology list	179
topology preview	179
topology rebalance	179
topology redistribute	179
topology validate	179
topology view	180
verbose	180
verify	180
verify configuration	180
verify prerequisite	180
verify upgrade	181
C. Utility Command Reference	182
export	182
Export Utility Command Line Parameters	183
Export Utility Configuration File	184
Schema Management	185
Export Exit Codes	186
generateconfig	186
help	186
import	187
Import Utility Command Line Parameters	188
Import Utility Configuration File	189
Import Exit Codes	191

load admin metadata	191
load store data	192
makebootconfig	193
ping	198
Ping Command Line Parameters	198
Ping Exit Codes	199
Ping Report Text Output	201
Ping Report JSON Output	202
restart	204
runadmin	205
start	205
status	205
stop	206
version	206
D. Initial Capacity Planning	207
Shard Capacity	207
Application Characteristics	208
Replication Factor	208
Average Key Size	208
Average Value Size	208
Read and Write Operation Percentages	209
Hardware Characteristics	209
Shard Storage and Throughput Capacities	209
Shard Storage Capacity	209
Shard I/O Throughput capacity	210
Memory and Network Configuration	210
Machine Physical Memory	211
Sizing Advice	211
Determine JE Cache Size	212
Machine Network Throughput	213
Estimate total Shards and Machines	214
Number of Partitions	215
E. Tuning	216
Turn off the swap	216
Linux Page Cache Tuning	216
OS User Limits	217
File Descriptor Limits	218
Process and Thread Limits	218
Linux Network Configuration Settings	218
Server Socket Backlog	219
Isolating HA Network Traffic	219
Receive Packet Steering	219
Managing the Off-heap Cache	220
Configuring the Off-heap Cache	221
F. Solid State Drives (SSDs)	225
Trim requirements	225
Enabling Trim	225
G. Diagnostics Utility	226
Setting up the tool	226

Packaging information and files	227
Verifying Storage Node configuration	229
Key Distribution Statistics Utility	230
H. Third Party Licenses	232

Preface

This document describes how to install and configure Oracle NoSQL Database (Oracle NoSQL Database).

This book is aimed at the systems administrator responsible for managing an Oracle NoSQL Database installation.

Conventions Used in This Book

The following typographical conventions are used within this manual:

Information that you are to type literally is presented in monospaced font.

Variable or non-literal text is presented in *italics*. For example: "Go to your *KVHOME* directory."

Note

Finally, notes of special interest are represented using a note block such as this.

Chapter 1. Installing Oracle NoSQL Database

This chapter describes the installation process for Oracle NoSQL Database in a multi-host environment. If you are planning a large system for production use, please read [Initial Capacity Planning \(page 207\)](#) to estimate the number of storage nodes on which you will need to install the software. For simple uses when you already know the storage nodes you intend to use, simply follow the instructions below and Oracle NoSQL Database will make the best use of the storage nodes you provide.

Installation Prerequisites

Make sure that you have Java SE 8 or later installed on all of the hosts that you are going to use for the Oracle NoSQL Database installation. The command:

```
java -version
```

can be used to verify this.

Note

Oracle NoSQL Database is compatible with Java SE 8 (64 bit), and has been tested and certified against Oracle Java SE 8. It is recommended that you upgrade to the latest Java releases to take advantage of the latest bug fixes and performance improvements. The release notes included in the Oracle NoSQL Database download specify the exact Java versions that have been used for certification.

Note

Java SE Development Kit 8, Update 121 (JDK 8u121) introduces new behavior that can cause failure when running Oracle NoSQL Database in a secure configuration. These failures are the result of the addition of a new Java feature called `RMI Better constraint checking`. Using Oracle NoSQL Database in a secure configuration currently requires setting the RMI registry filter.

For more details, see the Oracle NoSQL Database Release Notes here: <http://docs.oracle.com/cd/NOSQL/html/relnotes.html#issues>

Make sure that the `jps` utility is working. Installing the JDK allows the `jps` tools to be available for use by the Storage Node Agent (SNA) in order to optimally manage Oracle NoSQL Database processes. The `jps` tools also allow you to diagnose any issues that may turn up. While Oracle NoSQL Database can continue to operate in the absence of the `jps` tools, it diminishes its ability to manage its processes.

If the JDK and its tools have been correctly installed, the output from `jps` should list at least one Java process (the `jps` process itself). Use the following command to verify this:

```
% jps
16216 Jps
```

Note

You must run the commands listed above as the OS user that will run the Oracle NoSQL Database SNA processes.

Linux and Oracle Solaris are officially supported platforms for Oracle NoSQL Database. Both Oracle Solaris x86 and Oracle Solaris SPARC are supported. A 64 bit JVM is required in order to run Oracle NoSQL Database.

You do not necessarily need root access on each node for the installation process.

Finally, **make sure** that some sort of reliable clock synchronization is running on each of the machines. Generally, a synchronization delta of less than half a second is required. Network Time Protocol (ntp) is sufficient for this purpose.

Installation

The following procedures describe how to install Oracle NoSQL Database:

1. Pick a directory where the Oracle NoSQL Database package files (libraries, Javadoc, scripts, and so forth) should reside. It is easiest if that directory has the same path on all nodes in the installation. You should use different directories for the Oracle NoSQL Database package files (referred to as KVHOME in this document) and the Oracle NoSQL Database data (referred to as KVROOT). Both the KVHOME and KVROOT directories should be local to the node (that is, not on a Network File System).

Note

To make future software upgrades easier, adopt a convention for KVHOME that includes the release number. Always use a KVHOME location such as `/var/kv/kv-M.N.O`, where M.N.O are the release.major.minor numbers. This can be easily achieved by simply unzip/untaring the distribution into a common directory (`/var/kv` in this example).

2. Extract the contents of the Oracle NoSQL Database package (`kv-M.N.O.zip` or `kv-M.N.O.tar.gz`) to create the KVHOME directory (i.e. KVHOME is the `kv-M.N.O/` directory created by extracting the package). If KVHOME resides on a network shared directory (not recommended) then you only need to unpack it on one machine. If KVHOME is local to each machine, then you should unpack the package on each node.
3. Verify the installation by issuing the following command on one of the nodes:

```
java -Xmx256m -Xms256m -jar KVHOME/lib/kvclient.jar
```

You should see some output that looks like this:

```
11gR2.M.N.O (....)
```

where M.N.O is the package version number.

Note

Oracle NoSQL Database is a distributed system and the runtime needs to be installed on every node in the cluster. While the entire contents of the Oracle NoSQL Database package do not need to be installed on every node, the contents of the lib and doc directories must be present. How this distribution is done is beyond the scope of this manual.

Installation Configuration

Before you configure Oracle NoSQL Database, you should determine the following parameters for each Storage Node in the store:

- *root*

Where the KVROOT directory should reside. There should be enough disk space on each node to hold the data to be stored in your Oracle NoSQL Database store. The KVROOT disk space requirements can be reduced if the *storagedir* parameter is used to store the data at a different location outside the KVROOT directory. It is best if the KVROOT is the same local directory path on each node (but not a shared or NFS mounted directory). The examples in this book assume that the KVROOT directory already exists.

- *port*

The TCP/IP port on which Oracle NoSQL Database should be contacted. This port should be free (unused) on each node. It is sometimes referred to as the *registry port*. The examples in this book use port 5000.

- *harange*

A range of free ports which the Replication Nodes use to communicate among themselves. These ports must be sequential and there must be at least as many as there are Replication Nodes running on each Storage Node in your store. The Storage Node Agent manages this allotment of ports, reserves one for an Admin service, and uses the rest to allocate one per Replication Node. The port range is specified as "startPort,endPort". "5010,5020" is used by the examples in this book.

- *servicerange*

A range of ports that may be used for communication among administrative services running on a Storage Node and its managed services. This parameter is optional and is useful when services on a Storage Node must use specific ports for firewall or other security reasons. By default the services use anonymous ports. The format of the value string is "startPort,endPort." For more information about the servicePortRange, see [Storage Node Parameters \(page 94\)](#).

- *store-security*

Specifies if security will be used or not.

If none is specified, no security will be used.

If configure is specified, security will be used and the security configuration utility will be invoked as part of the makebootconfig process.

If enable is specified, security will be used. You will need to configure security either by utilizing the security configuration utility or by copying a previously created configuration from another system.

Note

The `-store-security` parameter is optional. If it is not specified, security is configured by default. If you are performing a secure installation, then you must use the `securityconfig` utility to create the security folder before starting up the storage node agents. For more information on the configuration steps see [Configuring the KVStore \(page 12\)](#).

- *capacity*

The total number of Replication Nodes a Storage Node can support. Capacity is an optional parameter. Capacity can be set to values greater than 1 when the Storage Node has sufficient disk, cpu, memory and network bandwidth to support multiple Replication Nodes.

If capacity is set to 0, then this Storage Node may be used to host Arbiter Nodes. The pool of Storage Nodes in a zone configured to host Arbiter Nodes are used for Arbiter Node allocation. For more information see [Deploying an Arbiter Node Enabled Topology \(page 45\)](#).

Please keep the following configuration considerations in mind for nodes with capacity greater than one:

1. It is best if the Storage Node is configured with a capacity equal to the number of disks available on the machine. Such a configuration permits the placement of each Replication Node on its own disk and ensures that the Replication Nodes on the Storage Node are not competing for I/O resources. The location of this directory on its disk can be specified via the `storagedir` parameter.

For example:

```
> java -jar KVHOME/lib/kvstore.jar makebootconfig \  
-root /opt/ondb/var/kvroot \  
-port 5000 \  
-host node10 \  
-harange 5010,5025 \  
-capacity 3 \  
-storagedir /disk1/ondb/data \  
-storagedir /disk2/ondb/data \  
-storagedir /disk3/ondb/data
```

where capacity=3 equals the number of disks (disk1, disk2, disk3) located on the same Storage Node (node10).

2. Increase the *harange* parameter to account for the additional ports required by the Replication Nodes.
3. Increase the *servicerange* parameter to account for the additional ports required by the Replication Nodes.

The value defaults to the number of *storagedir* parameters if they were specified. Otherwise the value defaults to "1". "1" is used as the capacity by the examples in this book.

- *storagedir*

A path to the directory that will contain the environment associated with a Replication Node. For capacity values greater than one, multiple *storagedir* parameters must be specified, one for each Replication Node that will be hosted on the Storage Node. It is best if each directory path resolves to a separate disk. This is typically accomplished via suitable entries in */etc/fstab* that attach the file system on a disk to an appropriate location in the overall directory hierarchy. Placing each environment on a distinct disk ensures that the shards are not competing for I/O resources. It also isolates the impact of a disk failure to a single environment.

In the absence of explicit directory arguments the environments are located under the *KVROOT* directory.

- *storagedirsize*

The size for each storage directory. This is optional. If no size is specified, then data is evenly distributed across all shards. However, if you are performing an installation in an heterogeneous environment where some hardware has more storage capacity than other hardware, then use of this parameter will cause more data to be stored on shards that have more storage capacity.

It is an error to specify a storage directory size for some, but not all, storage directories.

For more information, see [Managing Storage Directory Sizes \(page 77\)](#).

- *num_cpus*

The total number of processors on the machine available to the Replication Nodes. It is used to coordinate the use of processors across Replication Nodes. If the value is 0, the system will attempt to query the Storage Node to determine the number of processors on the machine. This value defaults to "0". "0" numCPUs is used by the examples in this book.

This is an optional parameter.

- *memory_mb*

The total number of megabytes of memory that is available in the machine. It is used to guide the specification of the Replication Node's heap and cache sizes. This calculation

becomes more critical if a Storage Node hosts multiple Replication Nodes, and must allocate memory between these processes. If the value is 0, the store will attempt to determine the amount of memory on the machine, but that value is only available when the JVM used is the Oracle Hotspot JVM. The default value is "0". "0" is used by the examples in this book.

- *force*

Optionally specified to force generating the boot configuration files even if boot config verification finds any invalid parameters.

Steps to Configure KVSTORE Installation

Once you have determined the above information (see [Installation Configuration \(page 3\)](#)), you can configure the KVSTORE by following the steps below:

1. Create the initial "boot config" configuration file using the makebootconfig utility. You should do this on each Oracle NoSQL Database node.

Note

Boot config verification is integrated, which checks and validates all the parameters of makebootconfig against the environment before generating the boot configuration files. Optionally use the -force flag to bypass verification and generate the boot configuration files.

To create the "boot config" file, issue the following commands:

```
> mkdir -p KVRROOT      (if it does not already exist)
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar makebootconfig -root KVRROOT \
                                     -port 5000 \
                                     -host <hostname> \
                                     -hrange 5010,5020 \
                                     -capacity 1 \
                                     -num_cpus 0 \
                                     -memory_mb 0
```

For more information about makebootconfig command, see *Configuring Security with Makebootconfig* section in the *Oracle NoSQL Database Security Guide*.

2. Use the securityconfig tool to create the security directory (also creates security related files):

```
java -Xmx256m -Xms256m
-jar KVHOME/lib/kvstore.jar
securityconfig \
config create -root KVRROOT -kspwd (*****)
Created files
KVRROOT/security/security.xml
KVRROOT/security/store.keys
KVRROOT/security/store.trust
```

```
KVROOT/security/client.trust
KVROOT/security/client.security
KVROOT/security/store.passwd (Generated in CE version)
KVROOT/security/store.wallet/cwallet.sso (Generated in EE version)
Created
```

For more information, see *Configuring Security with Securityconfig* section in the *Oracle NoSQL Database Security Guide*.

Note

If multiple SNAs are configured, after you run `makebootconfig` on each SNA, copy the security directory to the KVROOT of each Oracle NoSQL Database Storage Node Agent (SNA).

```
scp -r KVROOT/security NODE:KVROOT/
```

3. Start the Oracle NoSQL Database Storage Node Agent (SNA) on each of the Oracle NoSQL Database nodes. The SNA manages the Oracle NoSQL Database processes on each node. It also owns and manages the registry port, which is the main way to communicate with Oracle NoSQL Database processes on that node. You can use the `start` utility for this:

```
nohup java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar start -root KVROOT &
```

Note

If the Replication Node or the Admin Service crashes, the SNA ensures that the processes restart.

4. Verify that the Oracle NoSQL Database processes are running using the `jps -m` command:

```
> jps -m
29400 ManagedService -root /tmp -class Admin -service
BootstrapAdmin.13250 -config config.xml
29394 StorageNodeAgentImpl -root /tmp -config config.xml
```

5. Ensure that the Oracle NoSQL Database client library can contact the Oracle NoSQL Database Storage Node Agent (SNA) by using the `ping` command:

```
ssh node01
java -jar KVHOME/lib/kvstore.jar ping -host node01 -port 5000
-security KVROOT/security/client.security

Login as: Anonymous (You can enter any user name here)
Anonymous's password: (Enter any password)

SNA at hostname: node01, registry port: 5000 is not registered.
No further information is available
Can't find store topology:
Could not contact any RepNode at: [node01:5000]
```

This message is not an error, but instead it is telling you that only the SN process is running on the local host. Once Oracle NoSQL Database is fully configured, the ping option will provide more details. If the SNA cannot be contacted, you see this instead:

```
Unable to connect to the storage node agent at host node01,  
port 5000, which may not be running; nested exception is:  
  
java.rmi.ConnectException: Connection refused to host: node01;  
nested exception is:  
java.net.ConnectException: Connection refused  
Can't find store topology:  
Could not contact any RepNode at: [node01:5000]
```

If the Storage Nodes do not start up, you can look through the adminboot and snaboot logs in the KVROOT directory to identify the problem.

Note

If you have not completed the steps in the [Configuring Security with Remote Access \(page 19\)](#), then the ping command for a secure store is only available locally.

Assuming the Storage Nodes have all started successfully, you can configure the KVStore. For more information on how to configure the KVSTORE, see [Configuring the KVStore \(page 12\)](#).

Note

For best results, you should configure your nodes such that the SNA starts automatically when your node boots up. How this is done is a function of how your operating system is designed, and so is beyond the scope of this manual. See your operating system documentation for information on automatic application launch at bootup.

Configuring the Firewall

To make sure your firewall works with Oracle NoSQL Database, you should set the ports specified by the `servicerange` parameter of the `makebootconfig` command. This parameter is used to constrain a store to a limited set of ports, usually for security or data center policy reasons. By default the services use anonymous ports.

Additionally, the port specified by `-port` parameter of the `makebootconfig` command need to be available as well.

The format of the value string is "startPort,endPort." The value varies with the capacity of the Storage Node.

For more information about the `servicePortRange` and determining its sizing, see [Storage Node Parameters \(page 94\)](#).

Chapter 2. Plans

This chapter describes plans, which are useful to perform the configuration of your store. If you are installing a store for the first time, you can skip ahead to the next chapter [Configuring the KVStore \(page 12\)](#).

You configure Oracle NoSQL Database with administrative commands called *plans*. A plan is made up of multiple operations. Plans may modify state managed by the Admin service, and may issue requests to kvstore components such as Storage Nodes and Replication Nodes. Some plans are simple state-changing operations, while others may be long-running operations that affect every node in the store over time.

For example, you use a plan to create a zone or a Storage Node or to reconfigure the parameters on a Replication Node.

Using Plans

You create and execute plans using the `plan` command in the administrative command line interface. By default, the command line prompt will return immediately, and the plan will execute asynchronously, in the background. You can check the progress of the plan using the `show plan id` command.

If you use the optional `-wait` flag for the `plan` command, the plan will run synchronously, and the command line prompt will only return when the plan has completed. The `plan wait` command can be used for the same purpose, and also lets you specify a time period. The `-wait` flag and the `plan wait` command are particularly useful when issuing plans from scripts, because scripts often expect that each command is finished before the next one is issued.

You can also create, but defer execution of the plan by using the optional `-noexecute` flag. If `-noexecute` is specified, the plan can be run later using the `plan execute -id <id>` command.

Feedback While a Plan is Running

There are several ways to track the progress of a plan.

- The `show plan -id` command provides information about the progress of a running plan. Note that the `-verbose` optional plan flag can be used to get more detail.
- You can issue the `verify` command using the Topology tab or the CLI as plans are executing. The `verify plan` provides service status information as services come up.

Note

The Topology tab and `verify` command are really only of interest for topology-related plans. For example, if the user is modifying parameters, the changes may not be visible via the topology tab or `verify` command.

- You can follow the store-wide log using the CLI's `logtail` command.

Plan States

Plans can be in these states:

Name	Description
APPROVED	The plan has been created, but is not yet running.
CANCELED	An INTERRUPTED or ERROR plan has been terminated using the CLI. To cancel a plan using the CLI, use the <code>cancel</code> command.
ERROR	A RUNNING plan has encountered a problem, and has ended without successfully completing.
INTERRUPTED	A RUNNING plan has been manually interrupted, using the <code>interrupt</code> command in the CLI.
INTERRUPT REQUESTED	A plan has been manually interrupted, but is still processing the interrupt request. A plan may have to cleanup or reverse steps taken during plan execution to be sure that the store remains in a consistent state.
RUNNING	The plan is currently executing.
SUCCEEDED	The plan has completed successfully.

Plans in INTERRUPTED, INTERRUPT REQUESTED or ERROR state can be retried using the `plan execute` command. Retrying may be an appropriate approach when the underlying problem was transient or has been rectified. Plans that are retried simply re-execute the same steps. Each step is idempotent, and can be safely repeated.

Note that Storage Nodes and Replication Nodes may encounter errors which are displayed in an error dialog before the plan has processed the information. The plan eventually sees the error and transitions to an ERROR state.

Reviewing Plans

You can find out what state a plan is in using the `show plans` command in the CLI. Use the `show plan -id <plan number>` command to see more details on that plan.

You can review the execution history of a plan by using the CLI `show plan` command. (How to use the CLI is described in detail in [Configuring the KVStore \(page 12\)](#).)

This example shows the output of the `show plan` command. The plan name, attempt number, started and ended date, status, and the steps, or tasks that make up the plan are displayed. In this case, the plan was executed once. The plan completed successfully.

```
kv-> show plan
1 Deploy KVLite          SUCCEEDED
```

```
2 Deploy Storage Node SUCCEEDED
3 Deploy Admin Service SUCCEEDED
4 Deploy KVStore SUCCEEDED
kv-> show plan -id 3
Plan Deploy Admin Service (3)
Owner: null
State: SUCCEEDED
Attempt number: 1
Started: 2012-11-22 22:05:31 UTC
Ended: 2012-11-22 22:05:31 UTC
Total tasks: 1
Successful: 1
```

Plan Ownership

In a secure Oracle NoSQL Database deployment, each plan command is associated with its creator as the owner. Only the owner of a plan can see and operate it. If a plan is created in an earlier version of Oracle NoSQL Database or in a non secure store, the owner is null.

Note

The SYSOPER privilege allows a role to perform cancel, execute, interrupt, and wait on any plan.

Users with the SYSVIEW privilege can see plans owned by other users, plans with null owner, and those plans whose owners have been removed from Oracle NoSQL Database.

For more information on configuring Oracle NoSQL Database securely and on roles, see the *Oracle NoSQL Database Security Guide*.

Chapter 3. Configuring the KVStore

Once you have installed Oracle NoSQL Database on each of the nodes that you could use in your store (see [Installing Oracle NoSQL Database \(page 1\)](#)), you must configure the store. To do this, you use the command line administration interface.

To configure your store, you create and then execute *plans*. Plans describe a series of operations that Oracle NoSQL Database should perform for you. You do not need to know what those internal operations are in detail. Instead, you just need to know how to use and execute the plans.

Note

For information on configuring a non-secure store see [Installing and Configuring a Non-secure Store \(page 127\)](#).

Configuration Overview

At a high level, configuring your store requires these steps:

1. [Configure and Start a Set of Storage Nodes \(page 14\)](#)
2. [Name your KVStore \(page 14\)](#)
3. [Create a Zone \(page 14\)](#)
4. [Create an Administration Process on a Specific Host \(page 16\)](#)
5. [Create a Storage Node Pool \(page 17\)](#)
6. [Create the Remainder of your Storage Nodes \(page 18\)](#)
7. [Create and Deploy Replication Nodes \(page 18\)](#)
8. [Configuring Security with Remote Access \(page 19\)](#)

You perform all of these activities using the Oracle NoSQL Database command line interface (CLI). The remainder of this chapter shows you how to perform these activities. Examples are provided that show you which commands to use, and how. For a complete listing of all the commands available to you in the CLI, see [CLI Command Reference \(page 130\)](#).

Start the Administration CLI

Note

You must follow the configuration steps as mentioned in [Steps to Configure KVSTORE Installation \(page 6\)](#) before running the Admin CLI.

To perform store configuration, you use the runadmin utility, which provides a command line interface (CLI). The runadmin utility can be used for a number of purposes. In this chapter, we use it to administer the nodes in our store, so we must tell runadmin what node and registry port it can use to connect to the store.

In this book, we use 5000 as the registry port. For these examples, we use the string node01 to represent the network name of the node to which runadmin connects.

Note

You should think about the name of the node to which the runadmin connects. The node used for initial configuration of the store, during store creation, cannot be changed.

The most important thing about this node is that it must have the Storage Node Agent running on it. All your nodes should have an SNA running on them at this point. If not, you need to follow the instructions in [Installing Oracle NoSQL Database \(page 1\)](#) before proceeding with the steps provided in this chapter.

Beyond that, be aware that if this is the very first node you have ever connected to the store using the CLI, then it becomes the node on which the master copy of the administration database resides. If you happen to care about which node serves that function, then make sure you use that node at this time.

To start runadmin for administration purposes:

```
ssh node01
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar runadmin \
-port 5000 -host node01 \
-security KVR00T/security/client.security
```

Note

If you have not completed the steps in the [Configuring Security with Remote Access \(page 19\)](#), then the runadmin command for a secure store is only available locally.

Note that once you have started the CLI, you can use its help command in order to discover all the administration commands available to you.

Also note that the configuration steps described in this chapter can be collected into a script file, and then that file can be passed to the utility using its -script command line option. See [Using a Script to Configure the Store \(page 28\)](#) for more information.

The plan Commands

Some of the steps described in this chapter make heavy use of the CLI's plan command. This command identifies a configuration action that you want to perform on the store. You can either run that action immediately or you can create a series of plans with the -noexecute flag and then execute them later by using the plan execute command.

You can list all available plans by using the plan command without arguments.

For a high-level description of plans, see [Plans \(page 9\)](#).

Configure and Start a Set of Storage Nodes

You should already have configured and started a set of Storage Nodes to host the KVStore cluster. If not, you need to follow the instructions in [Installing Oracle NoSQL Database \(page 1\)](#) before proceeding with this step.

Name your KVStore

When you start the command line interface, the `kv->` prompt appears. Once you see this, you can name your KVStore by using the `configure -name` command. The only information this command needs is the name of the KVStore that you want to configure.

Note that the name of your store is essentially used to form a path to records kept in the store. For this reason, you should avoid using characters in the store name that might interfere with its use within a file path. The command line interface does not allow an invalid store name. Valid characters are alphanumeric, '-', '_', and '.'.

For example:

```
kv-> configure -name mystore
Store configured: mystore
```

Note

The store name must be unique across all instances of NoSQL Database that will be monitored by a given instance of Enterprise Manager. For more information, see [Store Targets \(page 119\)](#).

Create a Zone

Once you have started the command line interface and configured a store name, you can create at least one zone. It is possible, and even desirable, to create more than one zone. Multiple zones are used to improve the availability of your store. These instructions describe the installation using a single zone. For a complete walk-through of a store deployment with multiple zones, see [Configuring with Multiple Zones \(page 20\)](#).

Note

Once you have added Storage Nodes to a zone, you cannot remove the zone from your store.

The usage is:

```
plan deploy-zone -name <zone name>
-rf <replication factor>
[-type [primary | secondary]]
[-arbiters | -no-arbiters ]
[-json ]
[-plan-name <name>] [-wait] [-noexecute] [-force]
```

where:

- `-arbiters`

If specified, Arbiter Nodes may be allocated on the Storage Node in the zone. This flag can only be specified on a primary zone.

- `-name`

A string to identify the name of the zone.

- `-no-arbiters`

If specified, Arbiter Nodes cannot be allocated on the Storage Node in the zone. This flag can only be specified on a primary zone.

- `-rf`

A number specifying the *Zone Replication Factor*.

A primary zone can also have a Replication Factor equal to zero. This type of zone is useful to only host Arbiter Nodes. Zero capacity Storage Nodes would be added to this zone in order to host the Arbiter Nodes.

Note

Only primary zones can host Arbiter Nodes.

- `-type`

Specifies the type of zone to create. If not specified, a Primary zone is created.

When you execute the `plan deploy-zone` command, the CLI returns the plan number and whatever additional information it has about plan status.

For more information on Primary and Secondary Replication Factors, see [Configuring with Multiple Zones \(page 20\)](#).

When you execute the `plan deploy-zone` command, the CLI returns the plan number. It also returns instructions on how to check the plan's status, or to wait for it to complete. For example:

```
kv-> plan deploy-zone -name "Boston" -rf 3 -wait
Executed plan 1, waiting for completion...
Plan 1 ended successfully
```

You can show the plans and their status by using the `show plans` command.

```
kv-> show plans
1 Deploy Zone (1)          SUCCEEDED
```

A zone may also have a Replication Factor equal to zero. This type of zone is useful to only host Arbiter Nodes. Zero capacity Storage Nodes would be added to this zone in order to host Arbiter Nodes. For more information see [Deploying an Arbiter Node Enabled Topology \(page 45\)](#).

Create an Administration Process on a Specific Host

Every KVStore has an administration database. You must deploy the Storage Node to which the command line interface is currently connecting to, in this case, "node01", and then deploy an Administration process on that same node, in order to proceed to configure this database. Use the `deploy-sn` and `deploy-admin` commands to complete this step.

The `deploy-admin` command will create an Administration process which is the same type as the zone the Storage Node is in. If the zone is primary, the admin will be a primary admin. If the zone is secondary, the admin will be a secondary admin. Secondary admins are needed to support failover, where a failed admin will be converted to an offline secondary in order to reestablish quorum using existing admins, and a secondary admin converted to a primary to take over for failed primaries. For more information on quorum, see the Oracle NoSQL Database Concepts manual.

To support failover, you must make sure that any zones that will be used to continue the operation of the store after a failure contain at least one admin node.

Note

A deployed admin must be the same type (PRIMARY/SECONDARY) as the zone they are in. Also, the number of admins deployed in a zone should be equal to the zone's Replication Factor.

Note that `deploy-sn` requires you to provide a zone ID. You can get this ID by using the `show topology` command:

```
kv-> show topology
store=mystore numPartitions=0 sequence=1
zn: id=zn1 name=Boston repFactor=3 type=PRIMARY allowArbiters=false
```

The zone ID is "zn1" in the above output.

When you deploy the node, provide the zone ID, the node's network name, and its registry port number. For example:

```
kv-> plan deploy-sn -zn zn1 -host node01 -port 5000 -wait
Executed plan 2, waiting for completion...
Plan 2 ended successfully
```

Having done that, create the administration process on the node that you just deployed. You do this using the `deploy-admin` command. This command requires the Storage Node ID (which you can obtain using the `show topology` command) and an optional plan name.

```
kv-> plan deploy-admin -sn sn1 -wait
Executed plan 3, waiting for completion...
Plan 3 ended successfully
```

Note

At this point you have a single administration process deployed in your store. This is enough to proceed with store configuration. However, to increase your store's

reliability, you should deploy multiple administration processes, each running on a different storage node. In this way, you are able to continue to administer your store even if one Storage Node becomes unreachable, taking an administration process with it. It also means that you can continue to monitor your store, even if you lose a node running an administration process.

Oracle strongly recommends that you deploy three administration processes for a production store. The additional administration processes do not consume many resources.

Before you can deploy any more administration processes, you must first deploy the rest of your Storage Nodes. This is described in the following sections.

Create a Storage Node Pool

Once you have created your Administration process, you can create a Storage Node Pool. This pool is used to contain all the Storage Nodes in your store. A Storage Node pool is used for resource distribution when creating or modifying a store. You use the `pool create` command to create this pool. Then you join Storage Nodes to the pool using the `pool join` command.

Note that a default pool called `AllStorageNodes` will be created automatically and all SNs will be added to it during the topology deployment process. Therefore, the `pool` commands are optional if you use the `AllStorageNodes` pool as the default pool during deployment.

Note

You may have multiple kinds of storage nodes in different zones that vary by processor type, speed and/or disk capacity. So the storage node pool lets you define a logical grouping of storage nodes by whatever specification you pick.

Remember that we already have a Storage Node created. We did that when we created the Administration process. Therefore, after we add the pool, we can immediately join that first SN to the pool.

The `pool create` command only requires you to provide the name of the pool.

The `pool join` command requires the name of the pool to which you want to join the Storage Node, and the Storage Node's ID. You can obtain the Storage Node's ID using the `show topology` command.

For example:

```
kv-> pool create -name BostonPool
Added pool BostonPool

kv-> show topology
store=mystore numPartitions=0 sequence=2
zn: id=zn1 name=Boston repFactor=3 type=PRIMARY allowArbiters=false
sn=[sn1] zn:[id=zn1 name=Boston] slc09kuu:5000 capacity=1 RUNNING

kv-> pool join -name BostonPool -sn sn1
```

```
Added Storage Node(s) [sn1] to pool BostonPool
```

Create the Remainder of your Storage Nodes

Having created your Storage Node Pool, you can create the remainder of your Storage Nodes. Storage Nodes host the various Oracle NoSQL Database processes for each of the nodes in the store. Consequently, you must do this for each node that you use in your store. Use the `deploy-sn` command in the same way as you did in [Create an Administration Process on a Specific Host \(page 16\)](#). As you deploy each Storage Node, join it to your Storage Node Pool as described in the previous section.

Hint: Storage Node IDs increase by one as you add each Storage Node. Therefore, you do not have to keep looking up the IDs with `show topology`. If the Storage Node that you created last had an ID of 10, then the next Storage Node that you create has an ID of 11.

```
kv-> plan deploy-sn -zn zn1 -host node02 -port 5000 -wait
Executed plan 4, waiting for completion...
Plan 4 ended successfully
kv-> pool join -name BostonPool -sn sn2
Added Storage Node(s) [sn2] to pool BostonPool
kv-> plan deploy-sn -zn zn1 -host node03 -port 5000 -wait
Executed plan 5, waiting for completion...
Plan 5 ended successfully
kv-> pool join -name BostonPool -sn sn3
Added Storage Node(s) [sn3] to pool BostonPool
kv->
....
```

Continue this process until you have created Storage Nodes on every node in your store.

Note

Having deployed all your Storage Nodes, you can now deploy additional administration processes using the `deploy-admin` plan. See [Create an Administration Process on a Specific Host \(page 16\)](#) for details.

Create and Deploy Replication Nodes

The final step in your configuration process is to create Replication Nodes on every node in your store. You do this using the `topology create` and `plan deploy-topology` commands in its place. The `topology create` command takes the following arguments:

- *topology name*
A string to identify the topology.
- *pool name*
A string to identify the pool.
- *number of partitions*

The initial configuration is based on the storage nodes specified by pool. This number is fixed once the topology is created and it cannot be changed. The command will automatically create an appropriate number of shards and replication nodes based upon the storage nodes in the pool.

You should make sure the number of partitions you select is more than the largest number of shards you ever expect your store to contain, because the total number of partitions is static and cannot be changed. For simpler use cases, you can use the following formula to arrive at a very rough estimate for the number of partitions:

```
(Total number of disks hosted by the storage nodes \
Replication Factor) * 10
```

To get a more accurate estimate for production use see [Number of Partitions \(page 215\)](#).

The plan `deploy-topology` command requires a topology name.

Once you issue the following commands, your store is fully installed and configured:

```
kv-> topology create -name topo -pool BostonPool -partitions 300
Created: topo
kv-> plan deploy-topology -name topo -wait
Executed plan 6, waiting for completion...
Plan 6 ended successfully
```

As a final sanity check, you can confirm that all of the plans succeeded using the `show plans` command:

```
kv-> show plans
1 Deploy Zone (1)          SUCCEEDED
2 Deploy Storage Node (2)  SUCCEEDED
3 Deploy Admin Service (3) SUCCEEDED
4 Deploy Storage Node (4)  SUCCEEDED
5 Deploy Storage Node (5)  SUCCEEDED
6 Deploy-RepNodes          SUCCEEDED
```

Having done that, you can exit the command line interface.

```
kv-> exit
```

Configuring Security with Remote Access

To configure security with remote access, see the following steps:

- Create the first admin user. See:

```
kv->execute 'CREATE USER admin IDENTIFIED BY "NoSql@+123" ADMIN'
```

- Grant readwrite role to the first admin user. See:

```
kv->execute "GRANT readwrite TO USER admin"
```

- Make a admin user security directory for remote access. See:

```
ssh CLIENT_HOST mkdir USER/security
```

- Copy the SSL trust file from the server node:

```
scp node01:KVR00T/security/client.trust USER/security/
```

- Generate a password store for the first admin user. This step will create admin.passwd file in USER/security directory. You can also copy the admin.passwd from other machines to USER/security directory if the file has not been created locally. For the commands to create admin.passwd, see:

```
java -jar KVHOME/lib/kvstore.jar  
securityconfig \  
pwdfile create -file USER/security/admin.passwd  
  
java -jar KVHOME/lib/kvstore.jar securityconfig \  
pwdfile secret \  
-file USER/security/admin.passwd -set -alias admin -secret NoSql@+123
```

- Create a admin user login file as USER/security/admin.security, add below information. See:

```
oracle.kv.auth.username=admin  
oracle.kv.auth.pwd.file=USER/security/admin.passwd  
oracle.kv.transport=ssl  
oracle.kv.ssl.trustStore=USER/security/client.trust
```

- Access the store remotely. See:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar runadmin \  
-port 5000 -host node01 \  
-security USER/security/admin.security
```

Configuring with Multiple Zones

Optimal use of available physical facilities is achieved by deploying your store across multiple zones. This provides fault isolation and availability for your data if a single zone fails. Each zone has a copy of your complete store, including a copy of all the shards. With this configuration, reads are always possible, so long as your data's consistency guarantees can be met, because at least one replica is located in every zone. Writes can also occur in the event of a zone loss so long as quorum can be maintained. For more information on quorum, see the Oracle NoSQL Database Concepts manual.

You can specify a different replication factor to each zone. A replication factor can then be quantified as one of the following:

- *Zone Replication Factor*

The number of copies, or replicas, maintained in a zone.

- *Primary Replication Factor*

The total number of replicas in all primary zones. This replication factor controls the number of replicas that participate in elections and acknowledgments. For additional

information on how to identify the *Primary Replication Factor* and its implications, see [Replication Factor \(page 208\)](#).

- *Secondary Replication Factor*

The total number of replicas in all secondary zones. Secondary replicas provide additional read-only copies of the data.

- *Store Replication Factor*

Represents for all zones in the store, the total number of replicas across the entire store.

Zones located nearby have the benefit of avoiding bottlenecks due to throughput limitations, as well as reducing latency during elections and commits.

Note

Zones come in two types. *Primary* zones contain nodes which can serve as masters or replicas. Zones are created as primary Zones by default. For good performance, primary zones should be connected by low latency networks so that they can participate efficiently in master elections and commit acknowledgments.

Secondary zones contain nodes which can only serve as replicas. Secondary zones can be used to provide low latency read access to data at a distant location, or to maintain an extra copy of the data to increase redundancy or increase read capacity. Because the nodes in secondary zones do not participate in master elections or commit acknowledgments, secondary zones can be connected to other zones by higher latency networks, because additional latency will not interfere with those time critical operations.

Using high throughput and low latency networks to connect primary zones leads to better results and improved performance. You can use networks with higher latency to connect to secondary zones so long as the connections provide sufficient throughput to support replication and sufficient reliability that temporary interruptions do not interfere with network throughput.

Note

Because any primary zone can host master nodes, write performance may be reduced if primary zones are connected through a limited throughput and/or high latency network link.

The following steps walk you through the process of deploying six Storage Nodes across three primary zones. You can then verify that each shard has a replica in every zone; service can be continued in the event of a zone failure.

1. For a new store, create the initial "boot config" configuration files using the makebootconfig utility:

```
java -jar kv/lib/kvstore.jar makebootconfig \  
-root Data/virtualroot/datacenter1/KVR00T \
```



```

-host localhost \
-port 5000 \
-harange 5010,5020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root Data/virtualroot/datacenter2/KVROOT \
-host localhost \
-port 6000 \
-harange 6010,6020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root Data/virtualroot/datacenter3/KVROOT \
-host localhost \
-port 7000 \
-harange 7010,7020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root Data/virtualroot/datacenter4/KVROOT \
-host localhost \
-port 8000 \
-harange 8010,8020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root Data/virtualroot/datacenter5/KVROOT \
-host localhost \
-port 9000 \
-harange 9010,9020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root Data/virtualroot/datacenter6/KVROOT \
-host localhost \
-port 10000 \
-harange 10010,10020 \
-capacity 1

```

2. Create and copy the security directory as below:

```

java -jar kv/lib/kvstore.jar securityconfig config create \
-root Data/virtualroot/datacenter1/KVROOT -kspwd NoSql@+123
Created files
Data/virtualroot/datacenter1/KVROOT/security/security.xml
Data/virtualroot/datacenter1/KVROOT/security/store.keys
Data/virtualroot/datacenter1/KVROOT/security/store.trust
Data/virtualroot/datacenter1/KVROOT/security/client.trust
Data/virtualroot/datacenter1/KVROOT/security/client.security

```

```
Data/virtualroot/datacenter1/KVROOT/security/store.passwd  
(Generated in CE version)  
Data/virtualroot/datacenter1/KVROOT/security/store.wallet/cwallet.sso  
(Generated in EE version)
```

Created

```
cp -r Data/virtualroot/datacenter1/KVROOT/security \  
Data/virtualroot/datacenter2/KVROOT/  
cp -r Data/virtualroot/datacenter1/KVROOT/security \  
Data/virtualroot/datacenter3/KVROOT/  
cp -r Data/virtualroot/datacenter1/KVROOT/security \  
Data/virtualroot/datacenter4/KVROOT/  
cp -r Data/virtualroot/datacenter1/KVROOT/security \  
Data/virtualroot/datacenter5/KVROOT/  
cp -r Data/virtualroot/datacenter1/KVROOT/security \  
Data/virtualroot/datacenter6/KVROOT/
```

3. Using each of the configuration files, start all of the Storage Node Agents:

```
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root Data/virtualroot/datacenter1/KVROOT &  
> [1] 12019  
  
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root -root Data/virtualroot/datacenter2/KVROOT &  
> [2] 12020  
  
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root -root Data/virtualroot/datacenter3/KVROOT &  
> [3] 12021  
  
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root -root Data/virtualroot/datacenter4/KVROOT &  
> [4] 12022  
  
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root -root Data/virtualroot/datacenter5/KVROOT &  
> [5] 12023  
  
> nohup java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar \  
start -root -root Data/virtualroot/datacenter6/KVROOT &  
> [6] 12024
```

4. Start the CLI:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar runadmin -host \  
localhost -port 5010 \  
-security Data/virtualroot/datacenter1/KVROOT/security/client.security  
kv->
```

5. Name your store:

```
kv-> configure -name MetroArea  
Store configured: MetroArea
```

6. Deploy the first Storage Node with administration process in the Manhattan zone:

```
kv-> plan deploy-zone -name Manhattan -rf 1 -wait  
Executed plan 1, waiting for completion...  
Plan 1 ended successfully  
kv-> plan deploy-sn -zn 1 -host localhost -port 5000 -wait  
Executed plan 2, waiting for completion...  
Plan 2 ended successfully  
kv-> plan deploy-admin -sn sn1 -wait  
Executed plan 3, waiting for completion...  
Plan 3 ended successfully  
kv-> pool create -name SNs  
Added pool SNs  
kv-> pool join -name SNs -sn sn1  
Added Storage Node(s) [sn1] to pool SNs
```

7. Deploy a second Storage Node in Manhattan zone:

```
kv-> plan deploy-sn -znname Manhattan -host localhost \  
-port 6000 -wait  
kv-> Executed plan 4, waiting for completion...  
Plan 4 ended successfully  
kv-> pool join -name SNs -sn sn2  
Added Storage Node(s) [sn2] to pool SNs
```

8. Deploy the first Storage Node with administration process in the Jersey City zone:

```
kv-> plan deploy-zone -name JerseyCity -rf 1 -wait  
Executed plan 5, waiting for completion...  
Plan 5 ended successfully  
kv-> plan deploy-sn -znname JerseyCity -host localhost \  
-port 7000 -wait  
Executed plan 6, waiting for completion...  
Plan 6 ended successfully  
kv-> plan deploy-admin -sn sn3 -wait  
Executed plan 7, waiting for completion...  
Plan 7 ended successfully  
kv-> pool join -name SNs -sn sn3  
Added Storage Node(s) [sn3] to pool SNs
```

9. Deploy a second Storage Node in Jersey City zone:

```
kv-> plan deploy-sn -znname JerseyCity -host localhost \
-port 8000 -wait
kv-> Executed plan 8, waiting for completion...
Plan 8 ended successfully
kv-> pool join -name SNs -sn sn4
Added Storage Node(s) [sn4] to pool SNs
```

10. Deploy the first Storage Node with administration process in the Queens zone:

```
kv-> plan deploy-zone -name Queens -rf 1 -wait
Executed plan 9, waiting for completion...
Plan 9 ended successfully
kv-> plan deploy-sn -znname Queens -host localhost -port 9000 -wait
Executed plan 10, waiting for completion...
Plan 10 ended successfully
kv-> plan deploy-admin -sn sn5 -wait
Executed plan 11, waiting for completion...
Plan 11 ended successfully
kv-> pool join -name SNs -sn sn5
Added Storage Node(s) [sn5] to pool SNs
```

11. Deploy a second Storage Node in Queens zone:

```
kv-> plan deploy-sn -znname Queens -host localhost \
-port 10000 -wait
kv-> Executed plan 12, waiting for completion...
Plan 12 ended successfully
kv-> pool join -name SNs -sn sn6
Added Storage Node(s) [sn6] to pool SNs
```

12. Create and deploy a topology:

```
kv-> topology create -name Topo1 -pool SNs -partitions 100
Created: Topo1
kv-> plan deploy-topology -name Topo1 -wait
kv-> Executed plan 13, waiting for completion...
Plan 13 ended successfully
```

13. Check service status with the show topology command:

```
kv-> show topology
store=MetroArea numPartitions=100 sequence=117
zn: id=zn1 name=Manhattan repFactor=1 type=PRIMARY allowArbiters=false
zn: id=zn2 name=JerseyCity repFactor=1 type=PRIMARY allowArbiters=false
zn: id=zn3 name=Queens repFactor=1 type=PRIMARY allowArbiters=false

sn=[sn1] zn=[id=zn1 name=Manhattan] node01:5000 capacity=1 RUNNING
[rg1-rn2] RUNNING
No performance info available
sn=[sn2] zn=[id=zn1 name=Manhattan] node02:6000 capacity=1 RUNNING
[rg2-rn2] RUNNING
```

```

    No performance info available
sn=[sn3] zn=[id=zn2 name=JerseyCity] node03:7000 capacity=1 RUNNING
  [rg1-rn3] RUNNING
    No performance info available
sn=[sn4] zn=[id=zn2 name=JerseyCity] node04:8000 capacity=1 RUNNING
  [rg2-rn3] RUNNING
    No performance info available
sn=[sn5] zn=[id=zn3 name=Queens] node05:9000 capacity=1 RUNNING
  [rg1-rn1] RUNNING
    No performance info available
sn=[sn6] zn=[id=zn3 name=Queens] node06:10000 capacity=1 RUNNING
  [rg2-rn1] RUNNING
    No performance info available

shard=[rg1] num partitions=50
  [rg1-rn1] sn=sn5
  [rg1-rn2] sn=sn1
  [rg1-rn3] sn=sn3
shard=[rg2] num partitions=50
  [rg2-rn1] sn=sn6
  [rg2-rn2] sn=sn2
  [rg2-rn3] sn=sn4

```

14. Verify that each shard has a replica in every zone:

```

kv-> verify configuration
Verify: starting verification of store MetroArea based upon
topology sequence #117
100 partitions and 6 storage nodes
Time: 2015-06-16 00:01:05 UTC   Version: 12.1.3.4.0
See node01:Data/virtualroot/datacenter1/kvroot/MetroArea/
                                log/MetroArea_{0..N}.log for
                                progress messages
Verify: Shard Status: healthy:2 writable-degraded:0
                                read-only:0 offline:0
Verify: Admin Status: healthy
Verify: Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
  RN Status: online:2 offline: 0 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
  RN Status: online:2 offline: 0 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
  RN Status: online:2 offline: 0
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:5000
  Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
  Status: RUNNING
  Ver: 12cR1.3.4.0 2015-05-29 12:09:04 UTC   Build id: db9ec397225c
Verify:      Admin [admin1]      Status: RUNNING,MASTER
Verify:      Rep Node [rg1-rn2]   Status: RUNNING,REPLICA
  sequenceNumber:127 haPort:5011 delayMillis:1 catchupTimeSecs:0

```

```

Verify: == checking storage node sn2 ==
Verify: Storage Node [sn2] on node02:6000
    Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn2]      Status: RUNNING,REPLICA
    sequenceNumber:127 haPort:6010 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:7000
    Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin2]      Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn3]      Status: RUNNING,REPLICA
    sequenceNumber:127 haPort:7011 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn4 ==
Verify: Storage Node [sn4] on node04:8000
    Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn3]      Status: RUNNING,REPLICA
    sequenceNumber:127 haPort:8010 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn5 ==
Verify: Storage Node [sn5] on node05:9000
    Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin3]      Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn1]      Status: RUNNING,MASTER
    sequenceNumber:127 haPort:9011
Verify: == checking storage node sn6 ==
Verify: Storage Node [sn6] on node06:10000
    Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn1]      Status: RUNNING,MASTER
    sequenceNumber:127 haPort:10010

Verification complete, no violations.

```

15. Follow the instructions mentioned in [Configuring Security with Remote Access \(page 19\)](#) to create the access for the user in the multiple zone deploy example.

In the previous example there are three zones (zn1 = Manhattan, zn2 = JerseyCity, zn3=Queens) with six Replication Nodes (two masters and four replicas) in this cluster. This means that this topology is not only highly available because you have three replicas within each shard, but it is also able to recover from a single zone failure. If any zone fails, the other two zones are enough to elect the new master, so service continues without any interruption.

Using a Script to Configure the Store

Note

You must follow the configuration steps as mentioned in [Steps to Configure KVSTORE Installation \(page 6\)](#) before running the Admin CLI.

Up to this point, we have shown how to configure a store using an interactive command line interface session. However, you can collect all of the commands used in the prior sections into a script file, and then run them in a single batch operation. To do this, use the load command in the command line interface. For example:

Using the load -file command line option:

```
ssh node01
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar runadmin -port 5000 -host node01 \
-security \
KVR00T/securtiy/client.security \
load -file script.txt
```

Using directly the load -file command:

```
kv-> load -file <path to file>
```

Using this command you can load the named file and interpret its contents as a script of commands to be executed.

The file, script.txt, would then contain content like this:

```
### Begin Script ###
configure -name mystore
plan deploy-zone -name "Boston" -rf 3 -wait
plan deploy-sn -zn zn1 -host node01 -port 5000 -wait
plan deploy-admin -sn sn1 -wait
pool create -name BostonPool
pool join -name BostonPool -sn sn1
plan deploy-sn -zn zn1 -host node02 -port 6000 -wait
pool join -name BostonPool -sn sn2
plan deploy-sn -zn zn1 -host node03 -port 7000 -wait
pool join -name BostonPool -sn sn3
topology create -name topo -pool BostonPool -partitions 300
plan deploy-topology -name topo -wait
exit
### End Script ###
```

Follow the instructions mentioned in [Configuring Security with Remote Access \(page 19\)](#) to create the access for the user in the multiple zone deploy example.

Smoke Testing the System

There are several things you can do to ensure that your KVStore is up and fully functional.

1. Run the ping command. See:

```

> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar ping -port 5000 \
-host node01 -security
USER/security/admin.security
Pinging components of store mystore based upon topology sequence #316
300 partitions and 3 storage nodes
Time: 2016-11-21 13:40:37 UTC   Version: 12.1.4.3.5
Shard Status: healthy:3 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:9 offline:0 maxDelayMillis:1 maxCatchupTimeSecs:0
Storage Node [sn1] on node01:5000
  Zone [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
  RN Status: online:1 offline:0
  Status: RUNNING
  Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: db9ec397225c
  Admin [admin1]           Status: RUNNING,MASTER
  Rep Node [rg1-rn1]       Status: RUNNING,REPLICA
    sequenceNumber:231 haPort:5011 delayMillis:1 catchupTimeSecs:0
  Rep Node [rg2-rn1]       Status: RUNNING,REPLICA
    sequenceNumber:231 haPort:5012 delayMillis:1 catchupTimeSecs:0
  Rep Node [rg3-rn1]       Status: RUNNING,MASTER
    sequenceNumber:227 haPort:5013
Storage Node [sn2] on node02:6000
  Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
  Status: RUNNING
  Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: db9ec397225c
  Rep Node [rg1-rn2]       Status: RUNNING,MASTER
    sequenceNumber:231 haPort:6010
  Rep Node [rg2-rn2]       Status: RUNNING,REPLICA
    sequenceNumber:231 haPort:6011 delayMillis:1 catchupTimeSecs:0
  Rep Node [rg3-rn2]       Status: RUNNING,REPLICA
    sequenceNumber:227 haPort:6012 delayMillis:1 catchupTimeSecs:0
Storage Node [sn3] on node03:7000
  Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
  Status: RUNNING
  Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: db9ec397225c
  Rep Node [rg1-rn3]       Status: RUNNING,REPLICA
    sequenceNumber:231 haPort:7010 delayMillis:1 catchupTimeSecs:0
  Rep Node [rg2-rn3]       Status: RUNNING,MASTER
    sequenceNumber:231 haPort:7011
  Rep Node [rg3-rn3]       Status: RUNNING,REPLICA
    sequenceNumber:227 haPort:7012 delayMillis:1 catchupTimeSecs:0

```

2. Look through the Javadoc. You can access it from the documentation index page, which can be found at KVHOME/doc/index.html.

If you run into installation problems or want to start over with a new store, then on every node in the system:

1. Stop the node using:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar stop -root KVR00T
```

2. Remove the contents of the KVR00T directory:

```
rm -rf KVR00T
```

3. Start over with the steps described in [Installation Configuration \(page 3\)](#).

Troubleshooting

Typical errors when bringing up a store are typos and misconfiguration. It is also possible to run into network port conflicts, especially if the deployment failed and you are starting over. In that case be sure to remove all partial store data and configuration and kill any remnant processes. Processes associated with a store as reported by "jps -m" are one of these:

```
kvstore.jar start -root KVR00T (SNA process)  
ManagedService
```

If you kill the SNA process it should also kill its managed processes.

There are detailed log files available in KVR00T/storename/log as well as logs of the bootstrap process in KVR00T/*.log. The bootstrap logs are most useful in diagnosing initial startup problems. The logs in storename/log appear once the store has been configured. The logs on the host chosen for the admin process are the most detailed and include a store-wide consolidated log file: KVR00T/storename/log/storename_*.log

Each line in a log file is prefixed with the date of the message, its severity, and the name of the component which issued it. For example:

```
2012-10-25 14:28:26.982 UTC INFO [admin1]  
Initializing Admin for store: kvstore
```

When looking for more context for events at a given time, use the timestamp and component name to narrow down the section of log to peruse.

Error messages in the logs show up with "SEVERE" in them so you can grep for that if you are troubleshooting. SEVERE error messages are also displayed in the CLI's show events command, and when you use the ping command.

In addition to log files, these directories may also contain *.perf files, which are performance files for the Replication Nodes.

In general, verify configuration is the tool of choice for understanding the state of the cluster. In addition to contacting the components, it will cross check each component's parameters against the Admin database. For example, verify configuration might report that a Replication Node's helperHosts parameter was at odds with the Admin. If this were the case then it might explain why a Replication Node cannot come up. Verify configuration also checks on Admins. It also verifies the configuration of Arbiter Nodes in the topology.

Additionally, in order to catch configuration errors early, you can use the diagnostics tool when troubleshooting your KVStore. Also, you can use this tool to package important information and files to be able to send them to Oracle Support, for example. For more information, see [Diagnostics Utility \(page 226\)](#)

Where to Find Error Information

As your store operates, you can discover information about any problems that may be occurring by looking at the plan history and by looking at error logs.

The plan history indicates if any configuration or operational actions you attempted to take against the store encountered problems. This information is available as the plan executes and finishes. Errors are reported in the plan history each time an attempt to run the plan fails. The plan history can be seen using the CLI `show plan` command.

Other problems may occur asynchronously. You can learn about unexpected failures, service downtime, and performance issues through the CLI's `show events` command. Events come with a time stamp, and the description may contain enough information to diagnose the issue. In other cases, more context may be needed, and the administrator may want to see what else happened around that time.

The store-wide log consolidates logging output from all services. Browsing this file might give you a more complete view of activity during the problem period. It can be viewed using the CLI's `logtail` command, or by directly viewing the `<storename>_N.log` file in the `<KVHOME>/<storename>/log` directory.

Service States

Oracle NoSQL Database uses four different types of services, all of which should be running correctly in order for your store to be in a healthy state. The four service types are the Admin, Storage Nodes, Replication Nodes and Arbiters Nodes. You should have multiple instances of these services running throughout your store.

Each service has a status that can be viewed using any of the following:

- The `show topology` command in the Administration CLI.
- Using the `ping` command.

The status values can be one of the following:

Name	Description
ERROR_NO_RESTART	The service is in an error state and is not automatically restarted. Administrative intervention is required.
ERROR_RESTARTING	The service is in an error state. Oracle NoSQL Database attempts to restart the service.
RUNNING	The service is running normally.
STARTING	The service is coming up.

Name	Description
STOPPED	The service was stopped intentionally and cleanly.
STOPPING	The service is stopping. This may take some time as some services can be involved in time-consuming activities when they are asked to stop.
SUCCEEDED	The plan has completed successfully.
UNREACHABLE	The service is not reachable by the Admin. If the status was seen using a command issued by the Admin, this state may mask a STOPPED or ERROR state. If an SN is UNREACHABLE, or an RN is having problems and its SN is UNREACHABLE, the first thing to check is the network connectivity between the Admin and the SN. However, if the managing SNA is reachable and the managed Replication Node is not, we can guess that the network is OK and the problem lies elsewhere.
WAITING_FOR_DEPLOY	The service is waiting for commands or acknowledgments from other services during its startup processing. If it is a Storage Node, it is waiting for the initial deploy-SN command. Other services should transition out of this phase without any administrative intervention from the user.

A healthy service begins with STARTING. It may transition to WAITING_FOR_DEPLOY for a short period before going on to RUNNING.

ERROR_RESTARTING and ERROR_NO_RESTART indicate that there has been a problem that should be investigated. An UNREACHABLE service may only be in that state temporarily, although if that state persists, the service may be truly in an ERROR_RESTARTING or ERROR_NO_RESTART state.

Useful Commands

The following commands may be useful to you when troubleshooting your KVStore.

- `java -Xmx256m -Xms256m \`
`-jar kvstore.tmp/kvstore.jar ping -host node01 -port 5000 \`
`-security USER/security/admin.security`

Reports the status of the store running on the specified host and port. This command can be used against any of the host and port pairs used for Storage Nodes.

- `jps -m`

Reports the Java processes running on a machine. If the Oracle NoSQL Database processes are running, they are reported by this command.

Note

This assumes that you have completed the steps in [Configuring Security with Remote Access \(page 19\)](#).

Chapter 4. Determining Your Store's Configuration

A store consists of a number of Storage Nodes. Each Storage Node can host one or more Replication Nodes, based on its capacity value. The term topology is used to describe the distribution of Replication Nodes. A topology is derived from the number and capacity of available Storage Nodes, the number of partitions in the store, and the replication factors of the store's zones. Topology layouts are also governed by a set of rules that maximize the availability of the store.

All topologies must obey the following rules:

1. Each Replication Node from the same shard must reside on a different Storage Node. This rule prevents a single Storage Node failure from causing multiple points of failure for a single shard.
2. The number of Replication Nodes assigned to a Storage Node must be less than or equal to the capacity of Storage Nodes.
3. A zone must have one or more Replication Nodes from each shard.
4. A valid Arbiter Node distribution is one in which the Arbiter Node is hosted on a Storage Node that does not contain other members of its shard.

The initial configuration, or topology of the store is set when the store is created. Over time, it may be necessary to change the topology of the store. There are several reasons for such a change:

1. You need to replace or upgrade an existing Storage Node.
2. You need to increase read throughput. This is done by increasing the replication factor and creating more copies of the store's data which can be used to service read only requests.
3. You need to increase write throughput. Since each shard has a single master node, distributing the data in the store over a larger number of shards provides the store with more nodes that can execute write operations.

You change the store's configuration by changing the number or capacity of Storage Nodes available, or the replication factor of a zone. To change from one configuration to another, you either create a new initial topology, or you clone an existing topology and modify it into your target topology. You then deploy this target topology.

Note

The deployment of the target topology is potentially a long-running operation and the time required scales with the amount of data that must be moved. During the deployment, the system updates the topology at each step. Because of that, the store passes through intermediate topologies which were not explicitly created by the user.

This chapter discusses how configuration, or topological changes are made in a store. It also describes how to deploy an Arbiter Node enabled topology.

Note

Configuration changes should not be made while a snapshot is being taken and vice versa. When making configuration changes it is safest to first create a snapshot as a backup and then make the changes. For additional information on creating snapshots, see [Taking a Snapshot \(page 60\)](#).

Steps for Changing the Store's Topology

When you change your topology, you should go through these steps:

1. [Make the Topology Candidate \(page 35\)](#)
2. [Transform the Topology Candidate \(page 36\)](#)
3. [View the Topology Candidate \(page 40\)](#)
4. [Validate the Topology Candidate \(page 41\)](#)
5. [Preview the Topology Candidate \(page 41\)](#)
6. [Deploy the Topology Candidate \(page 42\)](#)
7. [Verify the Store's Current Topology \(page 43\)](#)

Creating a new topology may be an iterative process. You may want to try different options to see what may be best before the changes are deployed. In the end, examine the topology candidate and decide if it is satisfactory. If not, apply more transformations, or start over with different parameters. You can view and validate topology candidates to decide if they are appropriate.

The possible transformations to expand the store include redistributing data, increasing replication factor, and rebalancing. These are described in [Transform the Topology Candidate \(page 36\)](#).

You can also contract the topology by removing Storage Nodes. For more information, see [Contracting a Topology \(page 39\)](#).

The following sections walk you through the process of changing the configuration for your store using the Administration Command Line Interface.

Make the Topology Candidate

To create the first topology candidate for an initial deployment, before any Replication Nodes exist, you use the `topology create` command. The `topology create` command takes a topology name, a pool name and the number of partitions as arguments.

Note

You should avoid using the dollar sign ('\$') character in topology candidate names. The CLI displays a warning when trying to create or clone topologies whose names contain the reserved character.

For example:

```
kv-> topology create -name firstTopo -pool BostonPool
-partitions 300
Created: firstTopo
```

This initial topology candidate can be deployed, without any further transformations, using the `plan deploy-topology` command.

After the store is deployed, topology candidates are created with the `topology clone` command. A clone's source can be another topology candidate, or the current, deployed topology. The `topology clone` command takes the following arguments:

- `-from <from topology>`

The name of the source topology candidate.

- `-name <to topology>`

The name of the clone.

For example:

```
kv-> topology clone -from topo -name CloneTopo
Created CloneTopo
```

Also, there is a variant of the `topology clone` command that takes the following arguments:

- `-current`

If specified, use the current, deployed topology as a source.

- `-name <to topology>`

The name of the clone.

For example:

```
kv-> topology clone -current -name ClonedTopo
Created ClonedTopo
```

Transform the Topology Candidate

After the initial deployment, the store is changed by deploying a topology candidate that differs from the topology currently in effect. This target topology is generated by transforming a topology candidate to expand the store by using the `topology redistribute`, `rebalance`, or `change-repfactor` command. The target topology candidate can be contracted by using the `topology contract` command instead.

Transformations follow the topology rules described in the previous section.

The `topology rebalance`, `redistribute` or `change-repfactor` commands can only make changes to the topology candidate if there are additional, or changed, Storage Nodes available. It uses the new resources to rearrange Replication Nodes and partitions so the topology complies with the topology rules and the store improves on read or write throughput.

The following are scenarios in how you might expand or contract the store.

Increase Data Distribution

You can increase data distribution in order to enhance write throughput by using the topology redistribute command. The redistribute command only works if new Storage Nodes are added to permit the creation of new shards. Partitions are distributed across the new shards, resulting in more Replication Nodes to service write operations.

The following example demonstrates adding a set of Storage Nodes and redistributing the data to those nodes. In this example four nodes are added because the zone's replication factor is four and the new partition requires four nodes to satisfy the replication requirements:

```
kv-> plan deploy-sn -zn zn1 -host node04 -port 5000 -wait
Executed plan 7, waiting for completion...
Plan 7 ended successfully
kv-> plan deploy-sn -zn zn1 -host node05 -port 5000 -wait
Executed plan 8, waiting for completion...
Plan 8 ended successfully
kv-> plan deploy-sn -zn zn1 -host node06 -port 5000 -wait
Executed plan 9, waiting for completion...
Plan 9 ended successfully
kv-> plan deploy-sn -zn zn1 -host node07 -port 5000 -wait
Executed plan 10, waiting for completion...
Plan 10 ended successfully
kv-> pool join -name BostonPool -sn sn4
Added Storage Node(s) [sn4] to pool BostonPool
kv-> pool join -name BostonPool -sn sn5
Added Storage Node(s) [sn5] to pool BostonPool
kv-> pool join -name BostonPool -sn sn6
Added Storage Node(s) [sn6] to pool BostonPool
kv-> pool join -name BostonPool -sn sn7
Added Storage Node(s) [sn7] to pool BostonPool
kv-> topology clone -current -name newTopo
Created newTopo
kv-> topology redistribute -name newTopo -pool BostonPool
Redistributed: newTopo
kv-> plan deploy-topology -name newTopo -wait
Executed plan 11, waiting for completion...
Plan 11 ended successfully
```

The redistribute command uses added capacity to create new shards and to migrate partitions to those shards. The command fails if the number of new shards is not greater than the current number of shards.

Note

You should not issue redistribute commands against a mixed shard store. A mixed shard store has shards whose Replication Nodes are operating with different software versions of Oracle NoSQL Database.

The system goes through these steps when it is redistributing a topology candidate:

1. New Replication Nodes are created for each shard and are assigned to Storage Nodes following the topology rules described earlier. It may be necessary to move existing Replication Nodes to different Storage Nodes to best use available resources while still complying with the topology rules.
2. Partitions are distributed evenly among all shards. Partitions that are in shards that are over populated will move to the shards with the least number of partitions.
3. You do not specify which partitions are moved.

Increase Replication Factor

You can increase the replication factor and create more copies of the data to improve read throughput and availability by using the `topology change-repfactor` command. More Replication Nodes are added to each shard so that it has the requisite number of nodes. The new Replication Nodes are populated from existing nodes in the shard. Since every shard in a zone has the same replication factor, if there are a large number of shards, this command may require a significant number of new Storage Nodes to be successful.

For additional information on how to identify your primary replication factor and its implications, see [Replication Factor \(page 208\)](#).

The following example increases the replication factor of the store to 4. The administrator deploys a new Storage Node and adds it to the Storage Node pool. The admin then clones the existing topology and transforms it to use a new replication factor of 4.

```
kv-> plan deploy-sn -zn zn1 -host node08 -port 5000 -wait
Executed plan 12, waiting for completion...
Plan 12 ended successfully
kv-> pool join -name BostonPool -sn sn8
Added Storage Node(s) [sn8] to pool BostonPool
kv-> topology clone -current -name repTopo
Created repTopo
kv-> topology change-repfactor -name repTopo -pool BostonPool -rf 4 -zn zn1
Changed replication factor in repTopo
kv-> plan deploy-topology -name repTopo -wait
Executed plan 13, waiting for completion...
Plan 13 ended successfully
```

The `change-repfactor` command fails if:

1. The new replication factor is less than or equal to the current replication factor.
2. The Storage Nodes specified by the storage node pool do not have enough capacity to host the required new Replication Nodes.

Balance a Non-Compliant Topology

Topologies must obey the rules described in [Determining Your Store's Configuration \(page 34\)](#). Changes to the physical characteristics of the store can make the current topology of the store violate those rules. For example, after performance tuning, you may want to

decrease the capacity of a Storage Node. If that node was already hosting the maximum permissible number of Replication Nodes, reducing the capacity will put the store out of compliance with the capacity rules.

You can balance a non-compliant configuration by using the `topology rebalance` command. This command requires a topology candidate name and a Storage Node pool name.

The following example examines the topology candidate named `repTopo` for any violations to the topology rules. If no improvements are needed as a result of this examination, the topology candidate is unchanged. However, if improvements are needed, then the topology rebalance command will move or create Replication Nodes, using the Storage Nodes in the `BostonPool` pool, in order to correct any violations. The command does not under any circumstances create additional shards.

```
kv-> topology rebalance -name repTopo -pool BostonPool
Rebalanced: repTopo
```

If there are an insufficient number of Storage Nodes, the `topology rebalance` command may not be able to correct all violations. In that case, the command makes as much progress as possible, and warns of remaining issues.

Contracting a Topology

You can contract a topology by using the `topology contract` command. This command requires a topology candidate name and a Storage Node pool name. This command supports the removal of Storage Nodes and contracts the topology by relocating Replication Nodes, deleting shards, and migrating partitions.

Note

Decreasing the replication factor is not currently supported. Also, Admin relocation is not supported. If an admin is present on a contracted Storage Node, the contraction operation will fail.

The following example contracts the topology by removing 3 Storage Nodes (`sn2`, `sn5` and `sn8`). First, you clone the pool using the `pool clone` command and remove the Storage Nodes from the cloned pool using the `pool leave` command. Then, the topology is contracted and deployed using the contracted pool. Finally, the Storage Nodes can be removed using the `plan remove-sn` command. This command automatically stops Storage Nodes before removal.

```
# Clone the existing Storage Node pool as to be contractedPool
kv-> pool clone -name contractedPool -from AllStorageNodes
Cloned pool contractedPool
kv-> pool leave -name contractedPool -sn sn2
Removed Storage Node(s) [sn2] from pool contractedPool
kv-> pool leave -name contractedPool -sn sn5
Removed Storage Node(s) [sn5] from pool contractedPool
kv-> pool leave -name contractedPool -sn sn8
Removed Storage Node(s) [sn8] from pool contractedPool

# Generate a contracted candidate topology
kv-> topology clone -current -name contractedTopology
```

```

Created contractedTopology
kv-> topology contract -name contractedTopology -pool contractedPool
Contracted: contractedTopology

# Deploy the contracted candidate topology as the real topology.
kv-> plan deploy-topology -name contractedTopology -wait
Executed plan 16, waiting for completion...
Plan 16 ended successfully

# Remove to-be-deleted SNs
kv-> plan remove-sn -sn sn2 -wait
Executed plan 17, waiting for completion...
Plan 17 ended successfully
kv-> plan remove-sn -sn sn5 -wait
Executed plan 18, waiting for completion...
Plan 18 ended successfully
kv-> plan remove-sn -sn sn8 -wait
Executed plan 19, waiting for completion...
Plan 19 ended successfully

```

View the Topology Candidate

You can view details of the topology candidate or a deployed topology by using the topology view command. The command takes a topology name as an argument. With the topology view command, you can view all at once: the store name, number of partitions, shards, replication factor, host name and capacity in the specified topology.

For example:

```

kv-> topology view -name repTopo
store=mystore numPartitions=300 sequence=315
zn: id=zn1 name=Boston repFactor=4 type=PRIMARY

sn=[sn1] zn:[id=zn1 name=Boston] node01:5000 capacity=1
[rg1-rn1]
sn=[sn2] zn:[id=zn1 name=Boston] node02:5000 capacity=1
[rg1-rn2]
sn=[sn3] zn:[id=zn1 name=Boston] node03:5000 capacity=1
[rg1-rn3]
sn=[sn4] zn:[id=zn1 name=Boston] node04:5000 capacity=1
[rg1-rn4]
sn=[sn5] zn:[id=zn1 name=Boston] node05:5000 capacity=1
sn=[sn6] zn:[id=zn1 name=Boston] node06:5000 capacity=1
sn=[sn7] zn:[id=zn1 name=Boston] node07:5000 capacity=1
sn=[sn8] zn:[id=zn1 name=Boston] node08:5000 capacity=1

shard=[rg1] num partitions=300
[rg1-rn1] sn=sn1
[rg1-rn2] sn=sn2
[rg1-rn3] sn=sn3

```

```
[rg1-rn4] sn=sn4
```

Validate the Topology Candidate

You can validate the topology candidate or a deployed topology by using the `topology validate` command. The `topology validate` command takes a topology name as an argument. If no topology is specified, the current topology is validated. Validation makes sure that the topology candidate obeys the topology rules described in [Determining Your Store's Configuration \(page 34\)](#). Validation generates "violations" and "notes".

Violations are issues that can cause problems and should be investigated.

Notes are informational and highlight configuration oddities that may be potential issues, but may be expected.

For example:

```
kv-> topology validate -name repTopo
Validation for topology candidate "repTopo":
4 warnings.
sn7 has 0 RepNodes and is under its capacity limit of 1
sn8 has 0 RepNodes and is under its capacity limit of 1
sn5 has 0 RepNodes and is under its capacity limit of 1
sn6 has 0 RepNodes and is under its capacity limit of 1
```

Preview the Topology Candidate

You should preview the changes that would be made for the specified topology candidate relative to a starting topology. You use the `topology preview` command to do this. This command takes the following arguments:

- *name*

A string to identify the topology.

- *start <from topology>*

If `-start` topology name is not specified, the current topology is used. This command should be used before deploying a new topology.

For example:

```
kv-> topology clone -current -name redTopo
Created redTopo
kv-> topology redistribute -name redTopo -pool BostonPool
Redistributed: redTopo
kv-> topology preview -name redTopo
Topology transformation from current deployed topology to redTopo:
Create 1 shard
Create 4 RNs
Migrate 150 partitions

shard rg2
```

```

4 new RNs: rg2-rn1 rg2-rn2 rg2-rn3 rg2-rn4
150 partition migrations
kv-> topology validate -name redTopo
Validation for topology candidate "redTopo":
No problems

```

Deploy the Topology Candidate

With a satisfactory topology candidate, you can use the admin service to generate and execute a plan which migrates the store to the new topology.

You can deploy the topology candidate by using the plan `deploy-topology` command. This command takes a topology name as an argument.

While the plan is executing, you can monitor the plan's progress. You have several options:

- The plan can be interrupted then retried, or canceled.
- Other, limited plans may be executed while a transformation plan is in progress to deal with ongoing problems or failures.

By default, the plan `deploy-topology` command refuses to deploy a topology candidate if it introduces new violations of the topology rules. This behavior can be overridden by using the `-force` optional plan flag on that command.

For example:

```

kv-> show topology
store=mystore numPartitions=300 sequence=315
zn: id=zn1 name=Boston repFactor=4 type=PRIMARY

sn=[sn1] zn=[id=zn1 name=Boston] node01:5000 capacity=1 RUNNING
[rg1-rn1] RUNNING
No performance info available
sn=[sn2] zn=[id=zn1 name=Boston] node02:5000 capacity=1 RUNNING
[rg1-rn2] RUNNING
No performance info available
sn=[sn3] zn=[id=zn1 name=Boston] node03:5000 capacity=1 RUNNING
[rg1-rn3] RUNNING
No performance info available
sn=[sn4] zn=[id=zn1 name=Boston] node04:5000 capacity=1 RUNNING
[rg1-rn4] RUNNING
No performance info available
sn=[sn5] zn=[id=zn1 name=Boston] node05:5000 capacity=1
sn=[sn6] zn=[id=zn1 name=Boston] node06:5000 capacity=1
sn=[sn7] zn=[id=zn1 name=Boston] node07:5000 capacity=1
sn=[sn8] zn=[id=zn1 name=Boston] node08:5000 capacity=1

shard=[rg1] num partitions=300
[rg1-rn1] sn=sn1
[rg1-rn2] sn=sn2
[rg1-rn3] sn=sn3

```

```

[rg1-rn4] sn=sn4
kv-> plan deploy-topology -name redTopo -wait
Executed plan 14, waiting for completion...
Plan 14 ended successfully
kv-> show topology
store=mystore numPartitions=300 sequence=470
  zn: id=zn1 name=Boston repFactor=4 type=PRIMARY

sn=[sn1]  zn:[id=zn1 name=Boston] node01:5000 capacity=1 RUNNING
  [rg1-rn1] RUNNING
    No performance info available
sn=[sn2]  zn:[id=zn1 name=Boston] node02:5000 capacity=1 RUNNING
  [rg1-rn2] RUNNING
    No performance info available
sn=[sn3]  zn:[id=zn1 name=Boston] node03:5000 capacity=1 RUNNING
  [rg1-rn3] RUNNING
    No performance info available
sn=[sn4]  zn:[id=zn1 name=Boston] node04:5000 capacity=1 RUNNING
  [rg1-rn4] RUNNING
    No performance info available
sn=[sn5]  zn:[id=zn1 name=Boston] node05:5000 capacity=1 RUNNING
  [rg2-rn1] RUNNING
    No performance info available
sn=[sn6]  zn:[id=zn1 name=Boston] node06:5000 capacity=1 RUNNING
  [rg2-rn2] RUNNING
    No performance info available
sn=[sn7]  zn:[id=zn1 name=Boston] node07:5000 capacity=1 RUNNING
  [rg2-rn3] RUNNING
    No performance info available
sn=[sn8]  zn:[id=zn1 name=Boston] node08:5000 capacity=1 RUNNING
  [rg2-rn4] RUNNING
    No performance info available

shard=[rg1] num partitions=150
  [rg1-rn1] sn=sn1
  [rg1-rn2] sn=sn2
  [rg1-rn3] sn=sn3
  [rg1-rn4] sn=sn4
shard=[rg2] num partitions=150
  [rg2-rn1] sn=sn5
  [rg2-rn2] sn=sn6
  [rg2-rn3] sn=sn7
  [rg2-rn4] sn=sn8

```

Verify the Store's Current Topology

You can verify the store's current topology by using the `verify` command. The `verify` command checks the current, deployed topology to make sure it obeys the topology rules described in [Determining Your Store's Configuration \(page 34\)](#).

You should examine the new topology and decide if it is satisfactory, and if not apply more transformations, or start over with different parameters.

For example:

```
kv-> verify configuration
Verify: starting verification of store mystore based upon
       topology sequence #470
300 partitions and 8 storage nodes
Time: 2016-11-21 13:40:37 UTC  Version: 12.1.4.3.5
See localhost:KVR00T/mystore/log/mystore_{0..N}.log for progress messages
Verify: Shard Status: healthy:2 writable-degraded:0 read-only:0 offline:0
Verify: Admin Status: healthy
Verify: Zone [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       RN Status: online:8 offline:0 maxDelayMillis:0 maxCatchupTimeSecs:0
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
       Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC  Build id: 8e70b50c0b0e
Verify:           Admin [admin1]           Status: RUNNING,MASTER
Verify:           Rep Node [rg1-rn1]       Status: RUNNING,MASTER ...
Verify: == checking storage node sn2 ==
Verify: Storage Node [sn2] on node02:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
       Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC  Build id: 8e70b50c0b0e
Verify:           Rep Node [rg1-rn2]       Status: RUNNING,REPLICA ...
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
       Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC  Build id: 8e70b50c0b0e
Verify:           Rep Node [rg1-rn3]       Status: RUNNING,REPLICA ...
Verify: == checking storage node sn4 ==
Verify: Storage Node [sn4] on node04:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
       Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC  Build id: 8e70b50c0b0e
Verify:           Rep Node [rg1-rn4]       Status: RUNNING,REPLICA ...
Verify: == checking storage node sn5 ==
Verify: Storage Node [sn5] on node05:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
       Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC  Build id: 8e70b50c0b0e
Verify:           Rep Node [rg2-rn1]       Status: RUNNING,MASTER ...
Verify: == checking storage node sn6 ==
Verify: Storage Node [sn6] on node06:5000
       Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
       Status: RUNNING
```

```

Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC Build id: 8e70b50c0b0e
Verify:          Rep Node [rg2-rn2]      Status: RUNNING,REPLICA ...
Verify: == checking storage node sn7 ==
Verify: Storage Node [sn7] on node07:5000
      Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
      Status: RUNNING
Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC Build id: 8e70b50c0b0e
Verify:          Rep Node [rg2-rn3]      Status: RUNNING,REPLICA ...
Verify: == checking storage node sn8 ==
Verify: Storage Node [sn8] on node08:5000
      Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
      Status: RUNNING
Ver: 12cR1.3.2.15 2015-03-04 06:35:02 UTC Build id: 8e70b50c0b0e
Verify:          Rep Node [rg2-rn4]      Status: RUNNING,REPLICA ...
Verification complete, no violations.

```

Deploying an Arbiter Node Enabled Topology

An Arbiter Node is a service that supports write availability when the store replication factor is two and a single Replication Node becomes unavailable. The role of an Arbiter Node is to participate in elections and respond to acknowledge requests if one of the two Replication Nodes in a shard becomes unavailable.

Arbiter Nodes are automatically configured in a topology if the store replication factor is two and a primary zone is configured to host Arbiter Nodes.

For example, suppose a store consists of a primary zone, "Manhattan" with two Storage Nodes deployed in the same shard. In this example, an Arbiter Node is deployed in the third Storage Node (capacity = 0) in order to provide write availability even if one of the two Replication Nodes in the shard becomes unavailable.

Note

Durability.ReplicaAckPolicy must be set to SIMPLE_MAJORITY, so that writes can succeed if a Replication Node becomes unavailable in a shard. For more information on ReplicaAckPolicy, see this Javadoc page: http://docs.oracle.com/cd/E17277_02/html/java/com/sleepycat/je/Durability.ReplicaAckPolicy.html.

1. Create, start, and configure the store. Note that a Storage Node with capacity equal to zero is deployed, which will host the Arbiter Node.
 - Create the store:

```

java -jar kv/lib/kvstore.jar makebootconfig \
-root KVROOT \
-host node01 \
-port 8000 \
-harange 8010,8020 \
-capacity 1

```



```
java -jar kv/lib/kvstore.jar makebootconfig \
-root KVRROOT \
-host node02 \
-port 9000 \
-harange 9010,9020 \
-capacity 1

java -jar kv/lib/kvstore.jar makebootconfig \
-root KVRROOT \
-host node03 \
-port 10000 \
-harange 1000,10020 \
-capacity 0 \
```

- Create and copy the security directories:

```
java -jar kv/lib/kvstore.jar
securityconfig \
config create -root KVRROOT -kspwd NoSql@+123
Created files
KVRROOT/security/security.xml
KVRROOT/security/store.keys
KVRROOT/security/store.trust
KVRROOT/security/client.trust
KVRROOT/security/client.security
KVRROOT/security/store.passwd (Generated in CE version)
KVRROOT/security/store.wallet/cwallet.sso (Generated in EE version)

Created
scp -r KVRROOT/security node02:KVRROOT/
scp -r KVRROOT/security node03:KVRROOT/
```

- Start the store by running the following command on each Storage Node:

```
java -Xmx100m -Xms100m -jar KVHOME/lib/kvstore.jar \
start -root KVRROOT &
```

2. Load the following script `conf.txt` to deploy the zone, admin and Storage Nodes. To host an Arbiter Node, the zone must be primary and should have the `-arbiters` flag set.

```
ssh node01
java -Xmx100m -Xms100m -jar KVHOME/lib/kvstore.jar runadmin \
-port 8000 -host node01 load -file conf.txt \
-security KVRROOT/security/client.security
```

The file, `conf.txt`, would then contain content like this:

```
### Begin Script ###
plan deploy-zone -name "Manhattan" -type primary -arbiters -rf 2 -wait
plan deploy-sn -zn zn1 -host node01 -port 8000 -wait
pool create -name SNs
```

```
pool join -name SNs -sn sn1
plan deploy-admin -sn sn1 -port 8001 -wait
plan deploy-sn -zn zn1 -host node02 -port 9000 -wait
pool join -name SNs -sn sn2
plan deploy-sn -zn zn1 -host node03 -port 10000 -wait
pool join -name SNs -sn sn3
### End Script ###
```

3. Create a topology, preview it, and then deploy it:

```
kv-> topology create -name arbTopo -pool SNs -partitions 300
Created: arbTopo
```

```
kv-> topology preview -name arbTopo
Topology transformation from current deployed topology to arbTopo:
Create 1 shard
Create 2 RNs
Create 300 partitions
Create 1 AN
```

```
shard rg1
  2 new RNs : rg1-rn1 rg1-rn2
  1 new AN : rg1-an1
  300 new partitions
```

```
kv-> plan deploy-topology -name arbTopo -wait
Executed plan 6, waiting for completion...
Plan 6 ended successfully
```

4. Verify that the Arbiter Node is running.

```
kv-> verify configuration
Verify: starting verification of store mystore
based upon topology sequence #308
300 partitions and 3 storage nodes
Time: 2016-11-21 13:40:37 UTC   Version: 12.1.4.3.5
See node01:KVROOT/mystore/log/mystore_{0..N}.log
for progress messages
Verify: Shard Status: healthy:1 writable-degraded:0
                                   read-only:0 offline:0

Verify: Admin Status: healthy
Verify: Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
RN Status: online:2 offline:0 maxDelayMillis:6 maxCatchupTimeSecs:0
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:8000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: eadd643fa168+
Verify:      Admin [admin1]           Status: RUNNING,MASTER
Verify:      Rep Node [rg1-rn1]
Status: RUNNING,MASTER sequenceNumber:635 haPort:8011
```

```

Verify: == checking storage node sn2 ==
Verify: Storage Node [sn2] on node02:9000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: eadd643fa168+
Verify:      Rep Node [rg1-rn2]
Status: RUNNING,REPLICA
sequenceNumber:635 haPort:9010 delayMillis:6 catchupTimeSecs:0
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:10000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: eadd643fa168+
Verify:      Arb Node [rg1-an1]
Status: RUNNING,REPLICA sequenceNumber:0 haPort:node03:10010
...

```

5. Now suppose node02 is unreachable. Verify this by using `verify` configuration:

```

kv-> verify configuration
Verify: starting verification of store mystore
based upon topology sequence #308
300 partitions and 3 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
See node01:KVROOT/mystore/log/mystore_{0..N}.log
for progress messages
Verify: Shard Status: healthy:0 writable-degraded:1
                                read-only:0 offline:0

Verify: Admin Status: healthy
Verify:
    Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
RN Status: online:1 offline:1
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:8000
Zone:
    [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
    Status: RUNNING
    Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: eadd643fa168+
Verify:      Admin [admin1]      Status: RUNNING,MASTER
Verify:      Rep Node [rg1-rn1]
Status: RUNNING,MASTER sequenceNumber:901 haPort:8011
Verify: == checking storage node sn2 ==
Verify:      sn2: ping() failed for sn2 : Unable to connect to
the storage node agent at host node02, port 9000, which may not be
running; nested exception is:
    java.rmi.ConnectException: Connection refused to
    host: node02; nested exception is:
    java.net.ConnectException: Connection refused
Verify: Storage Node [sn2] on node02:9000

```

```

Zone:
  [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true] UNREACHABLE
Verify:      rg1-rn2: ping() failed for rg1-rn2 : Unable to connect
to the storage node agent at host node02, port 9000, which may not
be running; nested exception is:
  java.rmi.ConnectException: Connection refused to host: node02;
nested exception is:
  java.net.ConnectException: Connection refused
Verify:      Rep Node [rg1-rn2]      Status: UNREACHABLE
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:10000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=true]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: eadd643fa168+
Verify:      Arb Node [rg1-an1]
Status: RUNNING, REPLICA sequenceNumber:901 haPort:node03:10010
Verification complete, 3 violations, 0 notes found.
Verification violation: [rg1-rn2]
ping() failed for rg1-rn2 : Unable to connect to the storage node
agent at host node02, port 9000, which may not be running;
nested exception is:
  java.rmi.ConnectException: Connection refused to
host: node02; nested exception is:
  java.net.ConnectException: Connection refused
Verification violation: [sn2] ping() failed for sn2 : Unable to
connect to the storage node agent at host node02, port 9000, which
may not be running; nested exception is:
  java.rmi.ConnectException: Connection refused to host: node02;
nested exception is:
  java.net.ConnectException: Connection refused
...

```

In this case the Arbiter Node supports write availability so you can still perform write operations while node02 is repaired or replaced. Once node02 is restored, any written data will be migrated.

6. Test that you can still write to the store with the help of the Arbiter Node. For example, run the script file `test.kvsql` (see below for `test.kvsql`) using the Oracle NoSQL Database Shell utility (see below example). To do this, use the `load` command in the Query Shell:

```

> java -jar KVHOME/lib/sql.jar -helper-hosts node01:8000 \
-store mystore -security USER/security/admin.security
kvsql-> load -file ./test.kvsql
Statement completed successfully.
Statement completed successfully.
Loaded 3 rows to users.

```

Note

For the Enterprise Edition (EE) installation, make sure the kvstore-ee.jar is added in the classpath.

The following commands are collected in test.kvsql:

```
### Begin Script ###
load -file test.ddl
import -table users -file users.json
### End Script ###
```

Where the file test.ddl would contain content like this:

```
DROP TABLE IF EXISTS users;
CREATE TABLE users(id INTEGER, firstname STRING, lastname STRING,
age INTEGER, primary key (id));
```

And the file users.json would contain content like this:

```
{"id":1,"firstname":"Dean","lastname":"Morrison","age":51}
{"id":2,"firstname":"Idona","lastname":"Roman","age":36}
{"id":3,"firstname":"Bruno","lastname":"Nunez","age":49}
```

Chapter 5. Upgrading an Existing Oracle NoSQL Database Deployment

This section describes how to upgrade the software of your Oracle NoSQL Database deployment.

Installing new software requires that each node be restarted. Depending on the configuration of your store, it may be possible to upgrade it while the store continues to remain online and available to clients, which is useful in cases where downtime is not desirable. An offline upgrade can also be performed instead if desired. The offline upgrade involves shutting down all nodes, installing new software on all of them, and then restarting them. That may be simpler and is certainly permitted, but it does mean that the store is not available for the duration of the upgrade.

Online upgrade can succeed if the store's replication factor is greater than 2.

For stores with a replication factor greater than two, the shards can maintain their majorities and continue reading and writing data on behalf of clients while their components are restarted, one at a time. If the replication factor is 2 or 1, then the majorities cannot be maintained across the restart of a single node, and each shard will become unavailable for a short time.

Preparing to Upgrade

Before beginning the upgrade process, you should take a backup of the store by creating a snapshot. See [Taking a Snapshot \(page 60\)](#).

In Oracle NoSQL Database, configuration changes and other administrative activities involve plans. For information about plans, see [Plans \(page 9\)](#).

Note

During the upgrade process, you should not create any plans until all services in the store have been upgraded.

Application programs that use the kvstore client library should be upgraded to the new software version as soon as possible after the service components have been upgraded.

General Upgrade Notes

This section contains upgrade information that is generally true for all versions of Oracle NoSQL Database. Upgrade instructions and notes for specific releases are given in sections following this one.

When Oracle NoSQL Database is first installed, it is placed in a KVHOME directory, which may be per-machine, or optionally be shared by multiple Storage Nodes (for example, using NFS). Here, we call this existing KVHOME location, OLD_KVHOME.

Note

It is useful for installations to adopt a convention for KVHOME that includes the release number. That is, always use a KVHOME location such as /var/kv/kv-M.N.O, where M.N.O are the release.major.minor numbers. This can be easily achieved by simply unzip/untarring the distribution into a common directory (/var/kv in this example).

Installing new software requires that each node be restarted. Oracle NoSQL Database is a replicated system, so to avoid excessive failover events it is recommended that any node that is running as a MASTER be restarted after all those marked REPLICA. This command tells you which nodes are MASTER and REPLICA:

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar ping -host <hostname> -port <port> \
-security USER/security/admin.security
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

To make the process more debuggable, when upgrading a node and while the Storage Node is stopped, you should move the existing log files under KVROOT and KVROOT/<storename>/log to any other directory.

Use the host and registry port for any active node in the store. For example, in the following example, rg1-rn1 and rg2-rn1 are running as MASTER and should be restarted last:

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar ping -port 5000 -host node01 \
-security USER/security/admin.security
Pinging components of store mystore based upon topology sequence #315
300 partitions and 6 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
Shard Status: healthy:2 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:6 offline:0 maxDelayMillis:1 maxCatchupTimeSecs:0
Storage Node [sn1] on node01:5000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Admin [admin1] Status: RUNNING,MASTER
Rep Node [rg1-rn1] Status: RUNNING,MASTER
sequenceNumber:327 haPort:5011
Storage Node [sn2] on node02:6000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Rep Node [rg1-rn2] Status: RUNNING,REPLICA
```

```

sequenceNumber:327 haPort:6010 delayMillis:1 catchupTimeSecs:0
Storage Node [sn3] on node03:7000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Rep Node [rg1-rn3] Status: RUNNING,REPLICA
sequenceNumber:327 haPort:7010 delayMillis:1 catchupTimeSecs:0
Storage Node [sn4] on node04:8000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Rep Node [rg2-rn1] Status: RUNNING,MASTER
sequenceNumber:327 haPort:8010
Storage Node [sn5] on node05:9000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Rep Node [rg2-rn2] Status: RUNNING,REPLICA
sequenceNumber:327 haPort:9010 delayMillis:1 catchupTimeSecs:0
Storage Node [sn6] on node06:10000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 0c693aa1a5a0
Rep Node [rg2-rn3] Status: RUNNING,REPLICA
sequenceNumber:327 haPort:10010 delayMillis:1 catchupTimeSecs:0

```

When upgrading your store, place the updated software in a new KVHOME directory on a Storage Node running the admin service. The new KVHOME directory is referred to here as NEW_KVHOME. If the KVHOME and NEW_KVHOME directories are shared by multiple Storage Nodes (for example, using NFS), it is necessary to maintain both locations while the upgrade is going on. The original KVHOME directory is no longer needed once the upgrade is complete. In this case, the start up procedure on each node needs to be modified to refer to the value of NEW_KVHOME in order to have it use the new software.

Note

In cases where each node has its own copy of the software installation, then it is possible to replace the installation in place and not modify the value of KVHOME.

If you want to turn on security after upgrade from a non-secure store, follow the steps described in the Adding Security to a New Installation section in the *Oracle NoSQL Database Security Guide*.

Upgrade to This Release from Release 3.0 or Later

Upgrading a store from release 3 or later to this release can be accomplished one Storage Node at a time because Storage Nodes running a mix of the two releases are permitted to run simultaneously in the same store. This allows you to strategically upgrade Storage Nodes in the most efficient manner.

Note

Upgrading a 1.0 or 2.0 store directly to release 4 is not supported. You must first upgrade to release 3, and then upgrade to release 4. For more information see the Release 3 *Oracle NoSQL Database Administrator's Guide*.

Note

If your store contains more than a handful of Storage Nodes, you may want to perform your upgrade using a script. See [Using a Script to Upgrade to Release 4 \(page 58\)](#) for more information.

To avoid potential problems, new CLI commands are available to identify when nodes can be upgraded at the same time. These commands are described in the following procedure.

To upgrade your store, first install the latest software to upgrade the Admin CLI. Then, use the upgraded CLI to verify that all of the Storage Nodes do not violate any basic requirements:

```
kv-> verify prerequisite
...
Verification complete, no violations.
```

Once all violations are corrected, if any, install the latest software on a Storage Node that is running an admin service.

Do the following:

1. On a Storage Node running a release 3 or later admin service:
 - a. Place the updated software in a new KVHOME directory on a Storage Node running the admin service. The new KVHOME directory is referred to here as NEW_KVHOME. If nodes share this directory using NFS, this only needs to be done once for each shared directory.
 - b. Stop the Storage Node using the release 3 or later CLI. When you do this, this shuts down the admin service on that Storage Node.

If you have configured the node to automatically start the Storage Node Agent on reboot using /etc/init.d, Upstart, or some other mechanism first modify that script to point to NEW_KVHOME.

Once you have modified that script, shutdown the Storage Node:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar stop -root <kvroot>
```

- c. Restart the Storage Node using the release 4 code:

```
nohup java -Xmx256m -Xms256m \  
-jar NEW_KVHOME/lib/kvstore.jar start -root <kvroot> &
```

(If the system is configured to automatically restart the Storage Node Agent, this step may not be necessary.)

- d. Use the CLI to connect to the Storage Node which is now running the release 4 code:

```
java -Xmx256m -Xms256m \  
-jar NEW_KVHOME/lib/kvstore.jar runadmin -port 5000 -host node1 \  
-security USER/security/admin/security
```

- e. Verify that all the Storage Nodes in the store are running the proper software level required to upgrade to release 4. Note that any version of release 3, including any minor or patch release, meets the minimum software level requirements.

```
kv-> verify prerequisite  
Verify: starting verification of mystore based upon topology  
sequence #315  
300 partitions and 6 storage nodes.  
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5  
See node1:<KVR00T>/mystore/log/mystore_{0..N}.log for progress  
messages  
Verify prerequisite: Storage Node [sn3] on node3:5000  
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]  
Status: RUNNING  
Ver: 12cR1.3.5.2 2016-03-09 04:37:46 UTC Build id: 0c693aa1a5a0  
  
...  
  
Verification complete, no violations.
```

Note that only a partial sample of the verification command's output is shown here. The important part is the last line, which shows no violations.

The most likely reason for a violation is if you are (accidentally) attempting a release level downgrade. For example, it is illegal to downgrade from a higher minor release to a lower minor release. Possibly this is occurring simply because you are running the CLI using a package at a minor release level that is lower than the release level at other nodes in the store.

Note

It is legal to downgrade from a higher *patch* level to a lower patch level. So, for example downgrading from 2.1.4 to 2.1.3 would be legal, while downgrading from 2.1.3 to 2.0.39 would not be legal.

Also, a violation will occur if you attempt to upgrade 1.0 or 2.0 nodes directly to release 4. In this case, you must first upgrade to release 3, and then upgrade to release 4. For more information see the *Release 3 Oracle NoSQL Database Administrator's Guide*.

In any case, if the `verify prerequisite` command shows violations, resolve the situation before you attempt to upgrade the identified nodes.

- f. Obtain an ordered list of the nodes to upgrade.

```
kv-> show upgrade-order
Calculating upgrade order, target version: 12.1.4.3.5,
prerequisite: 12.1.3.0.5
sn3 sn4
sn2 sn5
sn6
```

This command displays one or more Storage Nodes on a line. Multiple Storage Nodes on a line are separated by a space. If multiple Storage Nodes appear on a single line, then those nodes can be safely upgraded at the same time, if desired. When multiple nodes are upgraded at the same time, the upgrade must be completed on all nodes before the nodes next on the list can be upgraded. If at some point you lose track of which group of nodes should be upgraded next, you can always run the `show upgrade-order` command again.

The Storage Nodes combined together on a single line can be upgraded together. Therefore, for this output, you would upgrade sn3 and sn4. Then upgrade sn2 and sn5. And, finally, upgrade sn6.

Note that you must completely upgrade a group of nodes before continuing to the next group. That is, upgrade sn3 and sn4 before you proceed to upgrading sn2, sn5, or sn6.

2. For each of the Storage Nodes in the first group of Storage Nodes to upgrade (sn3 and sn4, in this example):
 - a. Place the release 4 software in a new KVHOME directory. The new KVHOME directory is referred to here as NEW_KVHOME. If nodes share this directory using NFS, this only needs to be done once for each shared directory.
 - b. Stop the Storage Node using the release 3 or later utility.

If you have configured the node to automatically start the Storage Node Agent on reboot using `/etc/init.d`, Upstart, or some other mechanism first modify that script to point to NEW_KVHOME.

Once you have modified that script, shutdown the Storage Node using the old code:

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar stop -root <kvroot>
```

- c. Restart the Storage Node using the new code:

```
nohup java -Xmx256m -Xms256m \
-jar NEW_KVHOME/lib/kvstore.jar start -root <kvroot> &
```

(If the system is configured to automatically restart the Storage Node Agent, this step may not be necessary.)

3. Verify the upgrade before upgrading your next set of nodes. This command shows which nodes have been successfully upgraded, and which nodes still need to be upgraded:

```
kv-> verify upgrade
Verify: starting verification of mystore based upon topology
sequence #315
300 partitions and 6 storage nodes.
Time: 2016-03-09 04:37:46 UTC Version: 12.1.4.3.5
See node1:<KVROOT>/mystore/log/mystore_{0..N}.log for progress
messages
Verify upgrade: Storage Node [sn3] on node3:5000
Zone: [name=Boston id=zn1 type=PRIMARY]      Status: RUNNING
Ver: 12cR1.4.3.5 2016-11-21 13:40:37 UTC   Build id: 35728a5c21b1

...

Verify: sn2: Node needs to be upgraded from 12.1.3.5.2 to
version 12.1.4.3.5 or newer

...

Verification complete, 0 violations, 3 notes found.
Verification note: [sn2]      Node needs to be upgraded from
12.1.3.5.2 to version 12.1.4.3.5 or newer
Verification note: [sn5]      Node needs to be upgraded from
12.1.3.5.2 to version 12.1.4.3.5 or newer
Verification note: [sn6]      Node needs to be upgraded from
12.1.3.5.2 to version 12.1.4.3.5 or newer
```

For brevity and space, we only show part of the output generated by the verify upgrade command. Those nodes which have been upgraded are identified with a verification message that includes the current software version number:

```
Verify upgrade: Storage Node [sn3] on node3:5000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12cR1.4.3.5 2016-11-21 13:40:37 UTC   Build id: 35728a5c21b1
```

Those nodes which still need to be upgraded are identified in two different ways. First, the verification message for the node indicates that an upgrade is still necessary:

```
Verify: sn2: Node needs to be upgraded from 12.1.3.5.2 to
version 12.1.4.3.5 or newer
```

Second, the very end of the verification output identifies all the nodes that still need to be upgraded:

```
Verification complete, 0 violations, 3 notes found.
Verification note: [sn2]      Node needs to be upgraded from
12.1.3.5.2 to version 12.1.4.3.5 or newer
Verification note: [sn5]      Node needs to be upgraded from
12.1.3.5.2 to version 12.1.4.3.5 or newer
Verification note: [sn6]      Node needs to be upgraded from
```

12.1.3.5.2 to version 12.1.4.3.5 or newer

Note

If the verification shows nodes you thought were upgraded as being still in need of an upgrade, you *must* resolve that problem before upgrading the other nodes in your store. As a kind of a sanity check, you can verify just those nodes you just finished upgrading:

```
kv-> verify upgrade -sn sn3 -sn sn4
Verify: starting verification of mystore based upon topology
sequence #315
...
Verification complete, no violations.
```

4. You can continue upgrading groups of Storage Nodes, as identified by the `show upgrade-order` command. Follow the procedure outlined above. Stop the release 3 or later Storage Node using the release 3 or later stop command, then restart the Storage Node using the release 4 start command. Continue doing this until all Storage Nodes have been upgraded.

If at some point you lose track of which group of nodes should be upgraded next, you can always run the `show upgrade-order` command again:

```
kv-> show upgrade-order
Calculating upgrade order, target version: 12.1.4.3.5,
prerequisite: 12.1.3.0.5
sn2 sn5
sn6
```

5. When you are all done upgrading your Storage Nodes, the `verify upgrade` command will show no verification notes at the end of its output:

```
kv-> verify upgrade
Verify: starting verification of mystore based upon topology
sequence #315
...
Verification complete, no violations.
```

Using a Script to Upgrade to Release 4

For any deployments with more than a handful of Storage Nodes, the manual upgrade procedure described above becomes problematic. In that case, you should probably upgrade your store using a script.

An example script (bash shell script) is available for you to examine in the release 4 distribution. It can be found here:

```
<KVHOME>/examples/upgrade/onlineUpgrade
```

This script has the same upgrade restrictions as was described earlier in this section: it will only upgrade a release 3 or later installation to release 4, and your store must have a replication factor of at least 3 in order for your store to be available during the upgrade process.

The provided script is an example only. It must be modified in order for it to properly function for your installation.

Note that the script does not perform any software provisioning for you. This means you are responsible for placing the release 4 package on your host machines in whatever location you are using for your installation software. That said, the script communicates with your host machines using ssh, so you could potentially enhance the script to provision your machines using scp.

Because the script uses ssh, in order for it to function you must configure your machines to allow automatic login (that is, login over ssh without a password). ssh supports public/private key authentication, so this is generally a secure way to operate.

For information on how to configure ssh in this way, see http://www.linuxproblem.org/art_9.html. For information on how to install and configure ssh and the ssh server, see your operating system's documentation.

Chapter 6. Administrative Procedures

This chapter contains procedures that may be generally useful to the Oracle NoSQL Database administrator.

Note

Oracle NoSQL Database Storage Nodes and Admins make use of an embedded database (Oracle Berkeley DB, Java Edition). You should never directly manipulate the files maintained by this database. In general it is not advisable to move, delete or modify the files and directories located under KVROOT unless you are asked to do so by Oracle Customer Support. But in particular, *never* move or delete any file ending with a `jdb` suffix. These will all be found in an `env` directory somewhere under KVROOT.

Backing Up the Store

To back up the KVStore, you take snapshots of nodes in the store and copy the resulting snapshots to a safe location. Note that the distributed nature and scale of Oracle NoSQL Database makes it unlikely that a single machine can hold the backup for the entire store. These instructions do not address where and how snapshots are stored.

Taking a Snapshot

A snapshot provides consistency across all records within the same shard, but not across partitions in independent shards. The underlying snapshot operations are performed in parallel to the extent possible in order to minimize any potential inconsistencies.

To take a snapshot from the admin CLI, use the `snapshot create` command:

```
kv-> snapshot create -name <snapshot name>
```

Using this command, you can create or remove a named snapshot. (The name of the snapshot is provided using the `<name>` parameter.) You can also remove all snapshots currently stored in the store.

For example, to create and remove a snapshot:

```
kv-> snapshot create -name Thursday
Created snapshot named 110915-153514-Thursday on all 3 nodes
kv-> snapshot remove -name 110915-153514-Thursday
Removed snapshot 110915-153514-Thursday
```

You can also remove all snapshots currently stored in the store:

```
kv-> snapshot create -name Thursday
Created snapshot named 110915-153700-Thursday on all 3 nodes
kv-> snapshot create -name later
Created snapshot named 110915-153710-later on all 3 nodes
kv-> snapshot remove -all
```

Removed all snapshots

Note

Snapshots should not be taken while any configuration (topological) changes are being made, because the snapshot might be inconsistent and not usable. At the time of the snapshot, use ping and then save the information that identifies Masters for later use during a load or restore. For more information, see [Snapshot Management \(page 61\)](#).

Snapshot Management

When you run a snapshot, data is collected from every Replication Node in the system, including both Masters and replicas. If the operation does not succeed for at least one of the nodes in a shard, it fails.

If you decide to create an off-store copy of the snapshot, you should copy the snapshot data for only one of the nodes in each shard. If possible, copy the snapshot data taken from the node that was serving as the Master at the time the snapshot was taken.

At the time of the snapshot, you can identify which nodes are currently running as the Master using the ping command. There is a Master for each shard in the store and they are identified by the keyword: MASTER. For example, in the following example, replication node rg1-rn1, running on Storage Node sn1, is the current Master:

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar ping -port 5000 -host node01 \
-security USER/security/admin/security
Pinging components of store mystore based upon topology sequence #316
300 partitions and 3 storage nodes
Time: 2016-11-21 13:40:37 UTC   Version: 12.1.4.3.5
Shard Status: healthy:3 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:9 offline:0 maxDelayMillis:1 maxCatchupTimeSecs:0
Storage Node [sn1] on node01:5000
  Zone: [name=Boston id=zn1 type=PRIMARY]
  Status: RUNNING
  Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
    Admin [admin1]           Status: RUNNING,MASTER
    Rep Node [rg1-rn1]       Status: RUNNING,REPLICA
      sequenceNumber:231 haPort:5011 delayMillis:1 catchupTimeSecs:0
    Rep Node [rg2-rn1]       Status: RUNNING,REPLICA
      sequenceNumber:231 haPort:5012 delayMillis:1 catchupTimeSecs:0
    Rep Node [rg3-rn1]       Status: RUNNING,MASTER
      sequenceNumber:227 haPort:5013
Storage Node [sn2] on node02:6000
  Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
  Status: RUNNING
  Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: db9ec397225c
```



```

Rep Node [rg1-rn2]      Status: RUNNING,MASTER
sequenceNumber:231 haPort:6010
Rep Node [rg2-rn2]      Status: RUNNING,REPLICA
sequenceNumber:231 haPort:6011 delayMillis:1 catchupTimeSecs:0
Rep Node [rg3-rn2]      Status: RUNNING,REPLICA
sequenceNumber:227 haPort:6012 delayMillis:1 catchupTimeSecs:0
Storage Node [sn3] on node03:7000
Zone: [name=Boston id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Rep Node [rg1-rn3]      Status: RUNNING,REPLICA
sequenceNumber:231 haPort:7010 delayMillis:1 catchupTimeSecs:0
Rep Node [rg2-rn3]      Status: RUNNING,MASTER
sequenceNumber:231 haPort:7011
Rep Node [rg3-rn3]      Status: RUNNING,REPLICA
sequenceNumber:227 haPort:7012 delayMillis:1 catchupTimeSecs:0

```

You should save the above information and associate it with the respective snapshot, for later use during a load or restore.

Note

Snapshots include the admin database. Depending on how the store might need to be restored, the admin database may or may not be useful.

Snapshot data for the local Storage Node is stored in a directory inside of the KVR00T directory. For each Storage Node in the store, you have a directory named:

```
KVR00T/<store>/<SN>/<resource>/snapshots/<snapshot_name>/files
```

where:

- <store> is the name of the store.
- <SN> is the name of the Storage Node.
- <resource> is the name of the resource running on the Storage Node. Typically this is the name of a replication node.
- <snapshot_name> is the name of the snapshot.

Snapshot data consists of a number of files, and they all are important. For example:

```
> ls /var/kvroot/mystore/sn1/rg1-rn1/snapshots/110915-153514-Thursday
00000000.jdb 00000002.jdb 00000004.jdb 00000006.jdb
00000001.jdb 00000003.jdb 00000005.jdb 00000007.jdb
```

Note

To preserve storage, purge obsolete snapshots on a periodic basis.

Recovering the Store

There are two ways to recover your store from a previously created snapshot. The first mechanism allows you to use a backup to create a store with any desired topology. The second method requires you to restore the store using the *exact same* topology as was in use when the snapshot was taken.

Note

If you had to replace a failed Storage Node, that qualifies as a topology change. In that case, you must use the Load program to restore your store.

For information on how to replace a failed Storage Node, see [Replacing a Failed Storage Node \(page 79\)](#).

Using the Load Program

You can use the `oracle.kv.util.Load` program to restore a store from a previously created snapshot. You can run this program directly, or you can access it using `kvstore.jar`, as shown in the examples in this section.

By using this tool, you can restore the store to any topology, not just the one that was in use when the snapshot was created.

This mechanism works by iterating through all records in a snapshot, putting each record into the target store as it proceeds through the snapshot. It should be used only to restore to a new, empty store. Do not use this with an existing store because it only writes records if they do not already exist.

Note that to recover the store, you must load records from snapshot data captured for each shard in the store. For best results, you should load records using snapshot data captured from the replication nodes that were running as Master at the time the snapshot was taken. (If you have three shards in your store, then there are three Masters at any given time, and so you need to load data from three sets of snapshot data). To identify the Master, use `ping` at the time the snapshot was taken.

You should use snapshot data taken at the same point in time; do not, for example, use snapshot data for shard 1 that was taken on Monday, and snapshot data for shard 2 that was taken on Wednesday because this can cause your store to be restored in an inconsistent state.

This mechanism can only go at the speed of insertion of the new store. Because you probably have multiple shards in your store, you should be restoring your store from data taken from each shard. To do this, run the Load program in parallel, with each instance operating on data captured from different replication nodes.

The program's usage to load admin metadata is:

```
java -jar KVHOME/lib/kvstore.jar load \  
-store <storeName> -host <hostname> port <port> \  
-load-admin \  
-source <admin-backup-dir> \  

```

```
[-force] [-username <user>] \
[-security <security-file-path>]
```

The program's usage to load store data is:

```
java -jar KVHOME/lib/kvstore.jar load [-verbose] \
-store <storeName> -host <hostname> \
-port <port> -source <shard-backup-dir> \
[, <shard-backup-dir>]* \
[-checkpoint <checkpoint-files-directory>] \
[-username <user>] [-security <security-file-path>]
```

where:

- `-load-admin` Loads the store metadata from the snapshot to the new store. In this case the `-source` directory must point to the environment directory of the admin node from the snapshot. The store must not be available for use by users at the time of this operation.

Note

This option should not be used on a store unless that store is being restored from scratch. If `-force` is specified in conjunction with `-load-admin`, any existing metadata in the store, including tables and security metadata, will be overwritten. For more information, see [Load Program and Metadata \(page 65\)](#).

- `-host <hostname>` identifies the host name of a node in your store.
- `-port <port>` identifies the registry port in use by the store's node.
- `-security <security-file-path>` identifies the security file used to specify properties for login.
- `-source <admin-backup-dir> | <shard-backup-dir> [,<shard-backup-dir>]*`
`admin-backup-dir` specifies the admin snapshot directory containing the contents of the admin metadata that is to be loaded into the store.

`Shard-backup-dir` specifies the backup directories that represent the contents of snapshots created using the snapshot commands described at [Taking a Snapshot \(page 60\)](#).

- `-store <storeName>` identifies the name of the store.
- `-username <user>` identifies the name of the user to login to the secured store.

For example, suppose there is a snapshot in `/var/backups/snapshots/110915-153828-later`, and there is a new store named "mystore" on host "host1" using registry port 5000. Run the Load program on the host that has the `/var/backups/snapshots` directory:

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar load \
-source /var/backups/snapshots/110915-153514-Thursday -store mystore \
-host host1 -port 5000 -security KVR00T/security/client.security
```

Note

Before you load the records to the new store, you need to make sure the store is deployed. For more information, see [Configuring the KVStore \(page 12\)](#).

Load Program and Metadata

You can use the Load program to restore a store with metadata (tables, security) from a previously created snapshot.

The following steps describe how to load from a snapshot with metadata to a newly created store:

1. Create, start and configure the new store (target). Do not make the store accessible to applications yet.

- Create the new store:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar makebootconfig \  
-root KVRROOT \  
-host NewHost -port 8000 \  
-harange 8010,8020 \  
-capacity 1
```

- Create security directory:

```
java -jar kv/lib/kvstore.jar securityconfig \  
config create  
-root KVRROOT -kspwd NoSql@+123  
Created files  
KVRROOT/security/security.xml  
KVRROOT/security/store.keys  
KVRROOT/security/store.trust  
KVRROOT/security/client.trust  
KVRROOT/security/client.security  
KVRROOT/security/store.passwd (Generated in CE version)  
KVRROOT/security/store.wallet/cwallet.sso (Generated in EE version)  
  
Created
```

- Start the new store:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar start \  
-root KVRROOT &
```

- Configure the new store:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar runadmin \  

```

```
-port 8000 -host NewHost \  
-security KVR00T/security/client.security  
kv-> configure -name NewStore  
Store configured: NewStore
```

Note

Loading security metadata requires the names of the source store and the target store to be the same, otherwise the security metadata cannot be used later.

2. Locate the snapshot directories for the source store. There should be one for the admin nodes plus one for each shard. For example in a 3x3 store there should be 4 snapshot directories used for the load. The load program must have direct file-based access to each snapshot directory loaded. In this case, the snapshot source directory is in `/var/kvroot/mystore/sn1/admin1/snapshots/110915-153514-Thursday`.
3. Load the store metadata using the `-load-admin` option. Host, port, and store refer to the target store. In this case the `-source` directory must point to the environment directory of the admin node from the snapshot.

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar load \  
-source \  
/var/kvroot/mystore/sn1/admin1/snapshots/110915-153514-Thursday \  
-store NewStore -host NewHost -port 8000 \  
-load-admin \  
-security KVR00T/security/client.security
```

Note

This command can be run more than once if something goes wrong, as long as the store is not accessible to applications.

4. Deploy the store. For more information, see [Configuring the KVStore \(page 12\)](#).
5. Once the topology is deployed, load the shard data for each shard. To do this, run the Load program in parallel, with each instance operating on data captured from different replication nodes. For example, suppose there is a snapshot of OldStore in `var/backups/snapshots/140827-144141-back`.

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar load \  
-source var/backups/snapshots/140827-144141-back -store NewStore \  
-host NewHost -port 8000 \  
-security KVR00T/security/client.security
```

Note

This step may take a long time or might need to be restarted. In order to significantly reduce retry time, the use of a status file is recommended.

If the previous store has been configured with username and password, the program will prompt for username and password here.

6. The store is now ready for applications.

Restoring Directly from a Snapshot

You can restore a store directly from a snapshot. This mechanism is faster than using the Load program described in the previous section, but it can be used only to restore to the *exact same* topology as was used when the snapshot was taken. This means that all ports and host names or IP addresses (depending on your configuration) must be exactly the same as when the snapshot was taken.

You must perform this procedure for each Storage Node in your store, and for each service running on each Storage Node.

1. Put the to-be-recovered snapshot data in the recovery directory for the service corresponding to the snapshot data. For example, if you are recovering Storage Node sn1, service rg1-rn1 in store mystore, then log in to the node where that service is running and:

```
> mkdir KVRROOT/mystore/sn1/rg1-sn1/recovery
> mv /var/kvroot/mystore/sn1/rg1-rn1/snapshots/110915-153828-later \
KVRROOT/mystore/sn1/rg1-sn1/recovery/110915-153828-later
```

Do this for each service running on the Storage Node. Production systems should have only one resource running on a given Storage Node, but it is possible to deploy, for example, multiple replication nodes on a single Storage Node. A Storage Node can also have an administration process running on it, and this also needs to be restored.

2. Having done this, restart the Storage Node

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar stop -root /var/kvroot \
> nohup java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar start -root /var/kvroot &
```

On startup, the Storage Node notices the recovery directory, and moves that directory to the resource's environment directory and use it.

Note

Remember that this procedure recovers the store to the time of the snapshot. If your store was active since the time of the snapshot, then all data modifications made since the time of the last snapshot are lost.

Recovering from Data Corruption

Oracle NoSQL Database is capable of automatically detecting data corruption in its database. When data corruption is detected, Oracle NoSQL Database will automatically shutdown the associated Admin or Replication Nodes. Manual administrative action is then required before they can be brought back online.

Detecting Data Corruption

Oracle NoSQL Database Admin or Replication Node processes will exit when they detect data corruption. This is caused by a background task which detects data corruption caused by a disk failure, or similar physical media or I/O subsystem problem. Typically, the corruption is detected because of a checksum error in a log entry in one of the data (*.jdb) files contained in an Admin or Replication Node database environment. A data corruption error generates output in the debug log similar to this:

```
2016-10-25 16:59:52.265 UTC SEVERE [rg1-rn1] Process exiting
com.sleepycat.je.EnvironmentFailureException: (JE 7.3.2)
rg1-rn1(-1):kvroot/mystore/sn1/rg1-rn1/env
com.sleepycat.je.log.ChecksumException:
Invalid log entry type: 102 lsn=0x0/0x0 bufPosition=5
bufRemaining=4091 LOG_CHECKSUM:
Checksum invalid on read, log is likely invalid. Environment is
invalid and must be closed
...
2016-10-25 16:59:52.270 UTC SEVERE [rg1-rn1] Exception creating
service rg1-rn1:
(JE 7.3.2) rg1-rn1(-1):kvroot/mystore/sn1/rg1-rn1/env
com.sleepycat.je.log.ChecksumException:
Invalid log entry type: 102 lsn=0x0/0x0 bufPosition=5
bufRemaining=4091 LOG_CHECKSUM:
Checksum invalid on read, log is likely invalid. Environment is
invalid and must be closed. (12.1.4.3.0): oracle.kv.FaultException:
(JE 7.3.2) rg1-rn1(-1):kvroot/mystore/sn1/rg1-rn1/env
com.sleepycat.je.log.ChecksumException: Invalid log entry type: 102
lsn=0x0/0x0 bufPosition=5 bufRemaining=4091 LOG_CHECKSUM: Checksum
invalid on read, log is likely invalid. Environment is invalid and
must be closed. (12.1.4.3.0)
Fault class name: com.sleepycat.je.EnvironmentFailureException
...
2016-10-25 16:59:52.272 UTC INFO [rg1-rn1] Service status changed
from STARTING to ERROR_NO_RESTART
```

The EnvironmentFailureException will cause the process to exit. Because the exception was caused by log corruption, the service status is set to ERROR_NO_RESTART, which means that the service will not restart automatically.

Data Corruption Recovery Procedure

If an Admin or Replication Node has been stopped due to data corruption, then manual administration intervention is required in order to restart the Node:

1. Optional: Archive the corrupted environment data files.

If you want to send the corrupted environment to Oracle support for help in identifying the root cause of the failure, archive the corrupted environment data files. These are usually located at:

```
<KVR00T>/<STORE_NAME>/<SNx>/<Adminx>/"
```

or

```
<KVR00T>/<STORE_NAME>/<SNx>/<rgx-rnx>"
```

However, if you used the [plan change-storagedir \(page 154\)](#) CLI command to change the storage directory for your Replication Node, then you will find the environment in the location that you specified to that command.

You can use the [show topology \(page 171\)](#) CLI command to display your store's topology. As part of this information, the storage directory for each of your Replication Nodes are identified.

2. Confirm that a non-corrupted version of the data is available.

Before removing the files associated with the corrupted environment, confirm that another copy of the data is available either on another node or via a previously save snapshot. For a Replication Node, you must be using a Replication Factor greater than 1 and also have a properly operating Replication Node in the store in order for the data to reside elsewhere in the store. If you are using a RF=1, then you must have a previously saved snapshot in order to continue.

If the problem is with an Admin Node, there must be to be another Admin available in the store that is operating properly.

Use the [ping \(page 198\)](#) or [verify configuration \(page 180\)](#) commands to check if the available nodes are running properly and healthy.

3. Remove all the data files that reside in the corrupted environment.

Once the data files associated with a corrupted environment have been saved elsewhere, and you have confirmed that another copy of the data is available, delete all the data files in the enviroment directory. Make sure you only delete the files associated with the Admin or Replication Node that has failed due to a corrupted environment error.

```
# ls <KVR00T>/mystore/sn1/rg1-rn1/env
00000000.jdb 00000001.jdb 00000002.jdb je.config.csv
je.info.0 je.lck je.stat.csv

# rm <KVR00T>/mystore/sn1/rg1-rn1/env/*.jdb
```

4. Perform recovery using either Network Restore, or from a backup. Be aware the recovery from a backup will not work to recover an Admin Node.

- Recovery using Network Restore

Network restore can be used to recover from data corruption if the corrupted node belongs to a replication group that has other replication nodes available. Network restore is automatic recovery task. After removing all of the database files in the corrupted environment, you only need to connect to CLI and restart the corrupted node.

For a Replication Node:

```
kv-> plan start-service -service rg1-rn1
```

For an Admin:

```
kv-> plan start-service -service rg1-rn1
```

- Recovery from a backup (RNs only)

If the store does not have another member in the Replication Node's shard or if all of the nodes in the shard have failed due to data corruption, you will need to restore the node's environment from a previously created snapshot. See [Recovering the Store \(page 63\)](#) for details.

Note that to recover an Admin that has failed due to data corruption, you must have a working Admin somewhere in the store. Snapshots do not capture Admin data.

Using the Export and Import Utilities

The [export \(page 182\)](#) utility creates a package that contains user data and schema information. You can export either the entire store, or some subset of the tables in the store.

The [import \(page 187\)](#) utility consumes data from a package written by the export utility. You can import the entire contents of the export package, or you can import a subset of tables contained within the package.

Both utilities are designed to be run against a fully installed and configured store. The export utility will not write information regarding your store's topology. Nor will the import utility in any way attempt to reinstall or configure a store.

Security metadata is also not managed by these utilities. This means that the users and roles are not exported or imported. In order to reconstruct a store, these must be manually created.

The export and import utilities provide you an alternative way to back up and restore all or part of your store. You can use these utilities instead of, or in addition to, taking snapshots. Data can be exported to either a local file system, or to Oracle Storage Cloud Services.

Note

To use the export and import utilities with Oracle Storage Cloud Services, you must download and install Java jar files which provide necessary support. See [Installing the Cloud Storage JARs \(page 73\)](#) for details.

Exporting Data

You can export a complete store, or a subset of tables, using the export utility. For a complete description of this utility, its behavior, and its command line options, see the [export \(page 182\)](#) utility.

The export utility exports a single record at a time. For best results, the export utility should be used on a store which currently has no write activity. This utility does not create any kind of snapshot isolation.

To export data, you must create a configuration file which identifies the type of export (either local filesystem, or Oracle Storage Cloud Services), and the export destination. If you are exporting to a local filesystem, the directory you provide must currently exist but also must not currently contain an export package. If you are exporting to Oracle Storage Cloud Services, then the container name you provide must not currently exist.

The following examples use the local filesystem.

To export an entire store:

1. Create a destination directory:

```
mkdir /disk1/exports/current
```

2. Create a configuration file with the appropriate contents. For example, export-config.txt:

```
export-type = LOCAL
export-package-path = /disk1/exports/current
```

3. Run the export:

```
java -jar <KVHOME>/lib/kvtool.jar export -export-all \
-store kvstore \
-helper-hosts localhost:5000 -config export-config.txt \
-security USER/security/admin.security
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

Be aware that for a fully populated store, the export process could take a long time. For this reason, you can track the progress of an export by monitoring the contents of Export.log, which is created in the export package directory.

You can also export a single table, or a subset of tables. This export will also include any indices defined for the table. Use the -table command line option instead of the -export-all command line option. If you want to export more than one table, comma-separate the table names.

```
java -jar <KVHOME>/lib/kvtool.jar export \
-table userTable,inventoryTable -store kvstore \
-helper-hosts localhost:5000 -config export-config.txt \
-security USER/security/admin.security
```

Importing Data

You can import a complete store, or a subset of tables, using the `import` utility. For a complete description of this utility, its behavior, and its command line options, see the [import \(page 187\)](#) utility.

The dataset that you use for import must have been created using the export utility. See the [export \(page 182\)](#) utility for details.

Write activity may be on-going against the store at the time of the import. In this regard, the `import` utility is simply another client writing to the store. In the case of a conflict when writing a table row or record, your store data will be in a state defined by which client last wrote the data.

If data has reached its time-to-live (TTL) expiration datestamp, the data is not imported.

To import data, you must create a configuration file which identifies the type of export (either local filesystem, or Oracle Storage Cloud Services), and the location of the export package. You can also identify the TTL type that you want to use (ABSOLUTE or RELATIVE). For production systems, ABSOLUTE is usually the proper choice, and this is the default.

To import the entire contents of an export package:

1. Make sure the store is fully installed and operational. All security configuration must be configured for the store. The `import` utility will not install or configure a store for you.
2. Create a configuration file with the appropriate contents. For example, `import-config.txt`:

```
export-type = LOCAL
export-package-path = /disk1/exports/current
ttl = ABSOLUTE
```

3. Run the import. If you are using a secured store, you would have to provide a username and security file which has full write access to the store:

```
java -jar <KVHOME>/lib/kvtool.jar import -import-all \
-store kvstore \
-helper-hosts localhost:5000 -config import-config.txt \
-security USER/security/admin.security
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

Be aware that for a fully populated store, the import process could take a long time. For this reason, you can track the progress of an import by checking the `Import.log` file, which is written to the same directory as is identified by the `export_package_path` configuration file parameter.

You can also import a single table, or a subset of tables. Use the `-table` command line option instead of the `-import-all` command line option. If you want to import more than one table, comma-separate the table names.

```
java -jar <KVHOME>/lib/kvtool.jar import \  
-table userTable,inventoryTable -store kvstore \  
-helper-hosts localhost:5000 \  
-config import-config.txt \  
-security USER/security/admin.security
```

Installing the Cloud Storage JARs

To use the export and import utilities with Oracle Storage Cloud Services, you must download and install Java jar files which provide the necessary support. Do the following:

- Download the Oracle Storage Cloud Service Java SDK from this location:

<http://www.oracle.com/technetwork/topics/cloud/downloads/cloud-service-java-sdk-2121032.html>

- Unzip the downloaded SDK.
- The extracted zip file contains the necessary jar files in the `lib` directory. Copy the following jar files to the `lib` folder in your Oracle NoSQL Database installation:

```
jersey-client-x.x.jar  
jersey-core-x.x.jar  
jettison-x.x.jar  
oracle.cloud.storage.api-x.x.x.jar
```

where `x.x` represents the version number included on the file in the download package.

Managing Avro Schema

Avro is a data format that can be used by values in your store's records. Whether a record's value uses the Avro data format is determined by your development team.

When store records use the Avro data format, your development team must define schema for their usage of that format. This schema is provided in flat-text files in JSON format, and must then be added to the store using the CLI. Schema can also be enabled and disabled, and multiple versions of the schema can exist at the same time. The ability to support multiple versions of the schema is required in order to support the ability to change (or evolve) schema.

Adding Schema

Avro schema is defined in a flat-text file, and then added to the store using the command line interface. For example, suppose you have schema defined in a file called `my_schema.avsc`. Then (assuming your store is running) you start your command line interface and add the schema like this:

```
> java -Xmx256m -Xms256m \  
-jar <kvhome>/lib/kvstore.jar runadmin -port <port> -host <host> \  

```

```
-security USER/security/admin.security  
kv-> ddl add-schema -file my_schema.avsc
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#) section in the *Oracle NoSQL Database Administrator's Guide*.

Note that when adding schema to the store, some error checking is performed to ensure that the schema is correctly formed. Errors are problems that must be addressed before the schema can be added to the store. Warnings are problems that should be addressed, but are not so serious that the CLI refuses to add the schema. However, to add schema with Warnings, you must use the `-force` switch.

If you see any Errors or Warnings when you add schema to your store, you should discuss the problem with your development team so as to decide what to do about it.

Changing Schema

To change (evolve) existing schema, use the `-evolve` flag:

```
kv-> ddl add-schema -file my_schema.avsc -evolve
```

Note that when changing schema in the store, some error checking is performed to ensure that schema evolution can be performed correctly. This error checking consists of comparing the new schema to all currently enabled versions of that schema.

This error checking can result in either Errors or Warnings. Errors are fatal problems that must be addressed before the modified schema can be added to the store. Errors represent situations where data written with an old version of the schema cannot be read by clients using a new version of the schema.

Warnings are problems that can be avoided using a two-phase upgrade process. In a two-phase upgrade, all clients begin using the schema only for reading in phase I (the old schema is still used for writing), and then use the new schema for both reading and writing in phase II. Phase II may not be begun until phase I is complete; that is, no client may use the new schema for writing until all clients are using it for reading.

If you see any Errors or Warnings when you attempt to evolve schema in your store, you should discuss the problem with your development team so as to decide what to do about it.

Disabling and Enabling Schema

You cannot delete schema, but you can disable it:

```
kv-> ddl disable-schema -name avro.MyInfo.1
```

To enable schema that has been disabled:

```
kv-> ddl enable-schema -name avro.MyInfo.1
```

Showing Schema

To see all the schemas currently enabled in your store:

```
kv-> show schemas
```

To see all schemas, including those which are currently disabled:

```
kv-> show schemas -disabled
```

Increasing the capacity of a Storage Node

You can increase the capacity of a Storage Node by adding additional hard disks to the machine. Such a configuration permits the placement of each Replication Node on its own disk and ensures that the Replication Nodes on the SN are not competing for I/O resources. The location of this directory on its disk can be specified via the `storagedir` parameter.

The following example demonstrates deploying a new store and adding two more disks to a Storage Node, increasing the capacity from 1 to 3:

1. Create, start and configure the new store.

- Create the new store:

```
java -jar KVHOME/lib/kvstore.jar makebootconfig \  
-root KVRROOT \  
-host node20 -port 5000 \  
-harange 5010,5030 \  
-capacity 1 \  
-memory_mb 200 \  
-storagedir /disk1/ondb/data
```

- Create and copy security directory:

```
java -jar kv/lib/kvstore.jar  
securityconfig config create -root KVRROOT -kspwd NoSql@+123  
Created files  
KVRROOT/security/security.xml  
KVRROOT/security/store.keys  
KVRROOT/security/store.trust  
KVRROOT/security/client.trust  
KVRROOT/security/client.security  
KVRROOT/security/store.passwd (Generated in CE version)  
KVRROOT/security/store.wallet/cwallet.sso (Generated in EE version)  
  
Created
```

- Start the new store:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar start \  
-root KVRROOT &
```

- Configure the new store:

```
java -jar KVHOME/lib/kvstore.jar runadmin \  
-port 5000 -host node20 \  
-security KVRROOT/security/client.security
```

```
kv-> configure -name kvstore
Store configured: kvstore
```

2. Create a zone. Then create an administration process on a specific host:

```
kv-> plan deploy-zone -name Houston -rf 1 -wait
Executed plan 1, waiting for completion...
Plan 1 ended successfully
kv-> plan deploy-sn -znname "Houston" -port 5000 -wait -host node20
Executed plan 2, waiting for completion...
Plan 2 ended successfully
```

```
kv-> plan deploy-admin -sn sn1 -port 5001 -wait
Executed plan 3, waiting for completion...
Plan 3 ended successfully
```

3. Create the storage node pool. Then add the storage node to the pool:

```
kv-> pool create -name AllStorageNodes
```

```
kv-> pool join -name AllStorageNodes -sn sn1
```

4. Create a topology, preview it, and then deploy it:

```
kv-> topology create -name 1x1 -pool AllStorageNodes -partitions 120
Created: 1x1
```

```
kv-> topology preview -name 1x1
Topology transformation from current deployed topology to 1x1:
Create 1 shard
Create 1 RN
Create 120 partitions
```

```
shard rg1
  1 new RN : rg1-rn1
  120 new partitions
```

```
kv-> plan deploy-topology -name 1x1 -wait
Executed plan 4, waiting for completion...
Plan 4 ended successfully
```

5. Suppose two more disk drives were added to the Storage Node, mounted as disk2 and disk3. Add the storage directories using the plan `change-storagedir` command.

```
kv-> plan change-storagedir -sn sn1 -storagedir /disk2/ondb/data \
-add -wait
Executed plan 5, waiting for completion...
Plan 5 ended successfully
```

```
kv-> plan change-storagedir -sn sn1 -storagedir /disk3/ondb/data \
-add -wait
Executed plan 6, waiting for completion...
Plan 6 ended successfully
```

Note

It is possible to also specify the size of the directories when you do this. However, if you do that for these new storage directories, then you must also specify the size for all other storage directories. See [Managing Storage Directory Sizes \(page 77\)](#) for more information.

6. Change the capacity equal to the total number of disks now available on the Storage Node (3).

```
kv-> plan change-parameters -service sn1 -wait -params capacity=3
Executed plan 7, waiting for completion...
Plan 7 ended successfully
```

Note

You need to perform last two steps on all the Storage Nodes (in your cluster) to add the disk drives and increase the capacity of each Storage Node. In this case, it is a single node deployment, so the topology is now ready to be redistributed.

7. Redistribute your topology to expand the cluster in order to use the new capacity (3) of the Storage Node.

```
kv-> topology clone -current -name 3x1
Created 3x1

kv-> topology redistribute -name 3x1 -pool AllStorageNodes
Redistributed: 3x1

kv-> topology preview -name 3x1
Topology transformation from current deployed topology to 3x1:
Create 2 shards
Create 2 RNs
Migrate 80 partitions

shard rg2
  1 new RN : rg2-rn1
  40 partition migrations
shard rg3
  1 new RN : rg3-rn1
  40 partition migrations

kv-> plan deploy-topology -name 3x1 -wait
Executed plan 8, waiting for completion...
Plan 8 ended successfully
```

Managing Storage Directory Sizes

By default, Oracle NoSQL Database evenly distributes data across all the Storage Nodes in your store. It does this because it assumes all of the hardware in your store is homogenous, and so all the Storage Nodes are equal in terms of disk capacity.

However, if you are running a store in an environment where some Storage Nodes have more disk capacity than other Storage Nodes, then you can indicate that to Oracle NoSQL Database and it will place more data on the Storage Nodes with more capacity. Be aware that this can result in increased workload for the Storage Nodes with the larger storage capacity because (depending on your data access patterns) those Storage Nodes could see more read and/or write activity. Be sure to size your hardware to support that additional workload, if any.

To specify storage capacity, use plan `change-storagedir` as described in [Increasing the capacity of a Storage Node \(page 75\)](#). When you use plan `change-storagedir` be sure to specify the `-storagedirsize` parameter so as to indicate how large the new storage directory is.

Note

You must either specify the storage size for every storage directory in use for your store, or specify it for none of the directories in your store. It is an error to specify storage size for some but not all storage directories.

The value specified for this parameter must be a long, followed optionally by a unit string. Accepted unit strings are: KB, MB, GB, and TB, corresponding to 1024 , 1024^2 , 1024^3 , 1024^4 respectively. Acceptable strings are case insensitive. Valid delimiters between the long value and the unit string are `" "`, `"-"`, or `"_"`.

For example:

```
kv-> verbose
Verbose mode is now on
kv-> show topology
store=mystore numPartitions=300 sequence=308
  zn: id=zn1 name=Manhattan repFactor=3 type=PRIMARY
allowArbiters=false

sn=[sn1] zn:[id=zn1 name=Manhattan] node1:9000 capacity=1 RUNNING
  [rg1-rn1] RUNNING /storage-dir/sn1 0
  No performance info available
sn=[sn2] zn:[id=zn1 name=Manhattan] node2:9000 capacity=1 RUNNING
  [rg1-rn2] RUNNING /storage-dir/sn2 0
  single-op avg latency=0.0 ms multi-op avg latency=0.0 ms
sn=[sn3] zn:[id=zn1 name=Manhattan] node3:9000 capacity=1 RUNNING
  [rg1-rn3] RUNNING /storage-dir/sn3 0
  No performance info available

shard=[rg1] num partitions=300
  [rg1-rn1] sn=sn1 haPort=node1:9010
  [rg1-rn2] sn=sn2 haPort=node2:9010
  [rg1-rn3] sn=sn3 haPort=node3:9010
  partitions=1-300

kv-> plan change-storagedir -sn sn1 -storagedir /storage-dir/sn1 \
-storagedirsize "200 gb" -add -wait
Executed plan 7, waiting for completion...
```

```

Plan 7 ended successfully
kv-> plan change-storagedir -sn sn2 -storagedir /storage-dir/sn2 \
-storagedirsize "300 gb" -add -wait
Executed plan 8, waiting for completion...
Plan 8 ended successfully
kv-> plan change-storagedir -sn sn3 -storagedir /storage-dir/sn3 \
-storagedirsize "400 gb" -add -wait
Executed plan 9, waiting for completion...
Plan 9 ended successfully
kv-> show topology
store=mystore numPartitions=300 sequence=308
  zn: id=zn1 name=Manhattan repFactor=3 type=PRIMARY
allowArbiters=false

sn=[sn1] zn:[id=zn1 name=Manhattan] node1:9000 capacity=1 RUNNING
  [rg1-rn1] RUNNING /storage-dir/sn1 214748364800
           No performance info available
sn=[sn2] zn:[id=zn1 name=Manhattan] node2:9000 capacity=1 RUNNING
  [rg1-rn2] RUNNING /storage-dir/sn2 322122547200
           single-op avg latency=0.0 ms   multi-op avg latency=0.0 ms
sn=[sn3] zn:[id=zn1 name=Manhattan] node3:9000 capacity=1 RUNNING
  [rg1-rn3] RUNNING /storage-dir/sn3 429496729600
           single-op avg latency=0.0 ms   multi-op avg latency=0.0 ms

shard=[rg1] num partitions=300
  [rg1-rn1] sn=sn1 haPort=node1:9010
  [rg1-rn2] sn=sn2 haPort=node2:9010
  [rg1-rn3] sn=sn3 haPort=node3:9010
partitions=1-300

```

Note

If one or more of your Storage Nodes stores its data in the root directory, then instead of `plan change-storagedir`, set the `rootDirSize` parameter instead. For example:

```
kv-> plan change-parameters -service sn1 -params rootDirSize=200_gb
```

Replacing a Failed Storage Node

If a Storage Node has failed, or is in the process of failing, you can replace the Storage Node. Upgrading a healthy machine to another one with better specifications is also a common Storage Node replacement scenario. Generally, you should repair the underlying problem (be it hardware or software related) before proceeding with this procedure.

There are two ways to replace a failed Storage Node.

To replace a failed Storage Node by using a new, different Storage Node (node uses different host name, IP address, and port as the failed host):

1. If you are replacing hardware, bring it up and make sure it is ready for your production environment.

2. On the new, replacement node, create a "boot config" configuration file using the makebootconfig utility. Do this on the hardware where your new Storage Node runs.

To create the "boot config" file, issue the following commands:

```
> mkdir -p KVRROOT      (if it doesn't already exist)
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar makebootconfig -root KVRROOT \
                                           -port 5000 \
                                           -host <hostname> \
                                           -harange 5010,5020 \
```

3. Use the securityconfig tool to create the security directory. For more information, see [Steps to Configure KVSTORE Installation \(page 6\)](#). Copy the security directory from the healthy node to the failed node:

```
scp -r node02:KVRROOT/security KVRROOT/
```

4. Start the Oracle NoSQL Database software on the new node:

```
> nohup java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar start -root KVRROOT &
```

5. Deploy the new Storage Node to the new node. To do this using the CLI:

```
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar runadmin \
-port <5000> -host <host> \
-security USER/admin.security
kv-> plan deploy-sn -zn <id> -host <host> -port <5000> -wait
kv->
```

6. Add the new Storage Node to the Storage Node pool. (You created a Storage Node pool when you installed the store, and you added all your Storage Nodes to it, but it is otherwise not used in this version of the product.)

```
kv-> show pools
AllStorageNodes: sn1, sn2, sn3, sn4 ... sn25, sn26
BostonPool: sn1, sn2, sn3, sn4 ... sn25
kv-> pool join -name BostonPool -sn sn26
AllStorageNodes: sn1, sn2, sn3, sn4 ... sn25, sn26
BostonPool: sn1, sn2, sn3, sn4 ... sn25
kv->
```

7. Make sure the old Storage Node is not running. If the problem is with the hardware, then turn off the broken machine. You can also stop just the Storage Node software by:

```
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar stop -root KVRROOT &
```

8. Migrate the services from one Storage Node to another. The syntax for this plan is:

```
kv-> plan migrate-sn -from <old SN ID> -to <new SN ID>
```

Assuming that you are migrating from Storage Node 25 to 26, you would use:

```
kv-> plan migrate-sn -from sn25 -to sn26
```

9. The old Storage Node is shown in the topology and is reported as UNREACHABLE. The source SNA should be removed and its rootdir should be hosed out. Bringing up the old SNA will also bring up the old Replication Nodes and admins, which are no longer members of their replication groups. This should be harmless to the rest of the store, but it produces log error messages that might be misinterpreted as indicating a problem with the store. Use the `plan remove-sn` command to remove the old and unused Storage Node in your deployment.

```
kv-> plan remove-sn sn25 -wait
```

Note

Replacing a Storage Node qualifies as a topology change. This means that if you want to restore your store from a snapshot taken before the Storage Node was replaced, you must use the Load program. See [Using the Load Program \(page 63\)](#) for more information.

To replace a failed Storage Node by using an identical node (node uses the same host name, internet address, and port as the failed host):

1. Prerequisite information:
 - a. A running Admin process on a known host, with a known registry port.
 - b. The ID of the Storage Node to replace (e.g. "sn1").
 - c. Before starting the new Storage Node, the SN to be replaced must be taken down. This can be done administratively or via failure.

Note

It is recommended that the KVROOT is empty and that you do a full network recovery of data before proceeding.

The instructions below assume that the KVROOT is empty and has no valid data. When the new Storage Node Agent begins it starts the services it hosts, which recovers their data from other hosts. This recovery may take some time, depending on the size of the shards involved and it happens in the background.

2. Create the configuration using the `generateconfig` command:

The `generateconfig`'s usage is:

```
> java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar generateconfig \  
-host <hostname> -port <port> -sn <StorageNodeId> -target <zipfile> \  
-security <path to security login file>
```

For example:

```
> java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar generateconfig -host adminhost \  
-port 13230 -sn sn1 -target /tmp/sn1.config.zip \  
-security USER/security/admin.security
```

The command above creates the target "/tmp/sn1.config.zip" which is a zip file with the required configuration to re-create that Storage Node. The top-level directory in the zip file is the store's KVROOT.

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

3. Restore the Storage Node configuration on the target host:
 - a. Copy the zip file to the target host.
 - b. Unzip the archive into your KVROOT directory. That is, if KVROOT is /opt/kvroot, then do the following:

```
> cd/opt  
> unzip <path-to-sn1.config.zip>
```

4. Restart the Storage Node on the new host.

```
> java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar start -root KVROOT
```

Replacing a Failed Disk

If a disk has failed, or is in the process of failing, you can replace the disk. Disk replacement procedures are necessary to keep the store running. This section walks you through the steps of replacing a failed disk, to preserve data availability.

The following example deploys a KVStore to a set of three machines, each with 3 disks. Use the `storagedir` flag of the `makebootconfig` command to specify the storage location of the other two disks.

```
> java -jar KVHOME/lib/kvstore.jar makebootconfig \  
-root /opt/ondb/var/kvroot \  
-port 5000 \  
-host node09  
-h.arange 5010,5020 \  
-num_cpus 0 \  
-memory_mb 0 \  
-capacity 3 \  
-storagedir /disk1/ondb/data \  
-storagedir /disk2/ondb/data \  
-storagedir /disk3/ondb/data
```

With a boot configuration such as that shown above, the directory structure that is created and populated on each machine would then be:

- Machine 1 (SN1) -	- Machine 2 (SN2) -	- Machine 3 (SN3) -
/opt/ondb/var/kvroot	/opt/ondb/var/kvroot	/opt/ondb/var/kvroot
/security	/security	/security
log files	log files	log files
/store-name	/store-name	/store-name
/log	/log	/log
/sn1	/sn2	/sn3
config.xml	config.xml	config.xml
/admin1	/admin2	/admin3
/env	/env	/env
/disk1/ondb/data	/disk1/ondb/data	/disk1/ondb/data
/rg1-rn1	/rg1-rn2	/rg1-rn3
/env	/env	/env
/disk2/ondb/data	/disk2/ondb/data	/disk2/ondb/data
/rg2-rn1	/rg2-rn2	/rg2-rn3
/env	/env	/env

In this case, configuration information and administrative data is stored in a location that is separate from all of the replication data. The replication data itself is stored by each distinct Replication Node service on separate, physical media as well. Storing data in this way provides failure isolation and will typically make disk replacement less complicated and time consuming. For information on how to deploy a store, see [Configuring the KVStore \(page 12\)](#).

To replace a failed disk:

1. Determine which disk has failed. To do this, you can use standard system monitoring and management mechanisms. In the previous example, suppose disk2 on Storage Node 3 fails and needs to be replaced.
2. Then given a directory structure, determine which Replication Node service to stop. With the structure described above, the store writes replicated data to disk2 on Storage Node 3, so rg2-rn3 must be stopped before replacing the failed disk.
3. Use the plan stop-service command to stop the affected service (rg2-rn3) so that any attempts by the system to communicate with it are no longer made; resulting in a reduction in the amount of error output related to a failure you are already aware of.

```
kv-> plan stop-service -service rg2-rn3
```

4. Remove the failed disk (disk2) using whatever procedure is dictated by the operating system, disk manufacturer, and/or hardware platform.
5. Install a new disk using any appropriate procedures.
6. Format the disk to have the same storage directory as before; in this case, /disk2/ondb/var/kvroot.

7. With the new disk in place, use the `plan start-service` command to start the `rg2-rn3` service.

```
kv-> plan start-service -service rg2-rn3
```

Note

It can take a considerable amount of time for the disk to recover all of its data, depending on the amount of data that previously resided on the disk before failure. It is also important to note that the system may encounter additional network traffic and load while the new disk is being repopulated.

Repairing a Failed Zone by Replacing Hardware

If all of the machines belonging to a zone fail, and quorum is maintained, you can replace them by using new, different Storage Nodes deployed to the same zone.

If a zone fails but quorum is lost, you can perform a failover instead. To do this, see [Performing a failover \(page 105\)](#).

For example, suppose a store consists of three zones; `zn1`, deployed to the machines on the first floor of a physical data center, `zn2`, deployed to the machines on the second floor, and `zn3`, deployed to the third floor. Additionally, suppose that a fire destroyed all of the machines on the second floor, resulting in the failure of all of the associated Storage Nodes. In this case, you need to replace the machines in the `zn2` zone; which can be accomplished by doing the following:

1. Replace each individual Storage Node in the failed zone with new, different Storage Nodes belonging to same zone (`zn2`), although located in a new physical location. To do this, follow the instructions in [Replacing a Failed Storage Node \(page 79\)](#). Make sure to remove each old Storage Node after performing the replacement.
2. After replacing and then removing each of the targeted SNs, the zone to which those SNs belonged should now contain the new SNs.

Disabling Storage Node Agent Hosted Services

To disable all services associated with a stopped SNA use the `-disable-services` flag. This helps isolate failed services to avoid hard rollbacks during a failover. Also, in this way, the configuration can be updated during recovery after a failover. The usage is:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar {start | stop | restart}  
[-disable-services] [-verbose]  
-root KVROOT [-config <bootstrapFileName>]
```

where:

- `start -disable-services`

Starts an Oracle NoSQL Database Storage Node Agent with all of its hosted services disabled. If the SNA is already running, the command will fail.

- `stop -disable-services`

Stops an Oracle NoSQL Database Storage Node Agent, marking all of its services disabled so that they will not start when starting up the SNA in the future or until the services are reenabled.

- `restart -disable-services`

Restarts an Oracle NoSQL Database Storage Node Agent with all of its hosted services disabled.

Verifying the Store

Verification is a tool you can use to:

- Perform general troubleshooting of the store.

Verification inspects all components of the store. It also checks whether all store services are available, and for those services it checks whether there are any version or metadata mismatches.

- Check the status of a long-running plan

Some plans require many steps and may take some time to execute. The administrator can verify plans to check on progress of the plan, or as an aid to diagnose a plan that is in an ERROR state. For example, if you can verify a Deploy Store plan while it is running against many Storage Nodes. You can watch the verify report at each iteration to see that more and more nodes have created and have come online.

For more information on how to manage plans, see [Plans \(page 9\)](#).

- Provide additional information about a plan that is in an ERROR state.

You run store verification using the `verify` command in the CLI. It requires no parameters, and by default it runs in verbose mode. For example:

```
kv-> verify configuration
Verify: starting verification of store MetroArea based upon
topology sequence #117
100 partitions and 6 storage nodes
Time: 2015-06-16 00:01:05 UTC   Version: 12.1.4.3.5
See node01:Data/virtualroot/datacenter1/kvroot/MetroArea/
                                log/MetroArea_{0..N}.log for
                                progress messages
Verify: Shard Status: healthy:2 writable-degraded:0
                                read-only:0 offline:0
Verify: Admin Status: healthy
Verify: Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
    RN Status: online:2 offline: 0 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
    RN Status: online:2 offline: 0 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
```



```
RN Status: online:2 offline: 0
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:5000
      Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin1] Status: RUNNING,MASTER
Verify:      Rep Node [rg1-rn2] Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:5011 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn2 ==
Verify: Storage Node [sn2] on node02:6000
      Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn2] Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:6010 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:7000
      Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin2] Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn3] Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:7011 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn4 ==
Verify: Storage Node [sn4] on node04:8000
      Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn3] Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:8010 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn5 ==
Verify: Storage Node [sn5] on node05:9000
      Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin3] Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn1] Status: RUNNING,MASTER
      sequenceNumber:127 haPort:9011
Verify: == checking storage node sn6 ==
Verify: Storage Node [sn6] on node06:10000
      Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn1] Status: RUNNING,MASTER
      sequenceNumber:127 haPort:10010

Verification complete, no violations.
```

A silent mode is available which shows only problems.

```
kv-> verify configuration -silent
Verify: starting verification of store MetroArea based upon
topology sequence #117
100 partitions and 6 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
See node01:Data/virtualroot/datacenter1/kvroot/MetroArea/
log/MetroArea_{0..N}.log for progress messages
Verification complete, no violations.
```

Problems with the store are clearly reported. For example, if a Storage Node is unavailable, then in silent mode that problem is displayed in the following way:

```
kv-> verify configuration -silent
Verify: starting verification of store MetroArea based upon
topology sequence #117
100 partitions and 6 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
See node01:Data/virtualroot/datacenter1/kvroot/MetroArea/
log/MetroArea_{0..N}.log for progress messages
Verification complete, 2 violations, 0 notes found.
Verification violation: [rg2-rn2] ping() failed for rg2-rn2 :
Unable to connect to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host: node02;
    nested exception is:
    java.net.ConnectException: Connection refused
Verification violation: [sn2] ping() failed for sn2 : Unable to connect
to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host: node02;
    nested exception is:
    java.net.ConnectException: Connection refused
```

In verbose mode, the above problem is shown in the following way:

```
kv-> verify configuration
Verify: starting verification of store MetroArea based upon
topology sequence #117
100 partitions and 6 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
See node01:Data/virtualroot/datacenter1/kvroot/MetroArea/
log/MetroArea_{0..N}.log for progress messages
Verify: Shard Status: healthy:1 writable-degraded:1
read-only:0 offline:0
Verify: Admin Status: healthy
Verify: Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline: 1 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
RN Status: online:2 offline: 0 maxDelayMillis:1 maxCatchupTimeSecs:0
Verify: Zone [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
```

```

RN Status: online:2 offline: 0
Verify: == checking storage node sn1 ==
Verify: Storage Node [sn1] on node01:5000
      Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin1]      Status: RUNNING,MASTER
Verify:      Rep Node [rg1-rn2]   Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:5011 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn2 ==
Verify:      sn2: ping() failed for sn2 :
Unable to connect to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
      java.rmi.ConnectException: Connection refused to host: node02;
      nested exception is:
      java.net.ConnectException: Connection refused
Verify: Storage Node [sn2] on node02:6000
      Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
      UNREACHABLE
Verify:      rg2-rn2: ping() failed for rg2-rn2 :
Unable to connect to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
      java.rmi.ConnectException: Connection refused to host: node02;
      nested exception is:
      java.net.ConnectException: Connection refused
Verify:      Rep Node [rg2-rn2]   Status: UNREACHABLE
Verify: == checking storage node sn3 ==
Verify: Storage Node [sn3] on node03:7000
      Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin2]      Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn3]   Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:7011 delayMillis:1 catchupTimeSecs:0
Verify: == checking storage node sn4 ==
Verify: Storage Node [sn4] on node04:8000
      Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Rep Node [rg2-rn3]   Status: RUNNING,REPLICA
      sequenceNumber:127 haPort:8010 delayMillis:0 catchupTimeSecs:0
Verify: == checking storage node sn5 ==
Verify: Storage Node [sn5] on node05:9000
      Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
      Status: RUNNING
      Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify:      Admin [admin3]      Status: RUNNING,REPLICA
Verify:      Rep Node [rg1-rn1]   Status: RUNNING,MASTER
      sequenceNumber:127 haPort:9011

```

```

Verify: == checking storage node sn6 ==
Verify: Storage Node [sn6] on node06:10000
Zone: [name=Queens id=zn3 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: db9ec397225c
Verify: Rep Node [rg2-rn1] Status: RUNNING,MASTER
sequenceNumber:127 haPort:10010

Verification complete, 2 violations, 0 notes found.
Verification violation: [rg2-rn2] ping() failed for rg2-rn2 :
Unable to connect to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host: node02;
nested exception is:
    java.net.ConnectException: Connection refused
Verification violation: [sn2] ping() failed for sn2 :
Unable to connect to the storage node agent at host node02, port 6000,
which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host: node02;
nested exception is:
    java.net.ConnectException: Connection refused

```

Note

The verify output is only displayed in the shell when the command is finished. You can tail or grep the Oracle NoSQL Database log file in order to get a sense of how the verify is progressing. Look for the string Verify. For example:

```
grep Verify /KVRT1/mystore/log/mystore_0.log
```

Monitoring the Store

Information about the performance and availability of your store can be obtained both from a server side and client side perspective:

- Your Oracle NoSQL Database applications can obtain performance statistics using the `oracle.kv.KVStore.getStats()` class. This provides a client side view of the complete round trip performance for Oracle NoSQL Database operations.
- Oracle NoSQL Database automatically captures Replication Node performance statistics into a log file that can easily be imported and analyzed with spreadsheet software. Statistics are tracked, logged and written at a user specified interval to a CSV file (`je.stat.csv`) in the Environment directory. The logging occurs per-Environment when the Environment is opened in read/write mode.

Configuration parameters control the size and number of rotating log files used (similar to java logging, see [java.util.logging.FileHandler](#)). For a rotating set of files, as each file reaches a given size limit, it is closed, rotated out, and a new file is opened. Successively older files are named by adding "0", "1", "2", etc. into the file name. The format is `je.stat[version number].csv`

- The Oracle NoSQL Database administrative service collects and aggregates status information, alerts, and performance statistics components that are generated in the store. This provides a detailed, server side view of behavior and performance of the Oracle NoSQL Database server.
- Each Oracle NoSQL Database Storage Node maintains detailed logs of trace information from the services that are housed on that node. The administrative service presents an aggregated, store-wide view of these component logs, but the logs are nevertheless available on each Storage Node in the event that the administrative service is somehow not available, or if it is more convenient to examine the individual logs.
- Oracle NoSQL Database allows Java Management Extensions (JMX) agents to be optionally available for monitoring. The JMX interfaces allow you to poll the Storage Nodes for information about the storage node and about any replication nodes that are hosted on the Storage Node. For more information on JMX monitoring, see [Standardized Monitoring Interfaces \(page 112\)](#). For information on using JMX securely, see [Guidelines for using JMX securely](#) section in the *Oracle NoSQL Database Security Guide*.

You can monitor the status of the store by verifying it from within the CLI. See [Verifying the Store \(page 85\)](#) for more information. You can also use the CLI to examine events.

Events

Events are special messages that inform you of the state of your system. As events are generated, they are routed through the monitoring system so that you can see them. There are four types of events that the store reports:

1. State Change events are issued when a service starts up or shuts down.
2. Performance events report statistics about the performance of various services.
3. Log events are records produced by the various system components to provide trace information about debugging. These records are produced by the standard `java.util.logging` package.
4. Plan Change events record the progress of plans as they execute, are interrupted, fail or are canceled.

Note that some events are considered critical. These events are recorded in the administration service's database, and can be retrieved and viewed using the CLI.

Other Events

Plan Change events cannot be directly viewed through Oracle NoSQL Database's administrative interfaces. However, State Change events, Performance events, and Log events are recorded using the EventRecorder facility internal to the Admin. Only events that are considered "critical" are recorded, and the criteria for being designated as such vary with the type of the event. All state change events are considered critical, but only SEVERE log events are. Performance events are considered critical if the reported performance is below a certain threshold.

All such events can be viewed in the CLI using the `show events` and `show event` commands.

Use the CLI `show events` command with no arguments to see all the unexpired events in the database. You can bound the range of events that are displayed using the `-from` and `-to` arguments. You can filter events by type or id as well, using either the `-type` or the `-id` arguments respectively.

For example, this is a fragment of the output from the `show events` command:

```
kv-> show events
idarpdfbS STAT 2015-08-13 22:18:39.287 UTC sn1 RUNNING sev1
idarpeg0S STAT 2015-08-13 22:18:40.608 UTC sn2 RUNNING sev1
idarphmuS STAT 2015-08-13 22:18:44.742 UTC rg1-rn1 RUNNING sev1
idarpjLLS STAT 2015-08-13 22:18:47.289 UTC rg1-rn2 RUNNING sev1
idartfcuS STAT 2015-08-13 22:21:48.414 UTC rg1-rn2 UNREACHABLE sev2
                                     (reported by admin1)
```

This shows four service state change events (sev1) and one UNREACHABLE (sev2) log event. The tags at the beginning of each line are individual event record identifiers. If you want to see detailed information for a particular event, you can use the "show event" command, which takes as its argument an event record identifier:

```
kv-> show event -id idartfcuS
idartfcuS STAT 2015-08-13 22:21:48.414 UTC rg1-rn2 UNREACHABLE sev2
                                     (reported by admin1)
```

and so on, for a complete stack trace.

Events expire from the system after a set period, which defaults to thirty days.

The Sev1 flag is associated with the following service status change events: STARTING, WAITING_FOR_DEPLOY, RUNNING, STOPPING and STOPPED. Sev2 is associated with the ERROR_RESTARTING, ERROR_NO_RESTART and UNREACHABLE service status change events.

Setting Store Parameters

The three Oracle NoSQL Database service types; Admin, Storage Node and Replication Node; have configuration parameters, some of which can be tweaked after the service is deployed. To see the parameter values that can be changed, you use the following command in the CLI:

```
show parameters -service <id>
```

This command allows you to display service parameters and state for the specified service. The service may be a Replication Node, a Storage Node, or Admin service, as identified by any valid string. You can use the `-policy` optional flag to show global policy parameters.

Changing Parameters

All of the CLI commands used for creating parameter-changing plans share a similar syntax:

```
plan change-parameters -service <id>...
```

All such commands can have multiple `ParameterName=NewValue` assignment arguments on the same command line. If `NewValue` contains spaces, then the entire assignment argument

must be quoted within double quote marks. For example, to change the Admin parameter `collectorPollPeriod`, you would issue the command:

```
kv-> plan change-parameters -all-admins -params \
    "collectorPollPeriod=20 SECONDS"
```

The following commands are used to change service parameters:

- `plan change-parameters -service <shardId-nodeId> -params [assignments]`

This command is used to change the parameters of a single Replication Node, which must be identified using the shard and node numbers. The `shardId-nodeId` identifier must be given as a single argument with one embedded hyphen and no spaces. The `shardId` identifier is represented by `rgX`, where `X` refers to the shard number.

- `plan change-parameters -all-rns -params [assignments]`

This command is used to change the parameters of all Replication Nodes in a store. No Replication Node identifier is needed in this case.

- `plan change-parameters -service <storageNodeId> -params [assignments]`

This command is used to change the parameters of a single Storage Node instance. The `storageNodeId` is a simple integer.

- `plan change-parameters -all-admins -params [assignments]`

This command is used to change Admin parameters. Because each instance of Admin is part of the same replicated service, all instances of the Admin are changed at the same time, so no Admin identifier is needed in this command.

If an Admin parameter change requires the restarting of the Admin service, KVAdmin loses its connection to the server. Under normal circumstances, KVAdmin automatically reconnects after a brief pause, when the next command is given. At this point the plan is in the `INTERRUPTED` state, and must be completed manually by issuing the `plan execute` command.

- `plan change-parameters -security <id>`

This command is used to change security parameters. The parameters are applied implicitly and uniformly across all SNs, RNs and Admins.

In all cases, you can choose to create a plan and execute it; or to create the plan and execute it in separate steps by using the `-noexecute` option of the `plan` command.

Setting Store Wide Policy Parameters

Most admin, Storage Node, and replication node parameters are assigned to default values when a store is deployed. It can be inconvenient to adjust them after deployment, so Oracle NoSQL Database provides a way to set the defaults that are used during deployment. These defaults are called store-wide Policy parameters.

You can set policy parameters in the CLI by using this command:

```
change-policy -params [name=value]
```

The parameters to change follow the `-params` flag and are separated by spaces. Parameter values with embedded spaces must be separated by spaces. Parameter values with embedded spaces must be quoted. For example: `name = "value with spaces"`. If the optional `dry-run` flag is specified, the new parameters are returned without changing them.

Admin Parameters

The following parameters can be set for the Admin service:

- `adminLogFileCount=<Integer>`

Sets the number of log files that are kept. This value defaults to "20". It is used to control the amount of disk space devoted to logging history.

- `adminLogFileLimit=<Integer>`

Limits the size of log files. After reaching this limit, the logging subsystem switches to a new log file. This value defaults to "4,000,000" bytes. The limit specifies an approximate maximum amount to write (in bytes) to any one file. If the value is zero, then there is no limit.

- `collectorPollPeriod=<Long TimeUnit>`

Sets the Monitor subsystem's delay for polling the various services for status updates. This value defaults to "20" seconds. Units are supplied as a string in the `change-parameters` command, for example: `-params collectorPollPeriod="2 MINUTES"`

- `loggingConfigProps=<String>`

Property settings for the Logging subsystem in the Admin process. Its format is `property=value;property=value...`. Standard `java.util.logging` properties can be set by this parameter.

- `eventExpiryAge=<Long TimeUnit>`

You can use this parameter to adjust how long the Admin stores critical event history. The default value is "30 DAYS".

- `configProperties=<String>`

This is an omnibus string of property settings for the underlying BDB JE subsystem. Its format is `property=value;property=value...`

- `javaMiscParams=<String>`

This is an omnibus string that is added to the command line when the Admin process is started. It is intended for setting Java VM properties, such as `-Xmx` and `-Xms` to control the

heap size. If the string is not a valid sequence of tokens for the JVM command line, the Admin process fails to start.

Storage Node Parameters

The following parameters can be set for Storage Nodes:

- `serviceLogFileCount=<Integer>`

Sets the number of log files that are kept, for this Storage Node and for all Replication Nodes hosted on this Storage Node. This value defaults to "20". It is used to control the amount of disk space devoted to logging history.

- `serviceLogFileLimit=<Integer>`

Limits the size of log files. After reaching this limit, the logging subsystem switches to a new log file. This setting applies to this Storage Node and to all Replication Nodes hosted on this Storage Node. This value defaults to "2,000,000" bytes. The limit specifies an approximate maximum amount to write (in bytes) to any one file. If the value is zero, then there is no limit.

- `haPortRange=<String>`

Defines the range of port numbers available for assigning to Replication Nodes that are hosted on this Storage Node. A port is allocated automatically from this range when a Replication Node is deployed. The format of the value string is "lowport,highport".

- `haHostname=<String>`

Sets the name of the network interface used by the HA subsystem. A valid string for a hostname can be a DNS name or an IP address.

- `capacity=<Integer>`

Sets the number of Replication Nodes that can be hosted on this Storage Node. This value is used to inform decisions about where to place new Replication Nodes. Capacity can be set to values greater than 1 when the Storage Node has sufficient disk, CPU, and memory to support multiple Replication Nodes. Default value: "1".

If capacity is set to 0, then this Storage Node may be used to host Arbiter Nodes. The pool of Storage Nodes in a zone configured to host Arbiter Nodes are used for Arbiter Node allocation. For more information see [Deploying an Arbiter Node Enabled Topology \(page 45\)](#).

- `memoryMB=<Integer>`

Sets the amount of memory known to be available on this Storage Node, in megabytes. Defaults to "0", which means "unknown." and is determined automatically by the store as the total amount of RAM available on the machine.

You should not need to change this parameter under normal circumstances. Set it to a value less than the amount of RAM, if the machine has other applications running on it (not a recommended configuration) in order to reserve some memory for the other applications.

- numCPUs=<Integer>

Sets the number of CPUs known to be available on this Storage Node. Default value: 1.

- rnHeapPercent=<Integer>

Sets the percentage of a Storage Node's memory reserved for heap, for all RN processes hosted on this SN. Default value: 85.

- rnHeapMaxMB=<Integer>

Sets a hard limit for the maximum size of the Replication Node's Java VM heap. Default value is 0, which means the VM-specific limit is used. The default is roughly 32 GB, which represents the largest heap size that can make use of compressed object references.

Do not set this value to greater than 32 GB. Doing so can adversely impact your Replication Node's performance.

Settings larger than the maximum size that supports compressed object references will maintain the default limit unless the size is large enough that the heap can reference a larger number of objects given the increased memory requirements for uncompressed object references. Using these larger heap sizes is also not recommended.

- systemPercent=<Integer>

Sets the percentage of the Storage Node's memory which will be used for operating system purposes. This memory is used by the operating system for purposes such as the file system cache, page mapping tables, file system handles, thread stacks, and so forth.

If this parameter is set to a value less than 100, then the off-heap cache might be used if there is memory left over after allowing for the heap and system use. See [Managing the Off-heap Cache \(page 220\)](#) for details.

Default value is 100.

- mgmtClass=<String>

The name of the class that provides the Management Agent implementation. See [Standardized Monitoring Interfaces \(page 112\)](#) for more information. The port cannot be a privileged port number (<1024).

- servicePortRange=<String>

Sets the range of ports used for communication among administrative services running on a Storage Node and its managed services. This parameter is optional. By default the services use anonymous ports. The format of the value string is "startPort,endPort."

The range needs to be large enough to accommodate the Storage Node, all the Replication Nodes (as defined by the capacity parameter), Admin and Arbiter services hosted on the machine, as well as JMX, if enabled. The number of ports required also depends on whether the system is configured for security. For a non-secure system, the Storage Node consumes

1 port (which will be shared with the port assigned separately for the Registry Service, if it overlaps the service port range), and each Replication Node consumes 1 port in the range. An Admin, if configured, consumes 1 port. Arbiters also each consume 1 port. If JMX is enabled, that consumes 1 additional port. On a secure system, two additional ports are required for the Storage Node and two for the Admin. As a general rule, if possible, it is good practice to specify a range that is significantly larger than the minimum to allow for increases in Storage Node capacity or network problems that may render ports temporarily unavailable.

Note that the ports specified in the service port range should not overlap with the admin port or with ports in the HA range. The service port range can include the registry port, though, and the registry and Storage Node will share a port in that case.

For a non-secure system, you can use the following formula to arrive at an estimate for the port range size number:

```
1 (Storage Node) +
capacity (the number of Replication Nodes) +
Arbiters (the number of Arbiter Nodes) +
1 (if the Storage Node is hosting an admin) +
1 (if the Storage Node is running JMX)
```

For example, if a Storage Node has capacity 1, it is hosting an admin process, and neither Arbiters nor JMX are in use, the range size must be at least 3. You may want to increase the range size beyond this minimum. Doing so allows for safety and expansion of the Storage Node without requiring future changes to this parameter. If capacity were 2, the range size must be greater than or equal to 4.

If you are deploying a secure Oracle NoSQL Database then you can use the following formula to arrive at an estimate for the port range size number:

```
3 (Storage Nodes) +
capacity (the number of Replication Nodes) +
Arbiters (the number of Arbiter Nodes) +
3 (if the Storage Node is hosting an admin) +
1 (if the Storage node is running JMX)
```

where an additional port was added for each Storage Node, Replication Node or the Admin (if configured).

For more information on configuring Oracle NoSQL Database securely, see the *Oracle NoSQL Database Security Guide*.

- `rootDirPath=<path>`

The path to the Storage Node's root directory.

- `rootDirSize=<String>`

Sets the storage size the root directory. Use for heterogeneous installation environments where some Storage Nodes have more disk capacity than others. In that case, this parameter should be used only for those Storage Nodes that place data in the root directory.

If the Storage Nodes use some other directory (such as might be specified using `plan change-storagedir`) then do not use this parameter.

See [Managing Storage Directory Sizes \(page 77\)](#) for more information.

The value specified for this parameter must be a long, followed optionally by a unit string. Accepted unit strings are: KB, MB, GB, and TB, corresponding to 1024 , 1024^2 , 1024^3 , 1024^4 respectively. Acceptable strings are case insensitive. Valid delimiters between the long value and the unit string are `" "`, `"-"`, or `"_"`.

Note

When setting this parameter, no run-time checks are performed to verify that the actual directory size is greater than or equal to the specified size.

Replication Node Parameters

The following parameters can be set for Replication Nodes:

- `collectEnvStats=<Boolean>`

If true, then the underlying BDB JE subsystem dumps statistics into the `.stat` file. This information is useful for tuning JE performance. Oracle Support may request these statistics to aid in tuning or to investigate a problem.

- `maxTrackedLatency=<Long TimeUnit>`

The highest latency that is included in the calculation of latency percentiles.

- `configProperties=<String>`

Contains property settings for the underlying BDB JE subsystem. Its format is `property=value;property=value...`

- `javaMiscParams=<String>`

A string that is added to the command line when the Replication Node process is started. It is intended for setting Java VM properties, such as `-Xmx` and `-Xms` to control the heap size. If the string is not a valid sequence of tokens for the JVM command line, the Admin process fails to start.

- `loggingConfigProps=<String>`

Contains property settings for the Logging subsystem. The format of this string is like that of `configProperties`, above. Standard `java.util.logging` properties can be set by this parameter.

- `cacheSize=<Long>`

Sets the cache size in the underlying BDB JE subsystem. The units are bytes. The size is limited by the java heap size, which in turn is limited by the amount of memory available on the machine. You should only ever change this low level parameter under explicit directions from Oracle support.

- `latencyCeiling=<Integer>`

If the Replication Node's average latency exceeds this number of milliseconds, it is considered an "alertable" event. If JMX monitoring is enabled, the event also causes an appropriate notification to be sent.

- `throughputFloor=<Integer>`

Similar to `latencyCeiling`, `throughputFloor` sets a lower bound on Replication Node throughput. Lower throughput reports are considered alertable. This value is given in operations per second.

- `rnCachePercent=<Integer>`

The portion of an RN's memory set aside for the JE environment cache.

Global Parameters

The following store-wide non-security parameters can be implicitly and uniformly set across all Storage Nodes, Replication Nodes and Admins:

`collectorInterval =<Long TimeUnit>`

Sets the collection period for latency statistics at each component. This value defaults to "20" seconds. Values like average interval latencies and throughput are averaged over this period of time.

Security Parameters

The following store-wide security parameters can be implicitly and uniformly set across all Storage Nodes, Replication Nodes and Admins:

- `sessionTimeout=<Long TimeUnit>`

Specifies the length of time for which a login session is valid, unless extended. The default value is 24 hours.

- `sessionExtendAllowed=<Boolean>`

Indicates whether session extensions should be granted. Default value is true.

- `accountErrorLockoutThresholdInterval=<Long TimeUnit>`

Specifies the time period over which login error counts are tracked for account lockout monitoring. The default value is 10 minutes.

- `accountErrorLockoutThresholdCount=<Integer>`

Number of invalid login attempts for a user account from a particular host address over the tracking period needed to trigger an automatic account lockout for a host. The default value is 10 attempts.

- `accountErrorLockoutTimeout=<Long TimeUnit>`

Time duration for which an account will be locked out once a lockout has been triggered. The default value is 30 minutes.

- loginCacheTimeout=<Long TimeUnit>

Time duration for which KVStore components cache login information locally to avoid the need to query other servers for login validation on every request. The default value is 5 minutes.

The following password security parameters can be set:

Parameter Name	Value Range and Type	Description
passwordAllowedSpecial	Sub set or full set of #\$_%&'()*+,-./:;<=>?@[^_`{ }~ (string)-	Lists the allowed special characters.
passwordComplexityCheck	[true false] (boolean)	Whether to enable the password complexity checking. The default value is true.
passwordMaxLength	1 - 2048 (integer)	The maximum length of a password. The default value is 256.
passwordMinDigit	0 - 2048 (integer)	The minimum required number of numeric digits. The default value is 2.
passwordMinLength	1 - 2048 (integer)	The Minimum length of a password. The default value is 9.
passwordMinLower	0 - 2048 (integer)	The minimum required number of lower case letters. The default value is 2.
passwordMinSpecial	0 - 2048 (integer)	The minimum required number of special characters. The default value is 2.
passwordMinUpper	0 - 2048 (integer)	The minimum required number of upper case letters. The default value is 2.
passwordNotStoreName	[true false] (boolean)	If true, password should not be the same as current store name, nor is it the store name spelled backwards or with the numbers 1-100 appended. The default value is true.
passwordNotUserName	[true false] (boolean)	If true, password should not be the same as current user name, nor is it the user name

Parameter Name	Value Range and Type	Description
		spelled backwards or with the numbers 1-100 appended. The default value is true.
passwordProhibited	list of strings separated by comma (string)	Simple list of words that are not allowed to be used as a password. The default reserved words are: oracle,password,user,nosql.
passwordRemember	0 - 256 (integer)	The maximum number of passwords to be remembered that are not allowed to be reused when setting a new password. The default value is 3.

For more information on top-level, transport, and password security parameters see the *Oracle NoSQL Database Security Guide*.

Admin Restart

Changes to the following Oracle NoSQL Database parameters will result in a Admin restart by the Storage Node Agent:

Admin parameters:

- adminLogFileCount
- adminLogFileLimit
- configProperties
- javaMiscParams
- loggingConfigProps
- adminHttpPort

For example:

```
kv-> plan change-parameters -all-admins
-params adminLogFileCount=10
Started plan 14. Use show plan -id 14 to check status.
      To wait for completion, use plan wait -id 14
kv-> show plan -id 14
Plan Change Admin Params (14)
Owner: null
State:                                INTERRUPTED
Attempt number:                        1
Started:                               2013-08-26 20:12:06 UTC
Ended:                                2013-08-26 20:12:06 UTC
```

```

Total tasks:          4
Successful:           1
Interrupted:           1
Not started:           2
Tasks not started
  Task StartAdmin start admin1
  Task WaitForAdminState waits for Admin admin1 to reach RUNNING state
kv-> plan execute -id 14
Started plan 14. Use show plan -id 14 to check status.
      To wait for completion, use plan wait -id 14
kv-> show plan -id 14
Plan Change Admin Params (14)
State:                 SUCCEEDED
Attempt number:         1
Started:                2013-08-26 20:20:18 UTC
Ended:                  2013-08-26 20:20:18 UTC
Total tasks:            2
Successful:              2

```

Note

When you change a parameter that requires an Admin restart using the `plan change-parameters` command, the plan ends in an `INTERRUPTED` state. To transition it to a `SUCCESSFUL` state, re-issue the plan a second time using the `plan execute -id <id>` command.

Replication Node Restart

Changes to the following Oracle NoSQL Database parameters will result in a Replication Node restart by the Storage Node Agent:

Storage Node parameters:

- `serviceLogFileCount`
- `serviceLogFileLimit`
- `servicePortRange`

Replication Node parameters:

- `configProperties`
- `javaMiscParams`
- `loggingConfigProps`

Removing an Oracle NoSQL Database Deployment

There are no scripts or tools available to completely remove a Oracle NoSQL Database installation from your hardware. However, the procedure is simple. On each node (machine) comprising your store:

1. Shut down the Storage Node:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar stop -root KVROOT
```

Note that if an Admin process is running on the machine, this command also stops that process.

2. Physically remove the entire contents of KVROOT:

```
> rm -rf KVROOT
```

Once you have performed this procedure on every machine comprising your store, you have completely removed the Oracle NoSQL Database deployment from your hardware.

Fixing Incorrect Storage Node HA Port Ranges

When you initially configured your installation, you defined a range of ports to be used by the nodes when communication among themselves. (You did this in [Installation Configuration \(page 3\)](#).) This range of ports is called the *HA port range*, where *HA* is short hand for "replication."

If you have specified invalid values for the HA Port Range, you are unable to deploy a Replication Node (RN) or a secondary Administration process (Admin) on any misconfigured Storage Node. You discover the problem when you first attempt to deploy a store or a Admin Replica on a faulty Storage Node. You see these indications that the Replication Node did not come up on this Storage Node:

- The Admin displays an error dialog warning that the Replication Node is in the ERROR_RESTARTING state. The Topology tab also shows this state in red, and after a number of retries, it indicates that the Replication Node is in ERROR_NO_RESTART.
- The plan goes into ERROR state, and its detailed history – available by clicking on the plan in the Admin's Plan History tab, or through the CLI's `show plan <planID>` command – shows an error message like this:

```
Attempt 1  
state: ERROR  
start time: 10-03-11 22:06:12  
end time: 10-03-11 22:08:12  
DeployOneRepNode of rg1-rn3 on sn3/farley:5200 [RUNNING]  
failed. .... Failed to attach to RepNodeService for rg1-rn3,  
see log, /KVRT3/<storename>/log/rg1-rn3*.log, on host  
farley for more information.
```

- The critical events mechanism, accessible through the CLI shows an alert that contains the same error information from the plan history.
- An examination of the specified .log file or the store-wide log displayed in the Admin's Log tab shows a specific error message, such as:

```
[rg1-rn3] Process exiting
```

```
java.lang.IllegalArgumentException: Port number 1 is invalid because  
the port must be outside the range of "well known" ports
```

The misconfiguration can be addressed with the following steps. Some steps must be executed on the physical node which hosts the Oracle NoSQL Database Storage Node, while others can be done from any node which can access the CLI.

1. Using the CLI, cancel the deploy-store or deploy-admin plan which ran afoul of the misconfiguration.
2. On the Storage Node, kill the existing, misconfigured StorageNodeAgentImpl process and all its ManagedProcesses. You can distinguish them from other processes because they have the parameter `-root <KVROOT>`.
3. On the Storage Node, remove all files from the KVROOT directory.
4. On the Storage Node, re-create the Storage Node bootstrap configuration file in the KVROOT directory. For directions on how to do this, see [Installation Configuration \(page 3\)](#).
5. On the Storage Node, restart the Storage Node using the following command:

```
java -Xmx256m -Xms256m  
-jar KVHOME/lib/kvstore.jar restart
```
6. Using the CLI, re-deploy the storage node using the deploy-sn plan.

You can now create and execute a deploy-store or deploy-admin plan, using the same parameters as the initial attempt which uncovered your misconfigured Storage Node.

Chapter 7. Failover and Switchover Operations

Optimal use of available physical datacenters is achieved by deploying your store across multiple zones. This provides fault isolation as each zone has a copy of your complete store, including a copy of all the shards. With this configuration, when a zone fails, write availability is automatically reestablished as long as quorum is maintained.

Note

To achieve other levels of fault isolation, best practices for data center design should be applied. For example, site location, building selection, floor layout, mechanical design, electrical system design, modularity, etc.

However, if quorum is lost, manual procedures such as failovers can be used instead to recover from zone failures. For more information on quorum, see the Oracle NoSQL Database Concepts manual.

A failover is typically performed when the primary zone fails or has become unreachable and one of the secondary zones is transitioned to take over the primary role. Failover can also be performed to reduce the quorum to the available primary zones. Failover may or may not result in data loss.

Switchovers can be used after performing a failover (to restore the original configuration) or for planned maintenance.

A switchover is typically a role reversal between a primary zone and one of the secondary zones of the store. A switchover can also be performed to convert one or more zones to another type for maintenance purposes. Switchover requires quorum and guarantees no data loss. It is typically done for planned maintenance of the primary system.

In this chapter, we explain how failover and switchover operations are performed.

Note

Arbiters are not currently supported during failover and switchover operations.

Repairing a Failed Zone

If a zone fails but quorum is maintained, you have the option to repair the failed zone with new hardware by following the procedure described in [Repairing a Failed Zone by Replacing Hardware \(page 84\)](#).

Another option is to convert the failed zone to a secondary zone. In some cases, this approach can improve the high availability characteristics of the store by reducing the quorum requirements.

For example, suppose a store consists of two primary zones: zone 1 with a replication factor of three and zone 2, with a replication factor of two. Additionally, suppose zone 2 fails. In this case, quorum is maintained because you would have 3 out of the 5 replicas, but any additional failure would result in a loss of quorum.

Converting zone 2 to a secondary zone would reduce the primary replication factor to 3, meaning that each shard could tolerate an additional failure.

You should determine if switching zone types would actually improve availability. If so, then decide if it is worth doing in the current circumstances.

Performing a failover

If quorum is maintained, you do not need to do anything because the store is still performing normally.

In situations where a zone fails but quorum is lost, your only option is to perform a failover.

For example, suppose a store consists of two primary zones, "Manhattan" and "JerseyCity", each deployed in its own physical data center.

Note

For simplicity, this example uses a store with a replication factor of two. In general, a Primary Replication Factor of 3 is adequate for most applications and is a good starting point, because 3 replicas allow write availability if a single primary zone fails.

Additionally, suppose that the "Manhattan" zone fails, resulting in the failure of all of the associated Storage Nodes and a loss of quorum. In this case, if the host hardware of "Manhattan" was irreparably damaged or the problem will take too long to repair you may choose to initiate a failover.

The following steps walk you through the process of verifying failures, isolating Storage Nodes, and reducing admin quorum to perform a failover operation. This process allows service to be continued in the event of a zone failure.

1. Connect to the store. To do this, connect to an admin running in the JerseyCity zone:

```
java -Xmx256m -Xms256m -jar KVHOME/lib/kvstore.jar \  
runadmin -host jersey1 -port 6000 \  
-security USER/security/admin.security
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

2. Use the `verify configuration` command to confirm the failures:

```
kv-> verify configuration  
Connected to Admin in read-only mode  
Verify: starting verification of store mystore based upon  
topology sequence #207  
200 partitions and 2 storage nodes.  
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5  
See jersey1:/kvroot/mystore/log/mystore_{0..N}.log  
for progress messages
```

```

Verify: Shard Status: healthy:0 writable-degraded:0
                                read-only:1 offline:0
Verify: Admin Status: read-only
Verify: Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:0 offline:1
Verify: Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline:0
Verify: == checking storage node sn1 ==
Verify:      sn1: ping() failed for sn1 :
Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
    java.net.ConnectException: Connection refused
Verify: Storage Node [sn1] on nyc1:5000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
      UNREACHABLE
Verify:      admin1: ping() failed for admin1 :
Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
    java.net.ConnectException: Connection refused
Verify:      Admin [admin1]      Status: UNREACHABLE
Verify:      rg1-rn1: ping() failed for rg1-rn1 :
Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
    java.net.ConnectException: Connection refused
Verify:      Rep Node [rg1-rn1] Status: UNREACHABLE
Verify: == checking storage node sn2 ==
Verify: Storage Node [sn2] on jersey1:6000
Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 287a5a28cea4
Verify:      Admin [admin2]
Status: RUNNING,MASTER (non-authoritative)
Verify:      Rep Node [rg1-rn2]
Status: RUNNING,MASTER (non-authoritative)
                                sequenceNumber:217 haPort:6003
Verification complete, 4 violations, 0 notes found.
Verification violation: [admin1]      ping() failed for admin1 :
Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
    java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
    java.net.ConnectException: Connection refused
Verification violation: [rg1-rn1]      ping() failed for rg1-rn1 :

```

```

Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
  java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
      java.net.ConnectException: Connection refused
Verification violation: [sn1] ping() failed for sn1 :
Unable to connect to the storage node agent at host nyc1,
port 5000, which may not be running; nested exception is:
  java.rmi.ConnectException: Connection refused to host:
    nyc1; nested exception is:
      java.net.ConnectException: Connection refused

```

In this case, the Storage Node Agent at host nyc1 is confirmed unavailable.

3. To prevent a hard rollback and data loss, isolate failed nodes (Manhattan) from the rest of the system. Make sure all failed nodes are prevented from rejoining the store until their configurations have been updated.

To do this, you can:

- Disconnect the network physically or use a firewall.
 - Modify the start-up sequence on failed nodes to prevent SNAs from starting.
4. To make changes to the store, you first need to reduce admin quorum. To do this, use the `repair-admin-quorum` command, specifying the available primary zone:

```

kv-> repair-admin-quorum -zname JerseyCity
Connected to admin in read-only mode
Repaired admin quorum using admins: [admin2]

```

Now you can perform administrative procedures using the remaining admin service with the temporarily reduced quorum.

5. Use the `plan failover` command to update the configuration of the store with the available zones.

```

kv-> plan failover -zname \
JerseyCity -type primary \
-zname Manhattan -type offline-secondary -wait
Executing plan 8, waiting for completion...
Plan 8 ended successfully

```

The `plan failover` command fails if it is executed while other plans are still running. You should cancel or interrupt the plans, before executing this plan.

For example, suppose the `topology redistribute` is in progress. If you run the `plan failover` command, it will fail. For it to succeed, you need to first cancel or interrupt the `topology redistribute` command.

To do this, first use the `show plans` command to learn the plan ID of the topology redistribute command. In this case, 9. Then, cancel the topology redistribute command using the `plan cancel` command:

```
kv-> plan cancel -id 9
```

After performing the failover, confirm that the zone type of Manhattan has been changed to secondary using the `ping` command.

```
kv-> ping
Pinging components of store mystore based upon topology sequence #208
200 partitions and 2 storage nodes
Time: 2016-11-21 13:40:37 UTC   Version: 12.1.4.3.5
Shard Status: healthy:0 writable-degraded:1 read-only:0 offline:0
Admin Status: writable-degraded
Zone [name=Manhattan id=zn1 type=SECONDARY allowArbiters=false]
RN Status: online:0 offline:1
Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline:0
Storage Node [sn1] on nyc1:5000
Zone: [name=Manhattan id=zn1 type=SECONDARY allowArbiters=false]
  UNREACHABLE
    Admin [admin1]           Status: UNREACHABLE
    Rep Node [rg1-rn1]       Status: UNREACHABLE
Storage Node [sn2] on jersey1:6000
Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
  Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC   Build id: 508d38507fff
    Admin [admin2]           Status: RUNNING,MASTER
    Rep Node [rg1-rn2]       Status: RUNNING,MASTER
    Status: RUNNING,MASTER sequenceNumber:427 haPort:6011
```

6. The failover operation is now complete. Write availability in the store is reestablished using zone 2 as the only available primary zone. Zone 1 is offline. Any data that was not propagated from zone 1 prior to the failure will be lost.

Note

In this case, the store has only a single working copy of its data, so single node failures in the surviving zone will prevent read and write access, and, if the failure is a permanent one, may produce permanent data loss.

If the problems that led to the failover have been corrected and the original data from the previously failed nodes (Manhattan) is still available, you can return the old nodes to service by performing a switchover. To do this, see the next section.

Performing a Switchover

To continue from the example of the previous section, after performing the failover, you can return the old nodes to service by performing the following switchover procedure:

1. After the failed zones are repaired, restart all the Storage Nodes of the failed zones without starting any services (avoids hard rollback):

```
java -jar KVHOME/lib/kvstore.jar restart -disable-services \  
-root nyc1/KVROOT &
```

Note

When performing planned maintenance, there is no need to isolate nodes or disable services prior to bringing nodes back online.

2. Reestablish network connectivity or reenables the standard startup sequence of the previously failed zones.
3. Repair the topology so that the topology for the newly restarted Storage Nodes can be updated with changes made by the failover.

```
java -Xmx256m -Xms256m -jar KVHOME/lib/kvstore.jar runadmin \  
-host jersey1 -port 5000 \  
-security USER/security/admin.security
```

```
kv-> plan repair-topology -wait  
Executed plan 10, waiting for completion...  
Plan 10 ended successfully
```

Note

This assumes that you must have followed the steps as mentioned in [Configuring Security with Remote Access \(page 19\)](#).

Note

This command will also restart services on the previously failed nodes.

Use the `verify configuration` command to confirm that there are no configuration problems.

4. Run the `ping` command. The "maxCatchupTimeSecs" value will be used for the `-timeout` flag of the `await-consistency` command.

Use the `timeout` flag to specify an estimate of how long the switchover will take. For example, if the nodes have been offline for a long time it might take many hours for them to catch up so that they can be converted back to primary nodes.

```
kv-> ping  
Pinging components of store mystore based upon topology sequence #208  
200 partitions and 2 storage nodes  
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5  
Shard Status: healthy:1 writable-degraded:0 read-only:0 offline:0  
Admin Status: healthy  
Zone [name=Manhattan id=zn1 type=SECONDARY allowArbiters=false]
```



```

RN Status: online:1 offline:0 maxDelayMillis:120000
                                         maxCatchupTimeSecs:1800
Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline:0
Storage Node [sn1] on nyc1:5000
Zone: [name=Manhattan id=zn1 type=SECONDARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 508d38507fff
    Admin [admin1] Status: RUNNING,REPLICA
    Rep Node [rg1-rn1] Status: RUNNING,REPLICA
    sequenceNumber:434 haPort:5011 delayMillis:0 catchupTimeSecs:0
Storage Node [sn2] on jersey1:6000
Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 508d38507fff
    Admin [admin2] Status: RUNNING,MASTER
    Rep Node [rg1-rn2]
    Status: RUNNING,MASTER sequenceNumber:434 haPort:6011

```

In this case, 1800 seconds (30 minutes) is the value to be used.

5. Use the `await-consistency` command to specify the wait time (1800 seconds) used for the secondary zones to catch up with their masters.

The system will only wait five minutes for nodes to catch up when attempting to change a zone's type. If the nodes do not catch up in that amount of time, the plan will fail.

If the nodes will take more than five minutes to catch up, you should run the `await-consistency` command, specifying a longer wait time using the `-timeout` flag. In this case, the wait time (1800 seconds) is used:

```

kv-> await-consistent -timeout 1800 -znname Manhattan
The specified zone is consistent

```

By default, nodes need to have a delay of no more than 1 second to be considered caught up. You can change this value by specifying the `-replica-delay-threshold` flag. You should do this if network delays prevent the nodes from catching up within 1 second of their masters.

Note

If you do not want the switchover to wait for the nodes to catch up, you can use the `-no-replica-delay` threshold flag. In that case, nodes will be converted to primary nodes even if they are behind. You should evaluate whether this risk is worth taking.

6. Perform the switchover to convert the previously failed zone back to a primary zone.

```

kv-> topology clone -current -name newTopo
kv-> topology change-zone-type -name newTopo \
    -znname Manhattan -type primary

```

```
Changed zone type of zn1 to PRIMARY in newTopo
kv-> plan deploy-topology -name newTopo -wait
Executed plan 11, waiting for completion...
Plan 11 ended successfully
```

Confirm the zone type change of the Manhattan zone to PRIMARY by running the ping command.

```
kv-> ping
Pinging components of store mystore based upon topology sequence #208
200 partitions and 2 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
Shard Status: healthy:1 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline:0 maxDelayMillis:120000
                                         maxCatchupTimeSecs:1800
Zone [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
RN Status: online:1 offline:0
Storage Node [sn1] on nyc1:5000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 508d38507fff
    Admin [admin1]           Status: RUNNING,REPLICA
    Rep Node [rg1-rn1]       Status: RUNNING,REPLICA
    sequenceNumber:434 haPort:5011 delayMillis:0 catchupTimeSecs:0
Storage Node [sn2] on jersey1:6000
Zone: [name=JerseyCity id=zn2 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12.1.4.3.5 2016-11-13:40:37 UTC Build id: 508d38507fff
    Admin [admin2]           Status: RUNNING,MASTER
    Rep Node [rg1-rn2]       Status: RUNNING,MASTER
    sequenceNumber:434 haPort:6011
```

Chapter 8. Standardized Monitoring Interfaces

Oracle NoSQL Database allows Java Management Extensions (JMX) agents to be optionally available for monitoring, in addition to the native monitoring provided by the Admin CLI. These agents provide interfaces on each storage node that allow management clients to poll them for information about the status, performance metrics, and operational parameters of the storage node and its managed services, including replication nodes, and admin instances. Also, JMX can be used to monitor Arbiter Nodes.

Both these management agents can also be configured to push notifications about changes in the status of any of the services, and for violations of preset performance limits.

The JMX interface can be enabled in either the Community Edition or the Enterprise Edition.

The JMX service exposes MBeans for the three types of components. These MBeans are the java interfaces `StorageNodeMBean`, `RepNodeMBean`, and `AdminMBean` in the package `oracle.kv.impl.mgmt.jmx`. For more information about the status reported for each component, see the [javadoc](#) for these interfaces.

In this case, the information reported by JMX, is organized according to the Management Information Base (MIB) named `OracleNosqlMIB`, which is included with the Enterprise Edition, in the file `lib/nosql.mib`.

Note

For information on using JMX securely, see *Guidelines for using JMX securely* section in the *Oracle NoSQL Database Security Guide*.

Java Management Extensions (JMX)

JMX agents in NoSQL Database are read-only interfaces and allow you to poll the storage nodes for information about the storage node and about any replication nodes or admins that are hosted on the storage node. The available information includes service status (such as, `RUNNING`, `STOPPED` etc.), operational parameters, and performance metrics.

JMX traps/notifications are also delivered for particular events. Notifications are sent for every service status state change; and for violations of performance limits.

Enabling Monitoring

Monitoring can be enabled on a per-storage node basis in two different ways:

In the Bootfile

You can specify that you want to enable JMX in the storage node's boot configuration file.

Note

When you specify `-mgmt jmx`, a storage node's JMX agent uses the RMI registry at the same port number as is used for all other RMI services managed by the storage node.

By Changing Storage Node Parameters

You can still enable JMX after a store is deployed, by changing the storage node parameter "mgmtClass".

The value of the "mgmtClass" parameter may be one of the following class names:

- To enable JMX:

```
oracle.kv.impl.mgmt.jmx.JmxAgent
```

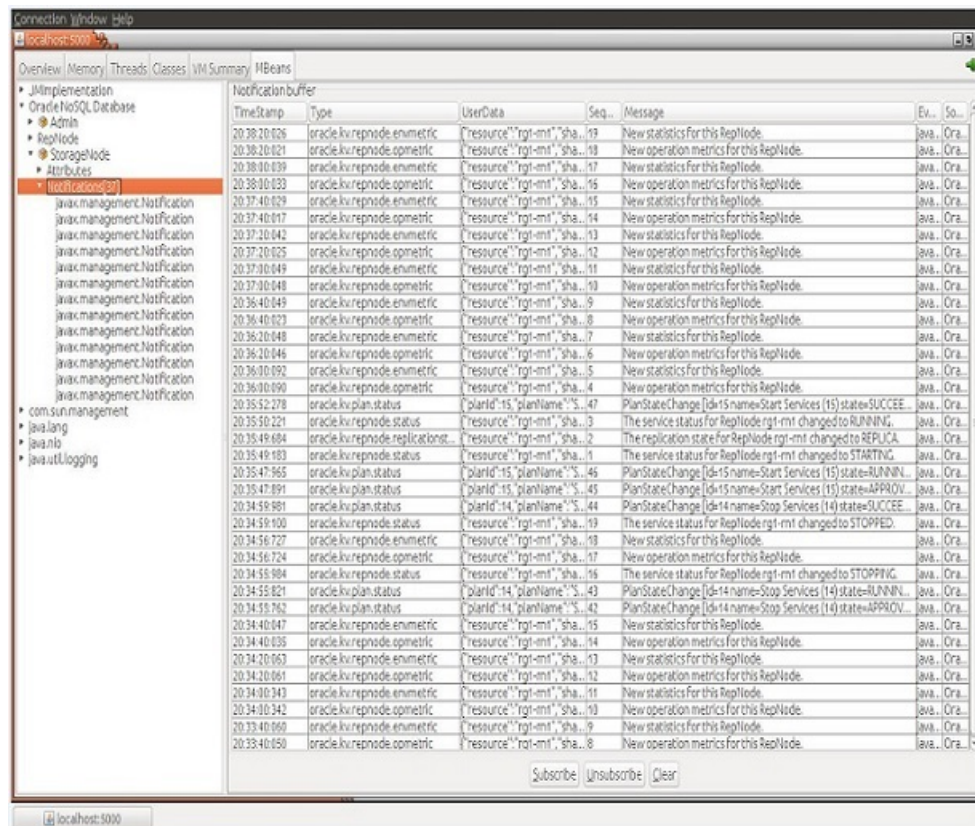
- To disable JMX:

```
oracle.kv.impl.mgmt.NoOpAgent
```

Displaying the NoSQL DB MBeans

To view the NoSQL Database JMX Mbeans in a monitoring tool such as JConsole, connect using the hostname and registry port for each Storage Node that you would like to view.

For example, in this case you would specify localhost:5000 to the JConsole Remote Process connection box in the New Connection tab.



Chapter 9. Integrating Oracle Enterprise Manager (OEM) with Oracle NoSQL Database

The monitoring of a store in Oracle NoSQL Database can be done through its native command-line interface (CLI). The monitoring data is available through Java Management Extensions (JMX) interfaces allowing customers to build their own monitoring solutions. For more information on monitoring data, see [Standardized Monitoring Interfaces \(page 112\)](#).

In this current release, the integration of Oracle's Enterprise Manager (OEM) with Oracle NoSQL Database (Oracle NoSQL Database) provides a graphical management interface tool to discover and monitor a deployed store.

The integration of Oracle NoSQL Database with OEM primarily takes the form of an EM plug-in. The plug-in allows monitoring through Enterprise Manager of NoSQL Database store components, their availability, performance metrics, and operational parameters. The current 12.1.0.9.0 version of the plug-in is compatible with *Oracle Enterprise Manager Cloud Control 12c Release 3 (Version 12.1.0.3.0)*.

Note

For a Storage Node Agent (SNA) to be discovered and monitored, it must be configured for JMX. JMX is not enabled by default. You can tell whether JMX is enabled on a deployed SNA issuing the `show parameters` command and checking the reported value of the `mgmtClass` parameter. If the value is not `oracle.kv.impl.mgmt.jmx.JmxAgent`, then you need to issue the `change-parameters plan` command to enable JMX.

For example:

```
plan change-parameters -service sn1 -wait \  
-params mgmtClass=oracle.kv.impl.mgmt.jmx.JmxAgent
```

For more information, see [Standardized Monitoring Interfaces \(page 112\)](#).

Also, the EM agent process must have read permission on the contents of \$KVROOT.

Importing and Deploying the EM Plug-in

Follow the steps below to import and deploy the EM plug-in:

1. Import the file (.opar) into the Enterprise Manager before deploying it. The plug-in is delivered to the user as a file inside the release package: `lib/12.1.0.9.0_oracle.nosql.snab_2000_0.opar`

For more information, see *Importing Plug-In Archives* section (15.4.4.4) of the *Oracle Enterprise Manager Cloud Control Administrator's Guide*, which you can find here: http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#autold27

2. Copy the .opar file to the host where Oracle Management Service (OMS) is running, and run the command:

Example:

```
$emcli import_update  
-file=/home/guy/12.1.0.9.0_oracle.nosql.snab_2000_0.opar -omslocal
```

3. Deploy the plug-in to the Oracle Management Service (OMS). You can deploy multiple plug-ins to an OMS instance in graphical interface or command line interface. For more information, see *Deploying Plug-Ins to Oracle Management Service* section (15.4.5) of the *Oracle Enterprise Manager Cloud Control Administrator's Guide*, which you can find here: http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#autold28

CLI Example:

```
$emcli deploy_plugin_on_server -plugin  
=oracle.nosql.snab:12.1.0.9.0 -sys_password=sysmanpass
```

4. Deploy the plug-in to the EM Agents where NoSQL Database components are running. For more information, see step 4, *Deploying Plug-Ins on Oracle Management Agent* section (15.4.7) of the *Oracle Enterprise Manager Cloud Control Administrator's Guide*, which you can find here: http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#autold33

CLI Example:

```
$emcli deploy_plugin_on_agent -agent_names=agent1.somewhere.com:3872;  
agent2.somewhere.com:3872 -plugin=oracle.nosql.snab:12.1.0.9.0
```

Note

The plugin components are now installed and can be configured.

Adding NoSQL Database Targets

Run the plug-in's discovery program on each host where a Storage Node Agent (SNA) is running, to add the components of a store as monitoring targets.

Follow the steps below to add NoSQL Database targets:

1. Select "Add Targets" from the "Setup" menu, then choose "Add Targets Manually".
2. Select "Add Targets Using Guided Process" on the "Add Targets Manually" page.
3. Select "Discover NoSQL SNA System Targets" in the "Target Types" drop-down list.



4. Click "Add Using Guided Process". This brings up the NoSQL Database Discovery program.
5. Select an agent on which you can run the discovery program. "Choose Agent" (Select Agent to Run Discovery On) in the first page of the program displays a list of all available EM agents.



6. Click "Next". This takes you to the "Components" (Manage NoSQL Database Targets: Select Store Components) page. This shows all the NoSQL Database components that were found on the agent's host. To be found, an SNA must be running when the discovery program runs. The SNA's configuration reports the SNA's managed components, such as Replication Nodes and Admins. For each component, two attributes are listed:

- Discovered
- Currently Managed

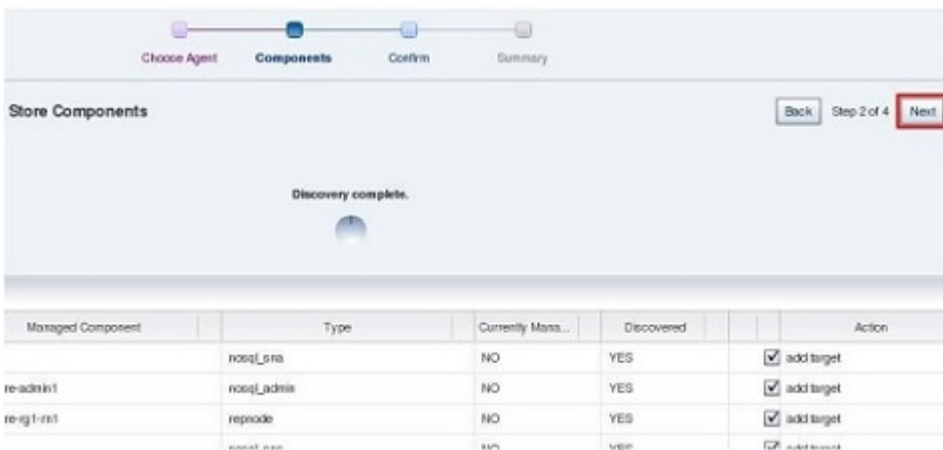
Each attribute can have a value of "Yes" or "No". For each component found, one of two actions is available:

- add target
- remove target

The action is enabled by means of a check box. The recommended action for a component is shown by the state of its check box.

- If the box is checked, then the action is recommended. The user can override the recommended action by checking or un-checking the box.

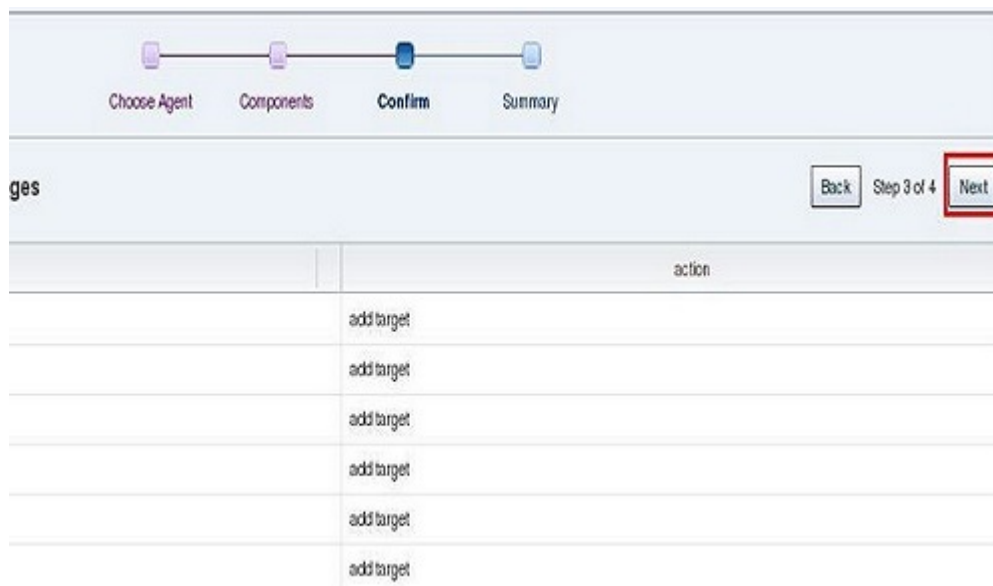
- If a component has Discovered = YES, it means that an instance of that component was found on the host.
- If a component has Currently Managed = YES, it means that the component is already configured for monitoring by EM.
- If a component is Discovered and not Currently Managed, then it is a candidate for being added as a target. For such components, the available action is "add target", which is the recommended action.
- If a component is Discovered and Currently Managed, it means that the component has already been discovered and added as a monitoring target. For such components, the available action is "remove target", but the recommended action is to do nothing, because the discovery report is in sync with EM's configuration.
- If a component is Currently Managed and not Discovered, it means that EM is configured to monitor a component that was unexpectedly not found on the agent's host. This could be so because the component no longer resides on the host; or it could reflect a temporary unavailability of the Storage Node Agent. For such components, the recommended action is "remove target".



Note

In most cases, the default recommended action is the correct action, and no checkboxes need to be altered.

7. Click "Next" once the desired configuration is set up on the "Components" page. This takes you to the "Confirm" (Manage NoSQL Database Targets: Confirm Changes) page, which shows a list of all the chosen actions.



8. Click "Next" to go to the "Summary" (Add SNA Targets: Apply Changes) page. This shows a report of success or failure of each action.
9. At this point, you may exit Discovery, or you may click on "Choose Agent", near the top of the page, to return to the first page of the program, to re-start and run discovery on a new agent.



Once all of the components of a store have been discovered and added, EM's model of the store's topology is complete.

Components of a NoSQL Store

Components of a NoSQL Database Store include the Store itself, Storage Node Agents, Replication Nodes, Admins, and Shards. Of these, Stores and Shards are abstract components that do not correspond to a particular service running on a host. Shards are implied by the existence of Replication Nodes that implement them, and a Store is implied by the existence

of the components that belong to it. These components are discovered when components that imply their existence are discovered.

For example, the first time discovery is run on an agent where components belonging to a Store are running, the Store itself will appear as a Discovered and not Managed component to be added. After the Store is added, subsequent runs of discovery on other agents where the existence of the Store is implied will show that the Store is Discovered and Managed, with a recommended action to do nothing. Newly discovered components belonging to the Store will be added as Members of the Store.

Likewise, Shards may appear to be discovered on multiple hosts, but a single Shard need be added only once.

Store Targets

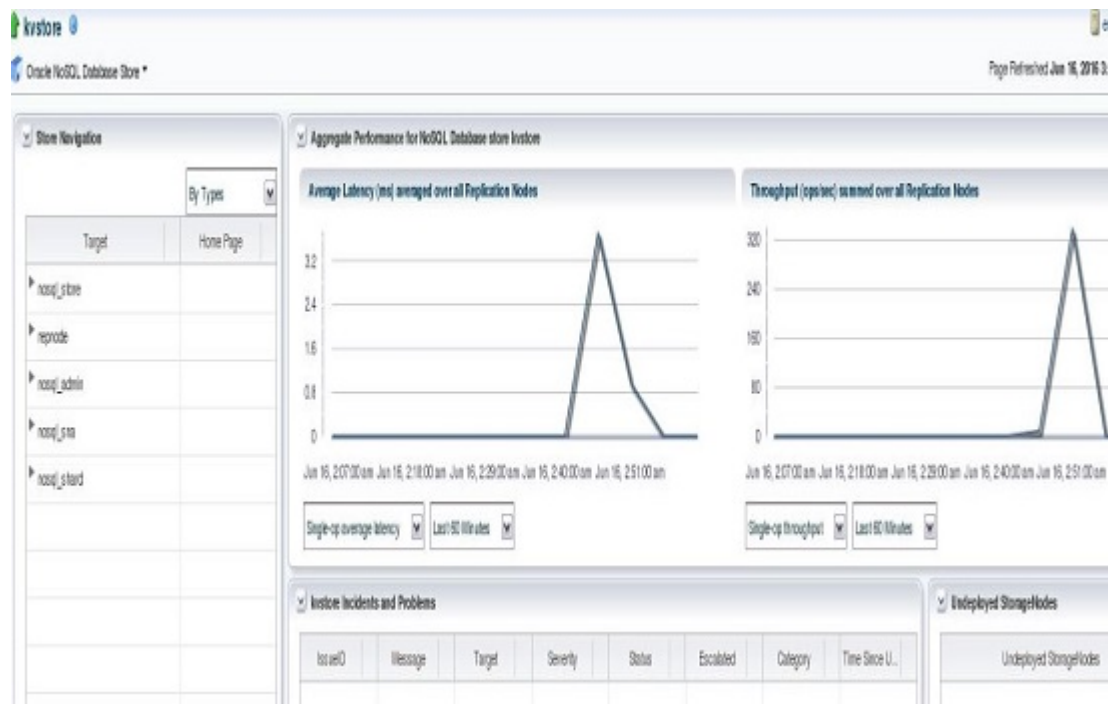
The name of the Store target will be the name of the Store as configured in the NoSQL Database CLI's "configure" command. For more information, see [configure \(page 136\)](#). This name must be unique across all instances of NoSQL Database that will be monitored by a given instance of EM.

Member components of the store have target names made up of their component IDs appended to the store name. For example, in a store named myStore, a Storage Node Agent with an id of "sn1" will have the target name "myStore-sn1", a Replication Node with an id of "rg1-rn1" will have the target name "myStore-rg1-rn1", and so forth. The undeployed StorageNodes will be "UNREGISTERED-hostname-port", for example, "UNREGISTERED-example1.oracle.com-5050". Once the components of a store have been added, you can find the page representing the store by searching for the store name in the "Search Target Name" box in the upper right part of EM's home page. You can also find it via Targets->All Targets or Targets->Systems.

Store Page

Clicking on the Store's name in any of the lists will take you to the Store's target page.

- The page has two large graphs showing the:
 - Average Latency Averaged over all Replication Nodes in the Store
 - Total Throughput for all Replication Nodes



- In the lower right is a list of "Undeployed Storage Node" agents.
- In the lower middle is a list of "Incidents and Problems" related to the store.
- On the left side of the page is the "Store Navigation" panel. This panel presents the topology of the store in three different ways:

- Types

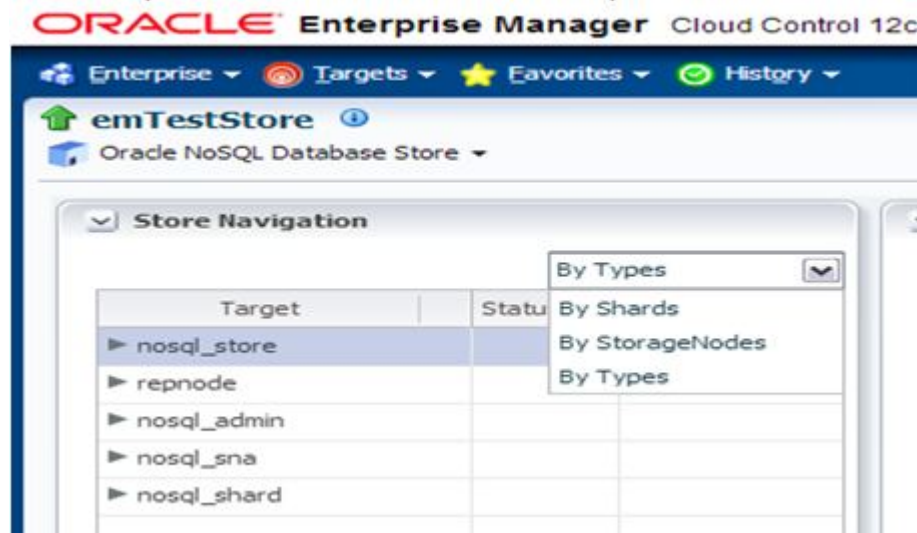
"By Types" groups targets by their target types; so all Replication Nodes are listed together, all Storage nodes are together, and so forth.

- StorageNodes

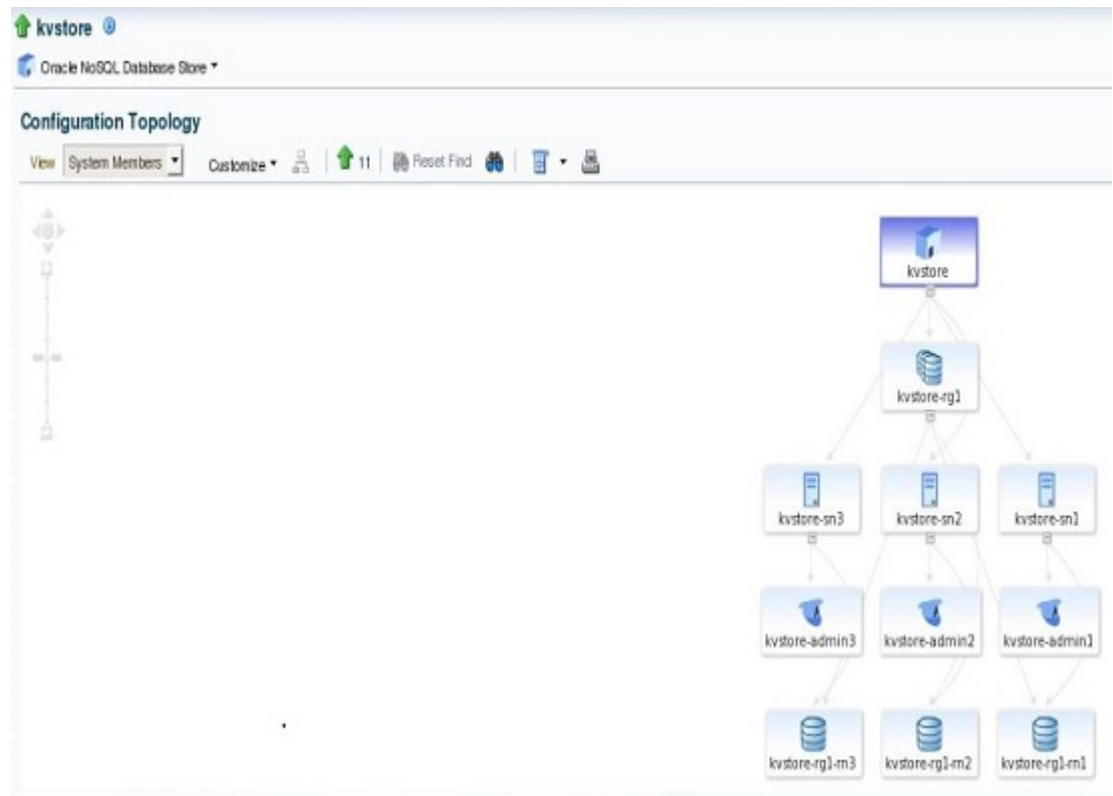
"By StorageNodes" shows the hierarchy of Store->Storage Node->Replication Node. Each Replication Node is managed by a Storage Node Agent, and always resides on the same host. A Storage Node Agent may manage more than one Replication Node, and this is reflected in the tree layout of the navigation panel.

- Shard

"By Shards" shows the hierarchy of Store->Shard->Replication Node.



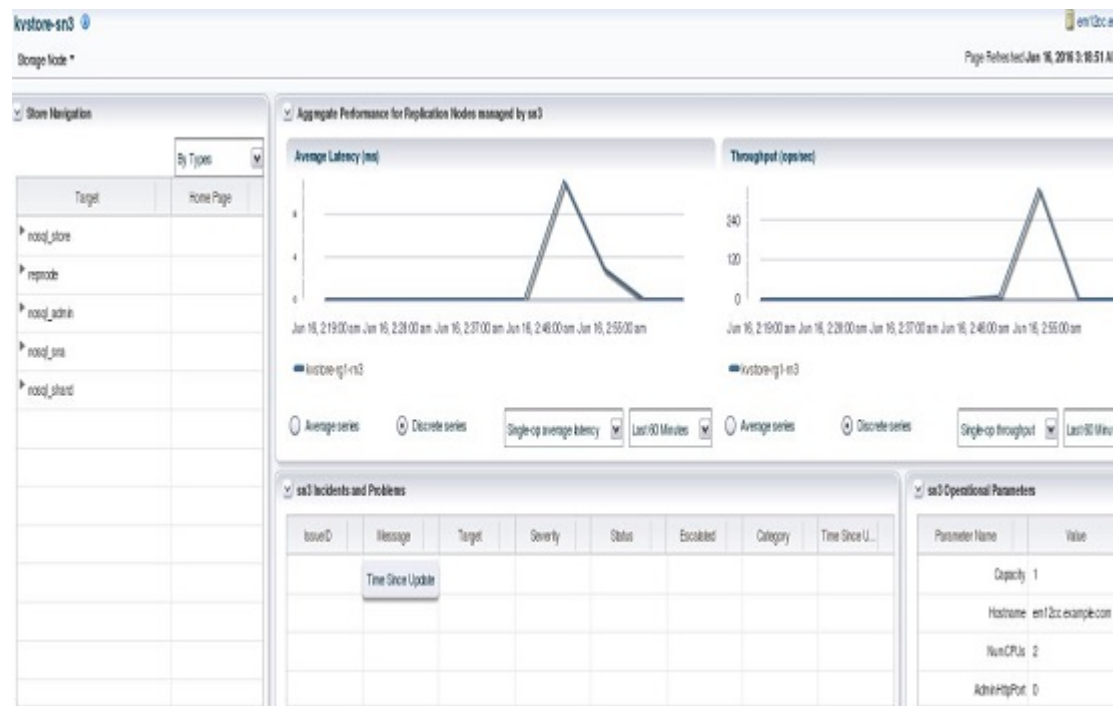
- Each component in the navigation panel has a status "up" or "down", or "unknown" and a link to the target page (labeled "Home Page") for that component. The status can be "unknown" if the targets have yet to be reported for the first time, or if OMS cannot contact the EM Agent.
- The "Store" page, (under menu item Members->Topology) shows the layout of the store as a graph, which is an overview of the "Configuration Topology".



Storage Node Page

On the "Storage Node" page, you see the same graphs of "Average Latency" and "Throughput". Here, the graphs show aggregate information for the Replication Nodes that are managed by the Storage Node. The graphs display either discrete series, with one line per Replication Node; or it can combine the series into a single line. The choice is made using the radio buttons at the bottom of the graph.

This page also shows the operational parameters for the Storage Node Agent.

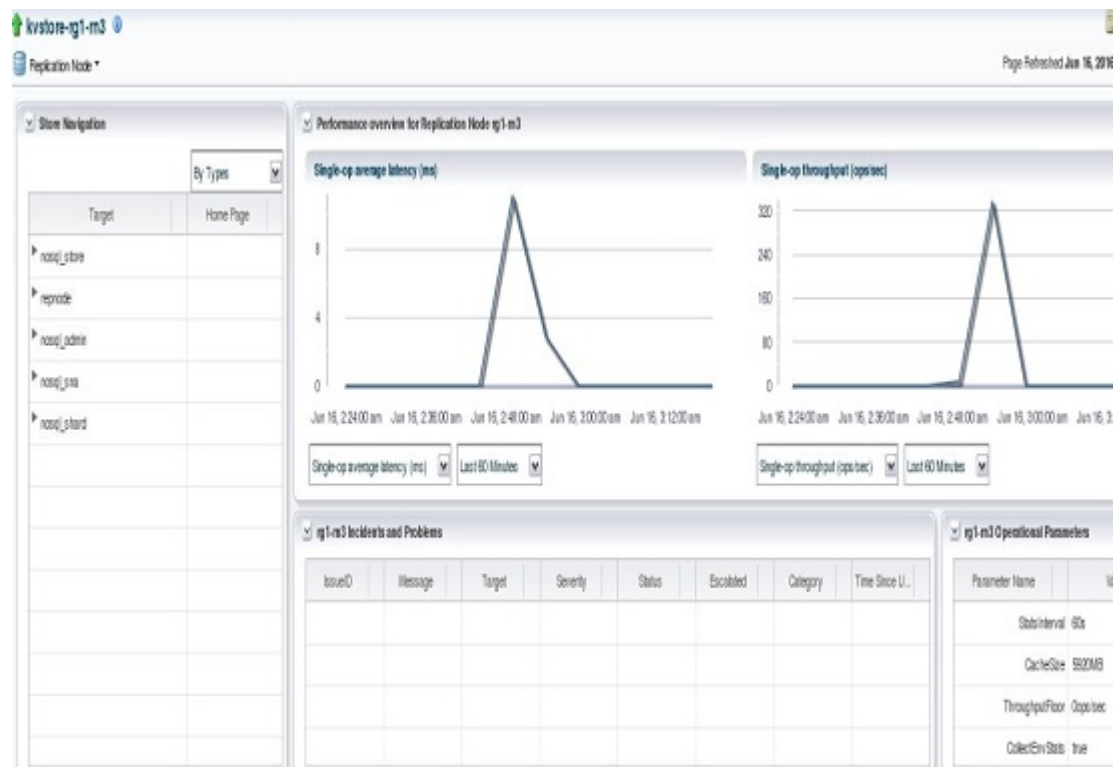


Shard Page

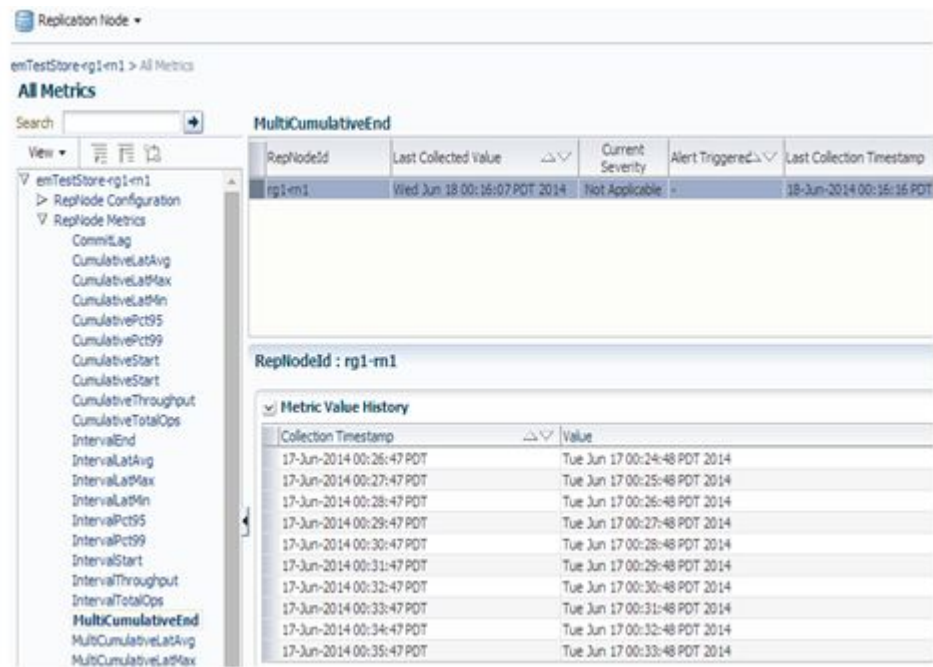
The “Shard” page is similar to the “Storage Node” page. It shows metrics collected from multiple Replication Nodes. These Replication Nodes are the ones that serve as the replication group for the Shard.



Page 124



On this page you can view a variety of metrics by choosing Replication Node->Monitoring->All Metrics. It also shows different time ranges.



From here you can examine and graph any of the numerous metric values that are collected from the Replication Node.

Appendix A. Installing and Configuring a Non-secure Store

This appendix provides a brief information on installing and configuring a non-secure store. For detailed information on installation and configuration, see:

- [Installing Oracle NoSQL Database \(page 1\)](#)
- [Configuring the KVStore \(page 12\)](#)

Installation Configuration

To install Oracle NoSQL Database, see the steps mentioned in chapter [Installing Oracle NoSQL Database \(page 1\)](#). Before you configure Oracle NoSQL Database, you should determine the parameters for each Storage Node in the store (see [Installation Configuration \(page 3\)](#) section for more information on the parameters). Follow the steps below:

Make the following changes in the commands while configuring a non-secure store:

1. Create the initial boot config configuration file using the makebootconfig command. To create the boot config file, issue the following commands:

```
> mkdir -p KVR00T (if it does not already exist)
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar makebootconfig -root KVR00T \
-port 5000 \
-host <hostname> \
-harange 5010,5020 \
-store-security none \
-capacity 1 \
-num_cpus 0 \
-memory_mb 0
```

2. Start the Oracle NoSQL Database Storage Node Agent (SNA) on each of the Oracle NoSQL Database nodes. You can use the start command as follows:

```
nohup java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar start -root KVR00T &
```

3. Ensure that the Oracle NoSQL Database Database client library can contact the Oracle NoSQL Database Storage Node Agent (SNA) by using the ping command:

```
java -jar kvstore.tmp/kvstore.jar ping
-host node01 -port 5000
SNA at hostname: node01, registry port: 5000 is not registered.

No further information is available
```

```
Can't find store topology:
Could not contact any RepNode at: [node01:5000]
```

4. If the Storage Nodes do not start up, you can look through the adminboot and snaboot logs in the KVR00T directory to identify the problem. You can also use the -host option to check an SNA on a remote host:

```
> java -Xmx256m -Xms256m
-jar KVHOME/lib/kvstore.jar ping -port 5000 -host node02
SNA at hostname: node02, registry port: 5000 is not registered. No
further information is available
Can't find store topology:
Could not contact any RepNode at: [node02:5000]
```

Assuming the Storage Nodes have all started successfully, you can configure the KVStore. To do this, you use the CLI command. Start runadmin:

```
> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar runadmin \
-port 5000 -host node01
```

Follow the steps below:

- Name your KVStore

The name of your store is essentially used to form a path to records kept in the store. For example:

```
kv-> configure -name mystore
Store configured: mystore
```

- Create a Zone

Once you have started the command line interface and configured a store name, you can create at least one zone. The usage is:

```
plan deploy-zone -name <zone name>
-rf <replication factor>
[-type [primary | secondary]]
[-arbiters | -no-arbiters ]
[-json ]
[-plan-name <name>] [-wait] [-noexecute] [-force]
```

- Create an Administration Process on a Specific Host

Every KVStore has an administration database. You must deploy the Storage Node to which the command line interface is currently connecting to, and then deploy an Administration process on that same node, to proceed to configure this database. Use the deploy-sn and deploy-admin commands to complete this step. For more information, see [Create an Administration Process on a Specific Host \(page 16\)](#).

- Create a Storage Node Pool

Once you have created your Administration process, you can create a Storage Node Pool. This pool is used to contain all the Storage Nodes in your store. You use the `pool create` command to create this pool. Then you join Storage Nodes to the pool using the `pool join` command. For more information, see [Create a Storage Node Pool \(page 17\)](#).

- Create the Remainder of your Storage Node

After creating storage node pool, you can create the remainder of your Storage Nodes. Storage Nodes host the various & processes for each of the nodes in the store. You must use `deploy-sn` command in the same way as you did in [Create an Administration Process on a Specific Host \(page 16\)](#) for each node that you use in your store. For more information, see [Create the Remainder of your Storage Nodes \(page 18\)](#).

- Create and Deploy Replication Nodes

This final step of the configuration process creates Replication Nodes on every node in your store. You use the `the topology create` and `plan deploy-topology` commands in its place. For more information, see [Create and Deploy Replication Nodes \(page 18\)](#).

Appendix B. CLI Command Reference

This appendix describes the following commands:

- [aggregate](#) (page 132)
- [await-consistent](#) (page 135)
- [change-policy](#) (page 136)
- [configure](#) (page 136)
- [connect](#) (page 137)
- [delete](#) (page 138)
- [ddl](#) (page 139)
- [execute](#) (page 140)
- [exit](#) (page 141)
- [get](#) (page 141)
- [help](#) (page 144)
- [hidden](#) (page 145)
- [history](#) (page 145)
- [load](#) (page 145)
- [logtail](#) (page 146)
- [page](#) (page 147)
- [ping](#) (page 147)
- [plan](#) (page 148)
- [pool](#) (page 163)
- [put](#) (page 164)
- [repair-admin-quorum](#) (page 167)
- [show](#) (page 167)

- [snapshot \(page 172\)](#)
- [table \(page 173\)](#)
- [table-size \(page 173\)](#)
- [timer \(page 176\)](#)
- [topology \(page 176\)](#)
- [verbose \(page 180\)](#)
- [verify \(page 180\)](#)

The Command Line Interface (CLI) is run interactively or used to run single commands. The general usage to start the CLI is:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar runadmin \  
-host <hostname> -port <port> [single command and arguments] \  
-security KVR00T/security/client.security
```

If you want to run a script file, you can use the "load" command on the command line:

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar runadmin -host <hostname> -port <port> \  
-security \  
KVR00T/securtiy/client.security \  
load -file <path-to-script>
```

If none of the optional arguments are passed, it starts interactively. If additional arguments are passed they are interpreted as a single command to run, then return. The interactive prompt for the CLI is:

```
"kv-> "
```

Upon successful completion of the command, the CLI's process exit code is zero. If there is an error, the exit code will be non-zero.

The CLI comprises a number of commands, some of which have subcommands. Complex commands are grouped by general function, such as "show" for displaying information or "ddl" for manipulating schema. All commands accept the following flags:

- -help
Displays online help for the command or subcommand.
- ?
Synonymous with -help. Displays online help for the command or subcommand.
- -verbose
Enables verbose output for the command.

CLI commands have the following general format:

1. All commands are structured like this:

```
"kv-> command [sub-command] [arguments]
```

2. All arguments are specified using flags which start with "-"
3. Commands and subcommands are case-insensitive and match on partial strings(prefixes) if possible. The arguments, however, are case-sensitive.

Inside a CLI script file, you can use # to designate a comment. Also, you can terminate a line with a backslash \ to continue a command onto the next line.

aggregate

Performs simple data aggregation operations on numeric fields like count, sum, average, keys, start and end. The aggregate command iterates matching keys or rows in the store so, depending on the size of the specified key or row, it may take a very long time to complete.

The aggregate subcommands are:

- [aggregate kv \(page 132\)](#)
- [aggregate table \(page 134\)](#)

aggregate kv

```
aggregate kv [-count] [-sum <field[,field,..]>] [-avg <field[,field,..]>]  
             [-key <key>] [-schema <name>]  
             [-start <prefixString>] [-end <prefixString>]
```

Performs simple data aggregation operations using the specified key.

where:

- -count

Returns the count of matching records.

- -sum

Returns the sum of the values of matching fields. All records with a specified schema with the named field are matched. Unmatched records are ignored.

- -avg

Returns the average of the values of matching fields. All records with a specified schema with the named field are matched. Unmatched records are ignored.

- -key

Specifies the key (prefix) to use.

- -schema

Specifies the Avro schema to use.

- -start and -end flags

Restricts the range used for iteration. This is particularly helpful when getting a range of records based on a key component, such as a well-formatted string. -start and -end arguments are inclusive.

For example, a simple count of all records in the store:

```
kv-> aggregate kv -count
count: 33508
```

Sum and average operate on specific field names in matching records which means that only Avro records containing the named fields are used. Sum and average only operate on numeric fields of Avro types INT, LONG, FLOAT, and DOUBLE.

For example, with the following schema:

```
{
  "type" : "record",
  "name" : "Cookie",
  "fields" : [ {
    "name" : "id",
    "type" : "string",
    "default" : ""
  }, {
    "name" : "frequency",
    "type" : "int",
    "default" : 0
  }, {
    "name" : "lastVisit",
    "type" : "string",
    "default" : ""
  }, {
    "name" : "segments",
    "type" : {
      "type" : "array",
      "items" : "string"
    },
    "default" : [ ]
  } ]
}
```

An example of sum on a field named frequency:

```
kv-> aggregate kv -sum frequency -key /visits/charitable_donors/date
```



```
sum(frequency): 2068
```

An example of average on a field named frequency:

```
kv -> aggregate kv -avg frequency -key /visits/charitable_donors/date  
avg(frequency): 2.494571773220748
```

aggregate table

```
aggregate table -name <name>  
  [-count] [-sum <field[,field,..]>]  
  [-avg <field[,field,..]>]  
  [-index <name>]  
  [-field <name> -value <value>]*  
  [-field <name> [-start <value>] [-end <value>]]  
  [-json <string>]
```

Performs simple data aggregation operations on numeric fields of the table.

where:

- -name
Specifies the table for the operation.
- -count
Returns the count of matching records.
- -sum
Returns the sum of the values of matching fields.
- -avg
Returns the average of the values of matching fields.
- -index
Specifies the name of the index to use. When an index is used, the fields named must belong to the specified index and the aggregation is performed over rows with matching index entries.
- -field and -value pairs are used to specify the field values of the primary key to use to match for the aggregation, or you can use an empty key to match the entire table.
- The -field flag, along with its -start and -end flags, can be used for restricting the range used to match rows.
- -json
Specifies the fields and values to use for the aggregation as a JSON input string.

See the example below:

```
# Create a table 'user_test' with an index on user_test(age):
kv-> execute 'CREATE TABLE user_test (id INTEGER,
firstName STRING, lastName STRING, age INTEGER, PRIMARY KEY (id))'
Statement completed successfully

kv-> execute 'CREATE INDEX idx1 on user_test (age)'
Statement completed successfully

# Insert 3 rows:
kv-> put table -name user_test -json
'{"id":1,"firstName":"joe","lastName":"wang","age":21}'
Operation successful, row inserted.
kv-> put table -name user_test -json
'{"id":2,"firstName":"jack","lastName":"zhao","age":32}'
Operation successful, row inserted.
kv-> put table -name user_test -json
'{"id":3,"firstName":"john","lastName":"gu","age":43}'
Operation successful, row inserted.

# Get count(*), sum(age) and avg(age) of rows in table:
kv-> aggregate table -name user_test -count -sum age -avg age
Row count: 3
Sum:
    age(3 values): 96
Average:
    age(3 values): 32.00

# Get count(*), sum(age) and avg(age) of rows where
age >= 30, idx1 is utilized to filter the rows:
kv-> aggregate table -name user_test -count -sum age
-avg age -index idx1 -field age -start 30
Row count: 2
Sum:
    age(2 values): 75
Average:
    age(2 values): 37.50
```

await-consistent

```
await-consistent -timeout <timeout-secs> [-zn <id> | -znname <name> ]...
[-replica-delay-threshold <time-millis>]
```

Waits for up to the specified number of seconds for the replicas in one or more zones, or in the entire store, to catch up with the masters in their associated shards. Prints information about whether consistency was achieved or, if not, details about which nodes failed to become consistent.

where:

- `-timeout`

Specifies the number of seconds for the replicas to catch up with the masters in their associated shards.

- `-zn <id>`

Specifies the zone name to restrict the zones whose replicas need to satisfy the requested consistency requirements. If this option is not specified, all replicas must meet the consistency requirements.

- `-znname <name>`

Specifies the zone name to restrict the zones whose replicas need to satisfy the requested consistency requirements. If this option is not specified, all replicas must meet the consistency requirements.

- `-replica-delay-threshold <time-millis>`

Specifies the maximum number of milliseconds that a replica may be behind the master and be considered caught up. The default is 1000 milliseconds (1 second).

When performing a switchover, you can use this command to wait for secondary nodes to catch up with their masters, and to obtain information about progress towards reaching consistency.

change-policy

```
change-policy [-dry-run] -params [name=value]*
```

Modifies store-wide policy parameters that apply to not yet deployed services. The parameters to change follow the `-params` flag and are separated by spaces.

Parameter values with embedded spaces must be quoted, for example, `name="value with spaces"`. If `-dry-run` is specified, the new parameters are returned without changing them.

For more information on setting policy parameters, see [Setting Store Wide Policy Parameters \(page 92\)](#).

configure

```
configure -name <storename>
```

Configures a new store. This call must be made before any other administration can be performed.

Use the `-name` option to specify the name of the KVStore that you want to configure. The name is used to form a path to records kept in the store. For this reason, you should avoid using characters in the store name that might interfere with its use within a file path. The command line interface does not allow an invalid store name. Valid characters are alphanumeric, `'-'`, `'_'`, and `'.'`.

connect

Encapsulates commands that connect to the specified host and registry port to perform administrative functions or connect to the specified store to perform data access functions.

The current store, if any, will be closed before connecting to another store. If there is a failure opening the specified KVStore, the following warning is displayed: "Warning: You are no longer connected to KVStore".

The subcommands are as follows:

- [connect admin \(page 137\)](#)
- [connect store \(page 137\)](#)

connect admin

```
connect admin -host <hostname> -port <registry port>
[-username <user>] [-security <security-file-path>]
```

Connects to the specified host and registry port to perform administrative functions. An Admin service must be active on the target host. If the instance is secured, you may need to provide login credentials.

where:

- -host <hostname>

Identifies the host name of a node in your store.

- -port <registry port>

The TCP/IP port on which Oracle NoSQL Database should be contacted. This port should be free (unused) on each node. It is sometimes referred to as the registry port.

- -username <user>

Specifies a username to log on as in a secure deployment.

- -security <security-file-path>

In a secured deployment, specifies a path to the security file. If not specified in a secure store, updating the sn-target-list will fail.

connect store

```
connect store [-host <hostname>] [-port <port>]
-name <storename> [-timeout <timeout ms>]
[-consistency <NONE_REQUIRED(default)
| ABSOLUTE| NONE_REQUIRED_NO_MASTER>]
[-durability <COMMIT_SYNC(default)>]
```

```
| COMMIT_NO_SYNC | COMMIT_WRITE_NO_SYNC>]  
[-username <user>] [-security <security-file-path>]
```

Connects to a KVStore to perform data access functions. If the instance is secured, you may need to provide login credentials.

Use the timeout, consistency and durability flags to override the default connect configuration.

where:

- -host <hostname>

Identifies the host name of a node in your store.

- -port <port>

The TCP/IP port on which Oracle NoSQL Database should be contacted. This port should be free (unused) on each node.

- -name <storename>

Identifies the name of the store.

- -timeout <timeout ms>

Specifies the store request timeout in milliseconds.

- -consistency

Specifies the store request consistency. The default value is NONE_REQUIRED.

- -durability

Specifies the store request durability. The default value is COMMIT_SYNC.

- -username <user>

Specifies a username to log on as in a secure deployment.

- -security <security-file-path>

In a secured deployment, specifies a path to the security file.

delete

Encapsulates commands that delete key/value pairs from store or rows from table. The subcommands are as follows:

- [delete kv \(page 139\)](#)
- [delete table \(page 139\)](#)

delete kv

```
delete kv [-key <key>] [-start prefixString] [-end prefixString] [-all]
```

Deletes one or more keys. If `-all` is specified, delete all keys starting at the specified key. If no key is specified, delete all keys in the store. The `-start` and `-end` flags can be used for restricting the range used for deleting.

For example, to delete all keys in the store starting at root:

```
kv -> delete kv -all
301 Keys deleted starting at root
```

delete table

```
delete table -name <name>
[-field <name> -value <value>]*
[-field <name> [-start <value>] [-end <value>]]
[-ancestor <name>]* [-child <name>]*
[-json <string>] [-delete-all]
```

Deletes one or multiple rows from the named table. The table name is a dot-separated name with the format `tableName[.childTableName]*`.

- The `-name` specifies the table name.
- `-field` and `-value` pairs are used to specify the field values of the primary key, or you can use an empty key to delete all rows from the table.
- The `-field` flag, along with its `-start` and `-end` flags, can be used for restricting the sub range for deletion associated with the parent key.
- `-ancestor` and `-child` flags are used to delete rows from specific ancestor and/or descendant tables as well as the target table.
- `-json` indicates that the key field values are in JSON format.
- `-delete-all` is used to delete all rows in a table.

ddl

Encapsulates operations that manipulate schemas in the store. The subcommands are as follows:

- [ddl add-schema \(page 140\)](#)
- [ddl enable-schema \(page 140\)](#)
- [ddl disable-schema \(page 140\)](#)

For details on managing schema in the store, see [Managing Avro Schema \(page 73\)](#).

ddl add-schema

```
ddl add-schema [-file <file> | -string <schema string>]
               [-evolve] [-force]
```

Adds a new schema or changes (evolves) an existing schema with the same name. Use the -evolve flag to indicate that the schema is changing. Use the -force flag to add the schema in spite of evolution warnings.

ddl enable-schema

```
ddl enable-schema -name <name>.<ID>
```

Enables an existing, previously disabled schema.

ddl disable-schema

```
ddl disable-schema -name <name>.<ID>
```

Disables an existing schema.

execute

```
execute <statement>
```

Oracle NoSQL Database provides a Data Definition Language (DDL) that you use to form table and index statements. Use the execute command to run the specified statement synchronously. The statement must be enclosed in single or double quotes. Before using this command, you need to connect to a store first.

For example:

```
kv-> execute 'CREATE TABLE users (id INTEGER, name STRING,
pets ARRAY(String), primary key (id))'
Statement completed successfully
kv-> execute 'DESCRIBE AS JSON TABLE users'
{
  "type" : "table",
  "name" : "users",
  "comment" : null,
  "shardKey" : [ "id" ],
  "primaryKey" : [ "id" ],
  "fields" : [ {
    "name" : "id",
    "type" : "INTEGER",
    "nullable" : true,
    "default" : null
  }, {
    "name" : "name",
    "type" : "STRING",
    "nullable" : true,
    "default" : null
  } ]
}
```

```

    }, {
      "name" : "pets",
      "type" : "ARRAY",
      "collection" : {
        "type" : "STRING"
      },
      "nullable" : true,
      "default" : null
    } ]
  }
}

```

For more information on using Data Definition Language (DDL) to perform table operations see [Getting Started with NoSQL Database Table API](#).

exit

```
exit | quit
```

Exits the interactive command shell.

get

Encapsulates commands that get key/value pairs from store or get rows from table. The subcommands are as follows:

- [get kv \(page 141\)](#)
- [get table \(page 144\)](#)

get kv

```
get kv [-key <keyString>] [-json] [-file <output>] [-all] [-keyonly]
[-valueonly] [-start <prefixString>] [-end <prefixString>]
```

Perform a simple get operation using the specified key. The obtained value is printed out if it contains displayable characters, otherwise the bytes array is encoded using Base64 for display purposes. "[Base64]" is appended to indicate this transformation. The arguments for the get command are:

- `-key <keyString>`

Indicates the full or the prefix key path to use. If `<keyString>` is a full key path, it returns a single value information. The format of this get command is: `get -key <keyString>`. If `<keyString>` is a prefix key path, it returns multiple key/value pairs. The format of this get command is: `get -key <keyString> -all`. Key can be composed of both major and minor key paths, or a major key path only. The `<keyString>` format is: "major-key-path/-/minor-key-path". Additionally, in the case of the prefix key path, a key can be composed of the prefix part of a major key path.

For example, with some sample keys in the KVStore:

```
/group/TC/-/user/bob
```



```
/group/TC/-/user/john
/group/TC/-/dep/IT
/group/SZ/-/user/steve
/group/SZ/-/user/diana
```

A get command with a key containing only the prefix part of the major key path results in:

```
kv -> get kv -key /group -all -keyonly
/group/TC/-/user/bob
/group/TC/-/user/john
/group/TC/-/dep/IT
/group/SZ/-/user/steve
/group/SZ/-/user/diana
```

A get command with a key containing a major key path results in:

```
kv -> get kv -key /group/TC -all -keyonly
/group/TC/-/user/bob
/group/TC/-/user/john
/group/TC/-/dep/IT
```

Get commands with a key containing major and minor key paths results in:

```
kv -> get kv -key /group/TC/-/user -all -keyonly
/group/TC/-/user/bob
/group/TC/-/user/john
kv -> get kv -key /group/TC/-/user/bob
{
  "name"   : "bob.smith",
  "age"    : 20,
  "email"  : "bob.smith@gmail.com",
  "phone"  : "408 555 5555"
}
```

- -json

Should be specified if the record is JSON.

- -file <output>

Specifies an output file, which is truncated, replacing all existing content with new content.

In the following example, records from the key /Smith/Bob are written to the file "data.out".

```
kv -> get kv -key /Smith/Bob -all -file ./data.out
```

In the following example, contents of the file "data.out" are replaced with records from the key /Wong/Bill.

```
kv -> get kv -key /Wong/Bill -all -file ./data.out
```

- -all

Specified for iteration starting at the specified key. If the key argument is not specified, the entire store will be iterated.

- -keyonly

Specified with -all to return only keys.

- -valueonly

Specified with -all to return only values.

- -start <prefixString> and -end <prefixString>

Restricts the range used for iteration. This is particularly helpful when getting a range of records based on a key component, such as a well-formatted string. Both the -start and -end arguments are inclusive.

Note

-start and -end only work on the key component specified by -key <keyString>. The value of <keyString> should be composed of simple strings and cannot have multiple key components specified.

For example, a log where its key structure is:

```
/log/<year>/<month>/-/<day>/<time>
```

puts all log entries for the same day in the same partition, but splits the days across shards. The time format is: "hour.minute".

In this way, you can do a get of all log entries in February and March, 2013 by specifying:

```
kv-> get kv -all -keyonly -key /log/2013 -start 02 -end 03
/log/2013/02/-/01/1.45
/log/2013/02/-/05/3.15
/log/2013/02/-/15/10.15
/log/2013/02/-/20/6.30
/log/2013/02/-/28/8.10
/log/2013/03/-/01/11.13
/log/2013/03/-/15/2.28
/log/2013/03/-/22/4.52
/log/2013/03/-/31/11.55
```

You can be more specific to the get command by specifying a more complete key path. For example, to display all log entries from April 1st to April 4th:

```
kv-> get kv -all -keyonly -key /log/2013/04 -start 01 -end 04
/log/2013/04/-/01/1.03
/log/2013/04/-/01/4.05
/log/2013/04/-/02/7.22
/log/2013/04/-/02/9.40
```

```
/log/2013/04/-/03/4.15
/log/2013/04/-/03/6.30
/log/2013/04/-/03/10.25
/log/2013/04/-/04/4.10
/log/2013/04/-/04/8.35
```

See the subcommand [get table \(page 144\)](#)

get table

```
get table -name <name> [-index <name>]
    [-field <name> -value <value>]+
    [-field <name> [-start <value>] [-end <value>]]
    [-ancestor <name>]+ [-child <name>]+
    [-json <string>] [-file <output>] [-keyonly]
    [-pretty] [-report-size]
```

Performs a get operation to retrieve row(s) from a named table. The table name is a dot-separated name with the format `tableName[.childTableName]*`.

- `-field` and `-value` pairs are used to specify the field values of the primary key or index key if using index specified by `-index`, or with an empty key to iterate the entire table.
- `-field` flag, along with its `-start` and `-end` flags, can be used to define a value range for the last field specified.
- `-ancestor` and `-child` flags are used to return results from specific ancestor and/or descendant tables as well as the target table.
- `-json` indicates that the key field values are in JSON format.
- `-file` is used to specify an output file, which is truncated.
- `-keyonly` is used to restrict information to keys only.
- `-pretty` is used for a nicely formatted JSON string with indentation and carriage returns.
- `-report-size` is used to show key and data size information for primary keys, data values, and index keys for matching records. When `-report-size` is specified no data is displayed.

help

```
help [command [sub-command]] [-include-deprecated]
```

Prints help messages. With no arguments the top-level shell commands are listed. With additional commands and sub-commands, additional detail is provided.

```
kv-> help load load -file <path to file>
Loads the named file and interpret its contents as a script of
commands to be executed. If any of the commands in the script
fail, execution will stop at that point.
```

Use `-include-deprecated` to show deprecated commands.

For example:

```
kv-> help show -include-deprecated
Usage: show admins
       datacenters
       events
       faults
       indexes
       parameters
       perf
       plans
       pools
       schemas
       snapshots
       tables
       topology
       upgrade-order
       users
       versions
       zones
```

hidden

```
hidden [on|off]
```

Toggles visibility and setting of parameters that are normally hidden. Use these parameters only if advised to do so by Oracle Support.

history

```
history [-last <n>] [-from <n>] [-to <n>]
```

Displays command history. By default all history is displayed. Optional flags are used to choose ranges for display.

load

```
load -file <path to file>
```

Loads the named file and interpret its contents as a script of commands to be executed. If any of the commands in the script fail, execution will stop at that point.

For example, suppose the following commands are collected in the script file load-contacts-5.txt:

```
### Begin Script ###
put -key /contact/Bob/Walker -value "{\"phone\":\"857-431-9361\", \"
  \"email\":\"Nunc@Quisque.com\", \"city\":\"Turriff\"}" \
  -json example.ContactInfo
put -key /contact/Craig/Cohen -value "{\"phone\":\"657-486-0535\", \"
  \"email\":\"sagittis@metalcop.net\", \"city\":\"Hamoir\"}" \
  -json example.ContactInfo
```

```

put -key /contact/Lacey/Benjamin -value "{\"phone\":\"556-975-3364\", \
\"email\":\"Duis@laceyassociates.ca\", \"city\":\"Wasseiges\"}" \
-json example.ContactInfo
put -key /contact/Preston/Church -value "{\"phone\":\"436-396-9213\", \
\"email\":\"preston@mauris.ca\", \"city\":\"Helmsdale\"}" \
-json example.ContactInfo
put -key /contact/Evan/Houston -value "{\"phone\":\"028-781-1457\", \
\"email\":\"evan@texfoundation.org\", \"city\":\"Geest-G\"}" \
-json example.ContactInfo
exit
### End Script ###

```

Then, the script can be run by using the load command in the data command line interface:

Note

A schema must be loaded to the store before this script can successfully run. For more information on adding schema, see "Adding Schema" section in Oracle NoSQL Database Getting Started.

```

> java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar runadmin -host node01 -port 5000 \
-security \
KVR00T/securtiy/client.security \
-store mystore
kv-> load -file ./load-contacts-5.txt
Operation successful, record inserted.
Operation successful, record inserted.
Operation successful, record inserted.
Operation successful, record inserted.
Operation successful, record inserted.

```

The following schema was previously added to the store:

```

{
  "type": "record",
  "name": "ContactInfo",
  "namespace": "example",
  "fields": [
    {"name": "phone", "type": "string", "default": ""},
    {"name": "email", "type": "string", "default": ""},
    {"name": "city", "type": "string", "default": ""}
  ]
}

```

For more information on using the load command, see [Using a Script to Configure the Store \(page 28\)](#).

logtail

Monitors the store-wide log file until interrupted by an "enter" key press.

page

```
page [on|<n>|off]
```

Turns query output paging on or off. If specified, *n* is used as the page height.

If *n* is 0, or "on" is specified, the default page height is used. Setting *n* to "off" turns paging off.

ping

```
ping [-json]
```

Pings the runtime components of a store. Components available from the Topology are contacted, as well as Admin services.

where:

- -json

Displays output in JSON format.

For example:

```
kv-> ping
Pinging components of store mystore based upon
topology sequence #308 300 partitions and 3 storage nodes
Time: 2016-11-21 13:40:37 UTC Version: 12.1.4.3.5
Shard Status: healthy:1 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:3 offline:0 maxDelayMillis:0 maxCatchupTimeSecs:0
Storage Node [sn1] on node01:8000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12cR1.4.0.2 2016-03-14 08:41:46 UTC Build id: 62e8510d6c5b+
  Admin [admin1]          Status: RUNNING,MASTER
  Rep Node [rg1-rn1]      Status: RUNNING,MASTER
                           sequenceNumber:6,087 haPort:8011
Storage Node [sn2] on node02:9000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12cR1.4.0.2 2016-03-14 08:41:46 UTC Build id: 62e8510d6c5b+
  Admin [admin2]          Status: RUNNING,REPLICA
  Rep Node [rg1-rn2]      Status: RUNNING,REPLICA
                           sequenceNumber:6,087 haPort:9011 delayMillis:0
                           catchupTimeSecs:0
Storage Node [sn3] on node03:10000
Zone: [name=Manhattan id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING
Ver: 12cR1.4.0.2 2016-03-14 08:41:46 UTC Build id: 62e8510d6c5b+
  Admin [admin3]          Status: RUNNING,REPLICA
```

```
Rep Node [rg1-rn3]      Status: RUNNING,REPLICA
sequenceNumber:6,087 haPort:10011 delayMillis:0
catchupTimeSecs:0
```

You can also access the ping utility through kvstore.jar. For more information see [ping \(page 198\)](#).

plan

Encapsulates operations, or jobs that modify store state. All subcommands with the exception of interrupt and wait change persistent state. Plans are asynchronous jobs so they return immediately unless -wait is used. Plan status can be checked using show plans. The optional arguments for all plans include:

- -wait

Wait for the plan to complete before returning.

- -plan-name

The name for a plan. These are not unique.

- -noexecute

Do not execute the plan. If specified, the plan can be run later using plan execute.

- -force

Used to force plan execution and plan retry.

The subcommands are as follows:

- [plan add-index \(page 149\)](#)
- [plan add-table \(page 150\)](#)
- [plan register-es \(page 152\)](#)
- [plan deregister-es \(page 152\)](#)
- [plan cancel \(page 153\)](#)
- [plan change-parameters \(page 153\)](#)
- [plan change-storagedir \(page 154\)](#)
- [plan change-user \(page 154\)](#)
- [plan create-user \(page 155\)](#)
- [plan deploy-admin \(page 155\)](#)
- [plan deploy-datacenter \(page 155\)](#)

- [plan deploy-sn \(page 155\)](#)
- [plan deploy-topology \(page 156\)](#)
- [plan deploy-zone \(page 156\)](#)
- [plan drop-user \(page 157\)](#)
- [plan evolve-table \(page 157\)](#)
- [plan grant \(page 159\)](#)
- [plan execute \(page 158\)](#)
- [plan failover \(page 158\)](#)
- [plan interrupt \(page 159\)](#)
- [plan migrate-sn \(page 160\)](#)
- [plan remove-admin \(page 160\)](#)
- [plan remove-datacenter \(page 161\)](#)
- [plan remove-index \(page 160\)](#)
- [plan remove-sn \(page 161\)](#)
- [plan remove-table \(page 161\)](#)
- [plan remove-zone \(page 161\)](#)
- [plan repair-topology \(page 162\)](#)
- [plan revoke \(page 162\)](#)
- [plan start-service \(page 162\)](#)
- [plan stop-service \(page 163\)](#)
- [plan wait \(page 163\)](#)

plan add-index

```
plan add-index -name <name> -table <name> [-field <name>]*  
    [-desc <description>]  
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Adds an index to a table in the store.

where:

- -name

Specifies the name of the index to add to a table.

- -table

Specifies the table name where the index will be added. The table name is a dot-separated name with the format `tableName[childTableName]*`.

- -field

Specifies the field values of the primary key.

plan add-table

```
plan add-table -name <name>
               [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Adds a new table to the store. The table name is a dot-separated name with the format `tableName[childTableName]*`.

Before adding a table, first use the `table create` command to create the named table. The following example defines a table (creates a table by name, adds fields and other table metadata).

```
## Enter into table creation mode
table create -name user -desc "A sample user table"
user->
user-> help
Usage: add-array-field |
add-field |
add-map-field |
add-record-field |
add-schema |
cancel |
exit |
primary-key |
remove-field |
set-description |
shard-key |
show
## Now add the fields
user-> help add-field
Usage: add-field -type <type> [-name <field-name> ] [-not-required]
[-nullable] [-default <value>] [-max <value>] [-min <value>]
[-max-exclusive] [-min-exclusive] [-desc <description>]
[-size <size>] [-enum-values <value[,value[,...]]]
<type>: INTEGER, LONG, DOUBLE, FLOAT, STRING, BOOLEAN, DATE, BINARY, FIXED_BINARY, ENUM
## Adds a field. Ranges are inclusive with the exception of String,
## which will be set to exclusive.
user-> add-field -type Integer -name id
user-> add-field -type String -name firstName
user-> add-field -type String -name lastName
user-> help primary-key
```

```
Usage: primary-key -field <field-name> [-field <field-name>]*
## Sets primary key.
user-> primary-key -field id
## Exit table creation mode
user-> exit
## Table User built.
```

Use `table list -create` to see the list of tables that can be added. The following example lists and displays tables that are ready for deployment.

```
kv-> table list
## Tables to be added:
## User -- A sample user table
kv-> table list -name user
## Add table User:
{
  "type" : "table",
  "name" : "User",
  "id" : "User",
  "description" : "A sample user table",
  "shardKey" : [ "id" ],
  "primaryKey" : [ "id" ],
  "fields" : [ {
    "name" : "id",
    "type" : "INTEGER"
  }, {
    "name" : "firstName",
    "type" : "STRING"
  }, {
    "name" : "lastName",
    "type" : "STRING"
  } ]
}
```

The following example adds the table to the store.

```
## Add the table to the store.
kv-> help plan add-table
kv-> plan add-table -name user -wait
Executed plan 5, waiting for completion...
Plan 5 ended successfully
kv-> show tables -name user
{
  "type" : "table",
  "name" : "User",
  "id" : "r",
  "description" : "A sample user table",
  "shardKey" : [ "id" ],
  "primaryKey" : [ "id" ],
  "fields" : [ {
    "name" : "id",
```

```
    "type" : "INTEGER"
  }, {
    "name" : "firstName",
    "type" : "STRING"
  }, {
    "name" : "lastName",
    "type" : "STRING"
  } ]
}
```

For more information and examples on table design, see the *Introducing Oracle NoSQL Database Tables and Indexes* section in the *Oracle NoSQL Database Getting Started with the Table API* guide.

plan register-es

```
plan register-es -clustername <name> -host <host>
                 -port <transport port> [-force]
```

Registers the Elasticsearch cluster with the Oracle NoSQL Database store, using the `register-es` plan command. It is only necessary to register one node of the cluster, as the other nodes in the cluster will be found automatically.

where:

- `-clustername`

Specifies the name of the Elasticsearch cluster.

- `-host`

Specifies the host name of a node in the cluster.

- `-port`

Specifies the transport port of a node in the cluster.

For more information, see *Integrating Elasticsearch with Oracle NoSQL Database* in the *Oracle NoSQL Database Full Text Search* guide.

plan deregister-es

```
plan deregister-es
```

Deregisters the Elasticsearch cluster from the Oracle NoSQL Database store, using the `deregister-es` plan command. This is allowed only if all full text indexes are first removed using the `plan remove-index` command, see [plan remove-index \(page 160\)](#).

For example:

```
kv-> plan deregister-es
Cannot deregister ES because these text indexes exist:
```

```
mytestIndex
JokeIndex
```

For more information, see [Integrating Elasticsearch with Oracle NoSQL Database](#) in the *Oracle NoSQL Database Full Text Search* guide.

plan cancel

```
plan cancel -id <plan id> | -last
```

Cancels a plan that is not running. A running plan must be interrupted before it can be canceled.

Use `show plans` to list all plans that have been created along with their corresponding plan IDs and status.

Use the `-last` option to reference the most recently created plan.

plan change-parameters

```
plan change-parameters -security | -service <id> |
    -all-rns [-zn <id> | -znname <name>] | -all-ans [-zn <id> |
    -znname <name>] | -all-admins [-zn <id> | -znname <name>]
    [-dry-run] [-plan-name <name>]
    [-wait] [-noexecute] [-force] -params [name=value]*
```

Changes parameters for either the specified service, or for all service instances of the same type that are deployed to the specified zone or all zones.

The `-security` flag allows changing store-wide global security parameters, and should never be used with other flags.

The `-service` flag allows a single instance to be affected; and should never be used with either the `-zn` or `-znname` flag.

The `-all-*` flags can be used to change all instances of the service type. The parameters to change follow the `-params` flag and are separated by spaces. The parameter values with embedded spaces must be quoted; for example, `name="value with spaces"`.

One of the `-all-*` flags can be combined with the `-zn` or `-znname` flag to change all instances of the service type deployed to the specified zone; leaving unchanged, any instances of the specified type deployed to other zones. If one of the `-all-*` flags is used without also specifying the zone, then the desired parameter change will be applied to all instances of the specified type within the store, regardless of zone.

If `-dry-run` is specified, the new parameters are returned without changing them. Use the command `show parameters` to see what parameters can be modified. For more information, see [show parameters](#) (page 169).

For more information on changing parameters in the store, see [Setting Store Parameters](#) (page 91).

plan change-storagedir

```
plan change-storagedir -sn <id> -storagedir <path> -add | -remove
    [-storagedirsize <size>] [-plan-name <name>] [-wait] [-noexecute]
    [-force]
```

Adds or removes a storage directory on a Storage Node, for storing a Replication Node.

where:

- -sn

Specifies the Storage Node where the storage directory is added or removed.

- -storagedir

Specifies the path to the storage directory on a Storage Node for storing a Replication Node.

- -add | -remove

If -add is specified, the storage dir is added.

If -remove is specified, the storage dir is removed.

- -storagedirsize

Specifies the size of the directory specified in -storagedir. This parameter is optional; however, it is an error to specify this parameter for some, but not all, storage directories.

Use of this parameter is recommended for heterogeneous installation environments where some hardware has more storage capacity than other hardware. If this parameter is specified for all storage directories, then the store's topology will place more data on the shards that offer more storage space. If this parameter is not used, then data is spread evenly across all shards.

The value specified for this parameter must be a long, followed optionally by a unit string. Accepted unit strings are: KB, MB, GB, and TB, corresponding to 1024 , 1024^2 , 1024^3 , 1024^4 respectively. Acceptable strings are case insensitive. Valid delimiters between the long value and the unit string are " ", "-", or "_".

```
-storagedirsize 200 MB
-storagedirsize 4_tb
-storagedirsize 5000-Mb
```

plan change-user

```
plan change-user -name <user name>
    [-disable | -enable] [-set-password [-password <new password>]
    [-retain-current-password]] [-clear-retained-password]
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Change a user with the specified name in the store. The -retain-current-password argument option causes the current password to be remembered during the -set-password operation as

a valid alternate password for configured retention time or until cleared using `-clear-retained-password`. If a retained password has already been set for the user, setting password again will cause an error to be reported.

This command is deprecated. For more information see User Modification in the *Oracle NoSQL Database Security Guide*.

plan create-user

```
plan create-user -name <user name>
  [-admin] [-disable] [-password <new password>]
  [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Create a user with the specified name in the store. The `-admin` argument indicates that the created user has full administrative privileges.

This command is deprecated. For more information see User Creation in the *Oracle NoSQL Database Security Guide*.

plan deploy-admin

```
plan deploy-admin -sn <id> [-plan-name <name>]
  [-wait] [-noexecute] [-force]
```

Deploys an Admin to the specified Storage Node. The admin type (PRIMARY/SECONDARY) is the same type as the zone the Storage Node is in.

For more information on deploying an admin, see [Create an Administration Process on a Specific Host \(page 16\)](#).

plan deploy-datacenter

Deprecated. See [plan deploy-zone \(page 156\)](#) instead.

plan deploy-sn

```
plan deploy-sn -zn <id> | -znname <name> -host <host> -port <port>
  [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Deploys the Storage Node at the specified host and port into the specified zone.

where:

- `-sn`

Specifies the Storage Node to deploy.

- `-zn <id> | -znname <name>`

Specifies the Zone where the Storage Node is going to be deployed.

- `-host`

Specifies the host name where the Storage Node is going to be deployed.

- -port

Specifies the port number of the host.

For more information on deploying your Storage Nodes, see [Create the Remainder of your Storage Nodes \(page 18\)](#).

plan deploy-topology

```
plan deploy-topology -name <topology name> [-plan-name <name>]
                    [-wait] [-noexecute] [-force]
```

Deploys the specified topology to the store. This operation can take a while, depending on the size and state of the store.

For more information on deploying a satisfactory topology candidate, see [Deploy the Topology Candidate \(page 42\)](#).

plan deploy-zone

```
plan deploy-zone -name <zone name>
                 -rf <replication factor>
                 [-type [primary | secondary]]
                 [-arbiters | -no-arbiters]
                 [-json ]
                 [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Deploys the specified zone to the store and creates a primary zone if -type is not specified.

where:

- -name

Specifies the name of the zone to deploy.

- -rf

Specifies the replication factor of the zone.

- -type

Specifies the type of the zone to deploy. It can be a primary or a secondary zone. If -type is not specified, a primary zone is deployed.

- -arbiters | -no-arbiters

If -arbiters is specified, Arbiter Nodes may be allocated on the Storage Node in the zone. This flag can only be specified on a primary zone.

If -no-arbiters is specified, Arbiter Nodes may not be allocated on the Storage Node in the zone.

The default value is -no-arbiters.

For more information on creating a zone, see [Create a Zone \(page 14\)](#).

plan drop-user

```
plan drop-user -name <user name>
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Drop a user with the specified name in the store. A logged-in user may not drop itself.

This command is deprecated. For more information see User Removal in the *Oracle NoSQL Database Administrator's Guide*.

plan evolve-table

```
plan evolve-table -name <name>
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Evolves a table in the store. The table name is a dot-separate with the format `tableName[.childTableName]*`.

Use the `table evolve` command to evolve the named table. The following example evolves a table.

```
## Enter into table evolution mode
kv-> table evolve -name User
kv-> show
{
  "type" : "table",
  "name" : "User",
  "id" : "r",
  "description" : "A sample user table",
  "shardKey" : [ "id" ],
  "primaryKey" : [ "id" ],
  "fields" : [ {
    "name" : "id",
    "type" : "INTEGER"
  }, {
    "name" : "firstName",
    "type" : "STRING"
  }, {
    "name" : "lastName",
    "type" : "STRING"
  } ]
}
## Add a field
kv-> add-field -type String -name address
## Exit table creation mode
kv-> exit
## Table User built.
kv-> plan evolve-table -name User -wait
## Executed plan 6, waiting for completion...
```



```
## Plan 6 ended successfully
kv-> show tables -name User
{
  "type" : "table",
  "name" : "User",
  "id" : "r",
  "description" : "A sample user table",
  "shardKey" : [ "id" ],
  "primaryKey" : [ "id" ],
  "fields" : [ {
    "name" : "id",
    "type" : "INTEGER"
  }, {
    "name" : "firstName",
    "type" : "STRING"
  }, {
    "name" : "lastName",
    "type" : "STRING"
  }, {
    "name" : "address",
    "type" : "STRING"
  } ]
}
```

Use table `list -evolve` to see the list of tables that can be evolved. For more information, see [plan add-table \(page 150\)](#) .

plan execute

```
plan execute -id <id> | -last
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Executes a created but not yet executed plan. The plan must have been previously created using the `-noexecute` flag .

Use the `-last` option to reference the most recently created plan.

plan failover

```
plan failover { [-zn <zone-id> | -znname <zone-name>]
    -type [primary | offline-secondary] }...
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Changes zone types to failover to a changed set of primary zones following a failure of primary zones that has resulted in a loss of quorum. The plan failover command changes zone types to either Primary or Secondary.

Note

Arbiters are not currently supported during failover and switchover operations.

The violations are corrected by executing a rebalance command once the components in the topology are repaired (the Storage Nodes that host components in the topology must be running to successfully deploy the new topology after altering the topology via the topology rebalance command).

where:

- `-zn <zone-id> | -znname <zone-name>`

Specifies a zone either by zone ID or by name.

- `-type [primary | offline-secondary]`

Specifies the new type (primary/offline-secondary) for the associated zone.

Zones whose new type is primary will be zones that are taking over from failed zones as new primary zones in order to reestablish quorum. For these zones, a quorum of the storage nodes in each shard in the zone needs to be available and responding to requests.

Zones whose new type is offline-secondary represent primary zones that are currently offline, resulting in the current loss of quorum. For these zones, all of the storage nodes in the zones must currently be unavailable. None of the command's zone type changes will be performed if these requirements are not met when the command starts.

This command cannot be performed when other plans are in progress for the store. You should cancel or interrupt the plans, before executing this plan.

plan grant

```
plan grant [-role <role name>]* -user <user_name>
```

Allows granting roles to users.

where:

- `-role <role name>`

Specifies the roles that will be granted. The role names should be the system-defined roles (except public) listed in the *Oracle NoSQL Database Security Guide*.

- `-user <user_name>`

Specifies the user who the role will be granted from.

This command is deprecated. For more information see Grant Role or Privilege in the *Oracle NoSQL Database Administrator's Guide*.

plan interrupt

```
plan interrupt -id <plan id> | -last
```

Interrupts a running plan. An interrupted plan can only be re-executed or canceled. Use `-last` to reference the most recently created plan.

plan migrate-sn

```
plan migrate-sn -from <id> -to <id>  
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Migrates the services from one Storage Node to another. The old node must not be running.

where:

- -from

Specifies the Storage Node (old) that you are migrating from.

- -to

Specifies the Storage Node (new) that you are migrating to.

For example, assuming that you are migrating from Storage Node 25 to 26, you would use:

```
kv-> plan migrate-sn -from sn25 -to sn26
```

Before executing the `plan migrate-sn` command, you can stop any running old Storage Node by using `-java -Xmx256m -Xms256m -jar KVHOME/lib/kvstore.jar stop -root KVR00T`.

plan remove-admin

```
plan remove-admin -admin <id> | -zn <id> | -znname <name>  
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Removes the desired Admin instances; either the single specified instance, or all instances deployed to the specified zone.

If you use the `-admin` flag and there are 3 or fewer Admins running in the store, or if you use the `-zn` or `-znname` flag and the removal of all Admins from the specified zone would result in only one or two Admins in the store, then the desired Admins will be removed only if you specify the `-force` flag.

Also, if you use the `-admin` flag and there is only one Admin in the store, or if you use the `-zn` or `-znname` flag and the removal of all Admins from the specified zone would result in the removal of all Admins from the store, then the desired Admins will not be removed.

plan remove-index

```
plan remove-index -name <name> -table <name>  
    [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Removes an index from a table.

where:

- -name

Specifies the name of the index to remove.

- -table

Specifies the table name to remove the index from. The table name is a dot-separated name with the format `tableName[childTableName]*`.

plan remove-datacenter

```
plan remove-datacenter
```

This command is deprecated. See [plan remove-zone \(page 161\)](#) instead.

plan remove-sn

```
plan remove-sn -sn <id>  
[-plan-name <name>] [-wait] [-noexecute] [-force]
```

Removes the specified Storage Node from the topology. The Storage Node is automatically stopped before removal.

This command is useful when removing unused, old Storage Nodes from the store. To do this, see [Replacing a Failed Storage Node \(page 79\)](#).

plan remove-table

```
plan remove-table -name <name> [-keep-data]  
[-plan-name <name>] [-wait] [-noexecute] [-force]
```

Removes a table from the store. The named table must exist and must not have any child tables. Indexes on the table are automatically removed. By default data stored in this table is also removed. Table data may be optionally saved by specifying the `-keep-data` flag. Depending on the indexes and amount of data stored in the table this may be a long-running plan.

The following example removes a table.

```
## Remove a table.  
kv-> plan remove-table -name User  
## Started plan 7. Use show plan -id 7 to check status.  
## To wait for completion, use plan wait -id 7.  
kv-> show tables  
## No table found.
```

For more information, see *Introducing Oracle NoSQL Database Tables and Indexes in the Oracle NoSQL Database Getting Started with the Table API* guide.

plan remove-zone

```
plan remove-zone -zn <id> | -znname <name>  
[-plan-name <name>] [-wait] [-noexecute] [-force]
```

Removes the specified zone from the store.

Before running this command, all Storage Nodes that belong to the specified zone must first be removed using the `plan remove-sn` command.

plan repair-topology

```
plan repair-topology
  [-plan-name <name>] [-wait] [-noexecute] [-force]
```

Inspects the store's deployed, current topology for inconsistencies in location metadata that may have arisen from the interruption or cancellation of previous deploy-topology or migrate-sn plans. Where possible, inconsistencies are repaired. This operation can take a while, depending on the size and state of the store.

plan revoke

```
plan revoke [-role <role name>]* -user <user_name>
```

Allows revoking roles to users.

where:

- -role <role name>

Specifies the roles that will be revoked. The role names should be the system-defined roles (except public) listed in the *Oracle NoSQL Database Security Guide*.

- -user <user_name>

Specifies the user who the role will be revoked from.

This command is deprecated. For more information see Revoke Role or Privilege in the *Oracle NoSQL Database Administrator's Guide*.

plan start-service

```
plan start-service {-service <id> | -all-rns [-zn <id> |
  -znname <name>] | -all-ans [-zn <id> | -znname <name>] |
  -zn <id> | -znname <name> } [-plan-name <name>]
  [-wait] [-noexecute] [-force]
```

Starts the specified service(s). The service may be a Replication Node, a Storage Node, an Arbiter Node, or Admin service, as identified by any valid string.

For example, to identify a Storage Node, use -service storageNodeId, where storageNodeId is a simple integer. To identify a Replication Node, use -service shardId-nodeId, where shardId-nodeId must be given as a single argument with one embedded hyphen and no spaces. The shardId identifier is represented by rgX, where X refers to the shard number.

where:

- -service

Specifies the name of the service to start.

- -all-rns

If specified, starts the services of all Replication Nodes in a store.

- `-all-ans`

If specified, starts all the Arbiter Nodes in the specified zone.

plan stop-service

```
plan stop-service {-service <id> |
  -all-rns [-zn <id> | -znname <name>] | -all-ans [-zn <id> |
  -znname <name>] | -zn <id> | -znname <name> }
  [-plan-name <name>] [-wait] [-noexecute] [-force]}
```

Stops the specified service(s). The service may be a Replication Node, a Storage Node, an Arbiter Node, or Admin service, as identified by any valid string.

For example, to identify a Storage Node, use `-service storageNodeId`, where `storageNodeId` is a simple integer. To identify a Replication Node, use `-service shardId-nodeId`, where `shardId-nodeId` must be given as a single argument with one embedded hyphen and no spaces. The `shardId` identifier is represented by `rgX`, where `X` refers to the shard number.

where:

- `-service`
- `-all-rns`

If specified, stops the services of all Replication Nodes in a store.

- `-all-ans`

If specified, stops all the Arbiter Nodes in the specified zone.

Use this command to stop any affected services so that any attempts by the system to communicate with it are no longer made; resulting in a reduction in the amount of error output related to a failure you are already aware of.

This command is useful during disk replacement process. Use the `plan stop-service` command to stop the affected service prior removing the failed disk. For more information, see [Replacing a Failed Disk \(page 82\)](#).

plan wait

```
plan wait -id <id> | -last [-seconds <timeout in seconds>]
```

Waits indefinitely for the specified plan to complete, unless the optional timeout is specified.

Use the `-seconds` option to specify the time to wait for the plan to complete.

The `-last` option references the most recently created plan.

pool

Encapsulates commands that manipulates Storage Node pools, which are used for resource allocations. The subcommands are as follows:

- [pool clone \(page 164\)](#)
- [pool create \(page 164\)](#)
- [pool join \(page 164\)](#)
- [pool leave \(page 164\)](#)
- [pool remove \(page 164\)](#)

pool clone

```
pool clone -name <name> -from <source pool name> [-json]
```

Clone an existing Storage Node pool to a new Storage Node pool to be used for resource distribution when creating or modifying a store.

For more information on using a cloned Storage Node pool when contracting a topology, see [Contracting a Topology \(page 39\)](#).

pool create

```
pool create -name <name>
```

Creates a new Storage Node pool to be used for resource distribution when creating or modifying a store.

For more information on creating a Storage Node pool, see [Create a Storage Node Pool \(page 17\)](#).

pool join

```
pool join -name <name> [-sn <snX>]* [-json]
```

Adds Storage Nodes to an existing Storage Node pool.

pool leave

```
pool leave -name <name> [-sn <snX>]* [-json]
```

Remove Storage Nodes from an existing Storage Node pool.

pool remove

```
pool remove -name <name>
```

Removes a Storage Node pool.

put

Encapsulates commands that put key/value pairs to the store or put rows to a table. The subcommands are as follows:

- [put kv \(page 165\)](#)
- [put table \(page 166\)](#)

put kv

```
put kv -key <keyString> -value <valueString> [-file]
      [-hex | -json <schemaName>] [-if-absent] [-if-present]
```

Put the specified key/value pair into the store. The following arguments apply to the put command:

- **-key<keyString>**

Specifies the name of the key to be put into the store. Key can be composed of both major and minor key paths, or a major key path only. The <keyString> format is: "major-key-path/-/minor-key-path".

For example, a key containing major and minor key paths:

```
kv-> put -key /Smith/Bob/-/email -value
      "{\"id\": 1, \"email\": \"bob.smith@gmail.com\"}"
      -json schema.EmailInfo
```

For example, a key containing only a major key path:

```
kv-> put -key /Smith/Bob -value "{\"name\":
      \"bob.smith\", \"age\": 20, \"phone\": \"408 555 5555\", \"email\":
      \"bob.smith@gmail.com\"}" -json schema.UserInfo
```

- **-value <valueString>**

If neither -json or -file is specified, the <valueString> is treated as a raw bytes array.

For example:

```
kv-> put -key /Smith/Bob/-/phonenummer -value "408 555 5555"
```

Note

The mapping of the raw arrays to data structures (serialization and deserialization) is left entirely to the application.

If used with -json to specify a Json string, the valueString should be encapsulated in quotation marks, and its internal field name and value with string type should also be encapsulated by string quote characters.

For example:

```
kv-> put -key /Smith/John/-/email -value
      "{\"id\": 1, \"email\": \"john.smith@gmail.com\"}"
      -json schema.EmailInfo
```

- **-file**

Indicates that the value is obtained from a file. The file to use is identified by the value parameter.

For example:

```
kv-> put -key /Smith/Bob -value ./smith-bob-info.txt  
-file -json schema.UserInfo
```

- -hex

Indicates that the value is a BinHex encoded byte value with base64 encoding.

- -json<schemaName>

Indicates that the value is a JSON string. Can be specified along with -file.

- -if-absent

Indicates that a key/value pair is put only if no value for the given key is present.

- -if-present

Indicates that a key/value pair is put only if a value for the given key is present.

put table

```
put table -name <name> [if-absent | -if-present ]  
[-json <string>] [-file <file>] [-exact] [-update]
```

Put a row into the named table. The table name is a dot-separated name with the format table[childTableName]*.

where:

- -if-absent

Indicates to put a row only if the row does not exist.

- -if-present

Indicates to put a row only if the row already exists.

- -json

Indicates that the value is a JSON string.

- -file

Can be used to load JSON strings from a file.

- -exact

Indicates that the input JSON string or file must contain values for all columns in the table and cannot contain extraneous fields.

- -update

Can be used to partially update the existing record.

repair-admin-quorum

```
repair-admin-quorum {-zn <id> | -znname <name> | -admin<id>}...
```

Repairs admin quorum by reducing membership of the admin group to the admins in the specified zones or the specific admins listed. This command should be used when attempting to recover from a failure that has resulted in a loss of admin quorum. This command can result in data loss.

After obtaining a working admin by calling this command, you should use the plan failover command to failover to the zones that remain available after a failure and to update the topology to match the changes made to the admins.

The arguments specify which admins to use as the new set of primary admins, either by specifying all of the admins in one or more zones or by identifying specific admins. The specified set of admins must not be empty, must contain only currently available admins, and must include all currently available primary admins. It may also include secondary admins, if desired, to increase the admin replication factor or because no primary admins are available.

Note

This command can be repeated if a temporary network or component failure causes the command invocation to fail.

show

Encapsulates commands that display the state of the store and its components or schemas. The subcommands are as follows:

- [show admins \(page 168\)](#)
- [show datacenters \(page 168\)](#)
- [show events \(page 168\)](#)
- [show faults \(page 169\)](#)
- [show indexes \(page 169\)](#)
- [show parameters \(page 169\)](#)
- [show perf \(page 169\)](#)
- [show plans \(page 169\)](#)

- [show pools \(page 170\)](#)
- [show schemas \(page 170\)](#)
- [show snapshots \(page 170\)](#)
- [show tables \(page 171\)](#)
- [show topology \(page 171\)](#)
- [show upgrade-order \(page 171\)](#)
- [show users \(page 171\)](#)
- [show versions \(page 171\)](#)
- [show zones \(page 172\)](#)

show admins

```
show admins
```

Displays basic information about Admin services.

show datacenters

```
show datacenters
```

Deprecated. See [show zones \(page 172\)](#) instead.

show events

```
show events [-id <id>] | [-from <date>] [-to <date> ]  
            [-type <stat | log | perf>]
```

Displays event details or list of store events. The status events indicate changes in service status.

Log events are noted if they require attention.

Performance events are not usually critical but may merit investigation. Events marked "SEVERE" should be investigated.

The following date/time formats are accepted. They are interpreted in the local time zone.

MM-dd-yy HH:mm:ss:SS
MM-dd-yy HH:mm:ss
MM-dd-yy HH:mm
MM-dd-yy
HH:mm:ss:SS
HH:mm:ss
HH:mm

For more information on events, see [Events \(page 90\)](#).

show faults

```
show faults [-last] [-command <command index>]
```

Displays faulting commands. By default all available faulting commands are displayed. Individual fault details can be displayed using the -last and -command flags.

show indexes

```
show indexes [-table <name>] [-name <name>]
```

Displays index metadata. By default the indexes metadata of all tables are listed.

If a specific table is named, its indexes metadata are displayed. If a specific index of the table is named, its metadata is displayed. For more information, see [plan add-index \(page 149\)](#).

Use SHOW INDEX statement to indicate the index type (TEXT, SECONDARY) when you enable text-searching capability to Oracle NoSQL Database, in-concert with the tables interface.

For example:

```
kv-> show index
Indexes on table Joke
JokeIndex (category, txt), type: TEXT
```

For more information, see *Creating Full Text Index in the Oracle NoSQL Database Full Text Search* guide.

show parameters

```
show parameters -policy | -service <name>
```

Displays service parameters and state for the specified service. The service may be a Replication Node, Storage Node, or Admin service, as identified by any valid string, for example rg1-rn1, sn1, admin2, etc. Use the -policy flag to show global policy parameters. Use the -security flag to show global security parameters.

```
show parameters -service sn1
```

When you enable text-searching capability to Oracle NoSQL Database, in-concert with the tables interface, the show parameter command also provides information on the Elasticsearch cluster name and transport port as values for the parameters searchClusterMembers and searchClusterName.

For more information, see *Integrating Elasticsearch with Oracle NoSQL Database in the Oracle NoSQL Database Full Text Search* guide.

show perf

```
show perf
```

Displays recent performance information for each Replication Node.

show plans

```
show plans [-last] [-id <id>] [-from <date>] [-to <date>][-num <howMany>]
```

Shows details of the specified plan or list all plans that have been created along with their corresponding plan IDs and status.

- The `-last` option shows details of the most recently created plan.
- The `-id <n>` option details the plan with the given id. If `-num <n>` is also given, list `<n>` plans, starting with plan `#<id>`.
- The `-num <n>` option sets the number of plans to the list. The default is 10.
- The `-from <date>` option lists plans after `<date>`.
- The `-to <date>` option lists plans before `<date>`.

Combining `-from` with `-to` describes the range between the two dates. Otherwise `-num` applies.

The following date formats are accepted. They are interpreted in the UTC time zone.

```
yyyy-MM-dd HH:mm:ss.SSS
yyyy-MM-dd HH:mm:ss
yyyy-MM-dd HH:mm
yyyy-MM-dd
MM-dd-yyyy HH:mm:ss.SSS
MM-dd-yyyy HH:mm:ss
MM-dd-yyyy HH:mm
MM-dd-yyyy
HH:mm:ss.SSS
HH:mm:ss
HH:mm
```

For more information on plan review, see [Reviewing Plans \(page 10\)](#).

show pools

```
show pools
```

Lists the Storage Node pools.

show schemas

```
show schemas [-disabled] | [-name <name>]
```

Displays schema details of the named schema or a list of schemas registered with the store.

Use the `-name` option to specify the name of the schema you want to check if it is currently enabled in the store.

Use the `-disabled` option to see all schemas, including those which are currently disabled.

show snapshots

```
show snapshots [-sn <id>]
```

Lists snapshots on the specified Storage Node. If no Storage Node is specified, one is chosen from the store. You can use this command to view the existing snapshots.

show tables

```
show tables -name <name>
```

Displays the table information. Use `-original` flag to show the original table information if you are building a table for evolution. The flag is ignored for building table for addition. For more information, see [plan add-table \(page 150\)](#) and [plan evolve-table \(page 157\)](#)

Use `show table -name <tableName>` statement to list the full text index. This command provides the table structure including the indexes that have been created for that table. For more information, see Creating Full Text Index in the *Oracle NoSQL Database Full Text Search* guide.

show topology

```
show topology [-zn] [-rn] [-an] [-sn] [-store] [-status] [-perf]
```

Displays the current, deployed topology. By default it shows the entire topology. The optional flags restrict the display to one or more of zones, Replication Nodes, Storage Nodes, Arbiter Nodes and store name, or specify service status or performance.

With this command you can obtain the ID of the zone to which Storage Nodes can be deployed to.

show upgrade-order

```
show upgrade-order
```

Lists the Storage Nodes which need to be upgraded in an order that prevents disruption to the store's operation.

This command displays one or more Storage Nodes on a line. Multiple Storage Nodes on a line are separated by a space. If multiple Storage Nodes appear on a single line, then those nodes can be safely upgraded at the same time. When multiple nodes are upgraded at the same time, the upgrade must be completed on all nodes before the nodes next on the list can be upgraded.

If at some point you lose track of which group of nodes should be upgraded next, you can always run the `show upgrade-order` command again.

show users

```
show users -name <name>
```

Lists the names of all users, or displays information about a specific user. If no user is specified, lists the names of all users. If a user is specified using the `-name` option, then lists detailed information about the user.

show versions

```
show versions
```

Lists the client and server version information.

For example

```
kv-> show versions
Client version: 12.1.3.4.0
Server version: 12.1.3.4.0
```

show zones

```
show zones [-zn <id>] | -znname <name>]
```

Lists the names of all zones, or display information about a specific zone.

Use the `-zn` or the `-znname` flag to specify the zone that you want to show additional information; including the names of all of the Storage Nodes in the specified zone, and whether that zone is a primary or secondary zone.

snapshot

Encapsulates commands that create and delete snapshots, which are used for backup and restore. The subcommands are as follows:

- [snapshot create \(page 172\)](#)
- [snapshot remove \(page 172\)](#)

snapshot create

```
snapshot create -name <name>
```

Creates a new snapshot using the specified name as the prefix.

Use the `-name` option to specify the name of the snapshot that you want to create.

Snapshots should not be taken while any configuration (topological) changes are being made, because the snapshot might be inconsistent and not usable.

snapshot remove

```
snapshot remove -name <name> | -all
```

Removes the named snapshot. If `-all` is specified, remove all snapshots.

Use the `-name` option to specify the name of the snapshot that you want to remove.

If the `-all` option is specified, remove all snapshots.

To create a backup of your store using a snapshot see [Taking a Snapshot \(page 60\)](#).

To recover your store from a previously created snapshot you can use the load utility or restore directly from a snapshot. For more information, see [Using the Load Program \(page 63\)](#) or [Restoring Directly from a Snapshot \(page 67\)](#).

table

Deprecated with exception of table-size. See [execute \(page 140\)](#) instead.

table-size

```
table-size -name <name> -json <string>
          [-rows <num> [[-primarykey | -index <name>] -keyprefix <size>]]
```

Calculates key and data sizes for the specified table using the row input, optionally estimating the NoSQL DB cache size required for a specified number of rows of the same format. Running this command on multiple sample rows can help determine the necessary cache size for desired store performance.

- -json specifies a sample row used for the calculation.
- -rows specifies the number of rows to use for the cache size calculation
- Use the -index or -primarykey and -keyprefix to specify the expected commonality of index keys in terms of number of bytes.

This command mainly does the following:

1. Calculates the key and data size based on the input row in JSON format.
2. Estimates the DB Cache size required for a specified number of rows in the same JSON format.

The output contains both detailed size info for primary key/index and the total size; internally it calls JE's DbCacheSize utility to calculate the cache size required for primary key and indexes with the input parameters:

```
java -jar $KVHOME/dist/lib/je.jar DbCacheSize
      -records <num> -key <size> -data <size> -keyprefix
      <size> -outputproperties -replicated <JE properties...>
      -duplicates]
```

where:

- -records <num>: The number of rows specified by -row <num>.
- -key <size>: The size of key get from step 1.
- -data <size>: The size of data get from step1.
- -keyprefix <size>: The expected commonality of keys, specified using -primarykey | -index <name> -keyprefix <size>
- -duplicates: Used only for table index.
- -<JE properties...>: The JE configuration parameters used in kvstore.

For example:


```
kv-> execute "create table user (id integer, address string,
zip_code string, primary key(id))"
kv-> execute "create index idx1 on user (zip_code)"
```

See the following cases:

1. Calculates the key size and data size based on the input row in JSON.

```
kv-> table-size -name user -json '{"id":1,
"address": "Oracle Building ZPark Beijing China",
"zip_code":"100000"}'
```

=== Key and Data Size ===

Name	Number of Bytes
Primary Key	8
Data	47
Index Key of idx1	7

2. Calculates the key/data size and the cache size of the table with 10000 rows.

```
kv-> table-size -name user -json '{"id":1,
"address": "Oracle Building ZPark Beijing China",
"zip_code":"100000"}'
-rows 10000
```

=== Key and Data Size ===

Name	Number of Bytes
Primary Key	8
Data	47
Index Key of idx1	7

=== Environment Cache Overhead ===

16,798,797 minimum bytes

=== Database Cache Sizes ===

Name	Number of Bytes	Description
Table	1,024,690	Internal nodes only
	1,024,690	Internal nodes and record versions
	1,024,690	Internal nodes and leaf nodes
idx1	413,728	Internal nodes only
	413,728	Internal nodes and record versions
	413,728	Internal nodes and leaf nodes
	1,438,418	Internal nodes only

Total	1,438,418	Internal nodes and record versions
	1,438,418	Internal nodes and leaf nodes

For more information, see the DbCacheSize javadoc: http://docs.oracle.com/cd/E17277_02/html/java/com/sleepycat/je/util/DbCacheSize.html

Note

The cache size is calculated in the following way:

- Cache size of table

```
java -jar KVHOME/lib/je.jar DbCacheSize -records
10000 key 8 -data 47 -outputproperties -replicated
<JE properties...>
```

The parameters are:

- Record number: 10000
- Primary key size: 8
- Data size: 47

- Cache size of table

```
java -jar KVHOME/lib/je.jar DbCacheSize -records
10000 -key 7 -data 8 -outputproperties -replicated
<JE properties...> -duplicates
```

The parameters are:

- Record number: 10000
- Index key size: 7
- Data size: 8. The primary key size is used here, since the data of secondary index is the primary key.
- Use -duplicates for index.
- Total size = cache size of table + cache size of idx1.

3. Calculates the cache size with a key prefix size for idx1

```
kv-> table-size -name user -json
'{"id":1, "address":"Oracle Building ZPark Beijing China",
"zip_code":"100000"}' -rows 10000 -index idx1 -keyprefix 3

=== Key and Data Size ===
```

Name	Number of Bytes
------	-----------------

```

-----
Primary Key          8
Data                47
Index Key of idx1    7

=== Environment Cache Overhead ===

16,798,797 minimum bytes

=== Database Cache Sizes ===

Name      Number of Bytes      Description
-----
Table      1,024,690      Internal nodes only
           1,024,690      Internal nodes and record versions
           1,024,690      Internal nodes and leaf nodes
-----
idx1       413,691      Internal nodes only
           413,691      Internal nodes and record versions
           413,691      Internal nodes and leaf nodes
-----
Total      1,438,381      Internal nodes only
           1,438,381      Internal nodes and record versions
           1,438,381      Internal nodes and leaf nodes

```

For more information, see the DbCacheSize javadoc: http://docs.oracle.com/cd/E17277_02/html/java/com/sleepycat/je/util/DbCacheSize.html

Note

A key prefix size is provided for idx1, the idx1's cache size is calculated like this:

```
java -jar KVHOME/lib/je.jar DbCacheSize -records
10000 -key 7 -data 8 -keyprefix 3 -outputproperties
-replicated <JE properties...> -duplicates
```

The above examples show that the cache size of idx1 is 413,691 and is smaller than 413,728 of case 2. For more information about the usage of keyprefix, see JE DbCacheSize document: http://docs.oracle.com/cd/E17277_02/html/java/com/sleepycat/je/util/DbCacheSize.html

timer

```
timer [on|off]
```

Turns the measurement and display of execution time for commands on or off.

topology

Encapsulates commands that manipulate store topologies. Examples are redistribution/rebalancing of nodes or changing replication factor. Topologies are created and modified using

this command. They are then deployed by using the `plan deploy-topology` command. For more information, see [plan deploy-topology \(page 156\)](#). The subcommands are as follows:

- [topology change-repfactor \(page 177\)](#)
- [topology change-zone-arbiters \(page 177\)](#)
- [topology change-zone-type \(page 178\)](#)
- [topology clone \(page 178\)](#)
- [topology contract \(page 178\)](#)
- [topology create \(page 178\)](#)
- [topology delete \(page 179\)](#)
- [topology list \(page 179\)](#)
- [topology preview \(page 179\)](#)
- [topology rebalance \(page 179\)](#)
- [topology redistribute \(page 179\)](#)
- [topology validate \(page 179\)](#)
- [topology view \(page 180\)](#)

topology change-repfactor

```
topology change-repfactor -name <name> -pool <pool name>  
    -zn <id> | -znname <name> -rf <replication factor>
```

Modifies the topology to change the replication factor of the specified zone to a new value. The replication factor may not be decreased at this time.

The command will create Replication Nodes and Arbiter Nodes and may remove Arbiter Nodes only in the zone specified in the command. If the change in replication factor increases the total primary replication factor equal to two and the zone is configured to allow Arbiters, then Arbiters are created in that zone. If the change in replication factor increases the total primary Replication Factor from two to a number greater than two and if the zone contained Arbiters, then they are removed from the zone. If some other zone contained Arbiters, a topology rebalance must be performed by the user to remove the Arbiters from the topology.

For more information on modifying the replication factor, see [Increase Replication Factor \(page 38\)](#).

topology change-zone-arbiters

```
topology change-zone-arbiters -name <name>  
    {-zn <id> | -znname <name>} {-arbiter | -no-arbiter}
```

Modifies the topology to change the Arbiter Node attribute of the specified zone.

topology change-zone-type

```
topology change-zone-type -name <name>
    {-zn <id> | -znname <name>} -type {primary | secondary}
```

Modifies the topology to change the type of the specified zone to a new type.

If one or more zones have their type changed and the resulting topology is deployed using the plan deploy-topology command, the following rules apply:

- The plan waits for up to five minutes for secondary nodes that are being converted to primary nodes to catch up with their masters.
- The plan will fail, and print details about lagging zones and nodes, if a quorum of secondary nodes in each shard fails to catch up within the required amount of time. This behavior helps to reduce the time that a newly added primary node cannot become a master, and so is not able to contribute to availability.
- Because this command can only be performed successfully if quorum can be maintained, it does not result in data loss.

topology clone

```
topology clone -from <from topology> -name <to topology>
```

or

```
topology clone -current -name <to topology>
```

Clones an existing topology so as to create a new candidate topology to be used for topology change operations.

topology contract

```
topology contract -name <name> -pool <pool name>
```

Modifies the named topology to contract storage nodes. For more information, see [Contracting a Topology \(page 39\)](#).

topology create

```
topology create -name <candidate name> -pool <pool name>
    -partitions <num>
```

Creates a new topology with the specified number of partitions using the specified storage pool.

You should avoid using the dollar sign ('\$') character in topology candidate names. The CLI displays a warning when trying to create or clone topologies whose names contain the reserved character.

If the primary replication factor is equal to two, the topology create command will allocate Arbiter Nodes on the Storage Nodes in a zone that supports hosting Arbiter Nodes. During topology deployment, an error is issued if there are not enough Storage Nodes for Arbiter

Node distribution. A valid Arbiter Node distribution is one in which the Arbiter Node is hosted on a Storage Node that does not contain other members of its Replication Group.

For more information on creating the first topology candidate, see [Make the Topology Candidate \(page 35\)](#).

topology delete

```
topology delete -name <name>
```

Deletes a topology.

topology list

```
topology list
```

Lists existing topologies.

topology preview

```
topology preview -name <name> [-start <from topology>]
```

Describes the actions that would be taken to transition from the starting topology to the named, target topology. If -start is not specified, the current topology is used. This command should be used before deploying a new topology.

topology rebalance

```
topology rebalance -name <name> -pool <pool name>  
[-zn <id> | -znname <name>]
```

Modifies the named topology to create a balanced topology. If the optional -zn flag is used, only Storage Nodes from the specified zone are used for the operation.

This command may also add, move or remove Arbiter Nodes. Arbiter Nodes are added if the new topology supports Arbiter Nodes and the old topology does not. Arbiter Nodes are removed if the old topology supported Arbiter Nodes and the new one does not. Arbiter Nodes may be moved to a zero Replication Factor datacenter if the Arbiter Nodes are hosted in a non zero Replication Factor datacenter.

For more information on balancing a non-compliant topology, see [Balance a Non-Compliant Topology \(page 38\)](#).

topology redistribute

```
topology redistribute -name <name> -pool <pool name>
```

Modifies the named topology to redistribute resources to more efficiently use those available.

For more information on redistributing resources to enhance write throughput, see [Increase Data Distribution \(page 37\)](#).

topology validate

```
topology validate [-name <name>]
```

Validates the specified topology. If no topology is specified, the current topology is validated. Validation generates violations and notes.

Violations are issues that can cause problems and should be investigated.

Notes are informational and highlight configuration oddities that can be potential issues or may be expected.

For more information, see [Validate the Topology Candidate \(page 41\)](#).

topology view

```
topology view -name <name>
```

Displays details of the specified topology. Also displays any available Arbiter Node information.

verbose

```
verbose [on|off]
```

Toggles or sets the global verbosity setting. This property can also be set on a per-command basis using the `-verbose` flag.

verify

Encapsulates commands that check various parameters of the store. The subcommands are as follows:

- [verify configuration \(page 180\)](#)
- [verify prerequisite \(page 180\)](#)
- [verify upgrade \(page 181\)](#)

verify configuration

```
verify configuration [-silent] [-json]
```

Verifies the store configuration by iterating the components and checking their state against that expected in the Admin database. This call may take a while on a large store.

The `-json` option specifies that output should be displayed in JSON format.

The `-silent` option suppresses verbose verification messages that are displayed as the verification is proceeding. Instead, only the initial startup messages and the final verification message is displayed. This option has no effect when the `-json` option is specified.

verify prerequisite

```
verify prerequisite [-silent] [-sn snX]*
```

Verifies that the storage nodes are at or above the prerequisite software version needed to upgrade to the current version. This call may take a while on a large store.

As part of the verification process, this command displays the components which do not meet the prerequisites or cannot be contacted. It also checks for illegal downgrade situations where the installed software is of a newer minor release than the current version.

When using this command, the current version is the version of the software running the command line interface.

Use the `-sn` option to specify those storage nodes that you want to verify. If no storage nodes are specified, all the nodes in the store are checked.

The `-silent` option suppresses verbose verification messages that are displayed as the verification is proceeding. Instead, only the initial startup messages and the final verification message is displayed.

verify upgrade

```
verify upgrade [-silent] [-sn snX]*
```

Verifies the storage nodes (and their managed components) are at or above the current version. This call may take a while on a large store.

As part of the verification process, this command displays the components which have not yet been upgraded or cannot be contacted.

When using this command, the current version is the version of the software running the command line interface.

Use the `-sn` option to specify those storage nodes that you want to verify. If no storage nodes are specified, all the nodes in the store are checked.

The `-silent` option suppresses verbose verification messages that are displayed as the verification is proceeding. Instead, only the initial startup messages and the final verification message is displayed.

Appendix C. Utility Command Reference

This appendix describes the following commands:

- [export](#) (page 182)
- [generateconfig](#) (page 186)
- [help](#) (page 186)
- [import](#) (page 187)
- [load admin metadata](#) (page 191)
- [makebootconfig](#) (page 193)
- [ping](#) (page 198)
- [restart](#) (page 204)
- [runadmin](#) (page 205)
- [start](#) (page 205)
- [status](#) (page 205)
- [stop](#) (page 206)
- [version](#) (page 206)

Oracle NoSQL Database utility commands are stand-alone utilities that do not require the use of the Oracle NoSQL Database Command Line Interface. They are available using one of two jar files. In some cases, kvstore.jar is used. In others, kvtool.jar is required. Both are packaged with the server libraries.

export

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvtool.jar export -export-all | -table <table_names>  
-store <storeName> -helper-hosts <helper_hosts>  
-config <config_file_name> [-username <user>]  
[-security <security-file-path>]
```

This utility creates a package which contains user data, schema and logging information. Use the [import](#) (page 187) utility to consume this data.

All data and metadata can be exported to either the local filesystem or Oracle Storage Cloud Service (for customers of Oracle's Cloud products). You can also optionally use this utility to export individual tables instead of the entire store. This utility will write:

- Application created data (excluding security data).
- Schema definitions. These include table definitions, Avro definitions and the index definitions. Table owner is written, or null if the table has no owner. All of this definition information is exported in JSON format.
- TTL information for every table record.

This utility *does not* export security data (such as user definitions), or store deployment information. Also, incremental export (that is, export from a given moment in time) is not supported. Finally, derived information such as index data and statistics is not exported, but all such derived information can be recreated upon data import.

It is possible that your store's schema will change during the export process. See [Schema Management \(page 185\)](#) for information on how the export utility handles evolving schema.

For best results, this utility should be used on a store which currently has no write activity. However, even if write activity is on-going during the export process, individual records are guaranteed to be correct in that they represent a committed state. However, if write activity is on-going, then this utility makes no guarantees regarding inter-record consistency. That is, this utility does not create any kind of snapshot isolation.

See [Using the Export and Import Utilities \(page 70\)](#) for usage information.

Export Utility Command Line Parameters

The export utility's command line parameters are:

- `-export-all` causes the entire store to be exported. If this option is specified, then `-table` cannot be specified.
- `-table` is the name of the table or tables you want to export. If you want to export multiple tables, then specify a comma-delimited list of table names.

If this parameter is specified, then `-export-all` cannot be specified.

- `-store` is the name of the Oracle NoSQL Database store you want to export data from. This parameter is required.
- `-helper-hosts` is a list of hostname and registry port pairs in `hostname:port` format. Comma-delimit each item in this list. At least one helper host must be specified.
- `-config` is the name of the configuration file to use. This parameter is required. See [Export Utility Configuration File \(page 184\)](#) for information on the configuration file for this utility.
- `-username` is the name of the user you want to export data as. This parameter is required if your store is configured to require authentication.
- `-security` is the client security configuration file. This parameter is required if your store is configured to require authentication. For information on the parameters contained in this

file, see *Configuring SSL in the Oracle NoSQL Database Getting Started with the Table API for Java* guide. For example:

```
oracle.kv.auth.username=clientUID1
oracle.kv.auth.pwdfile.file=/home/nosql/login.pwd
oracle.kv.transport=ssl
oracle.kv.ssl.trustStore=/home/nosql/client.trust
```

If you are using Kerberos, then this file would look something like this:

```
oracle.kv.auth.kerberos.keytab = kerberos/mykeytab
oracle.kv.auth.username = krbuser@EXAMPLE.COM
oracle.kv.auth.external.mechanism=kerberos
oracle.kv.auth.kerberos.services=
node01:oraclenosql/node01.example.com@EXAMPLE.COM
oracle.kv.auth.kerberos.mutualAuth=false
```

Export Utility Configuration File

The export utility uses a plain-text configuration file which describes the export type and the destination of the exported data. It is identified to the utility using the required `-config` command line parameter.

The contents of the configuration file differ depending on the value specified for the utility's `-export-type` parameter.

If `LOCAL` is specified, then the configuration file must contain the following information:

- `export-type = LOCAL`

Indicates that this export is to a local file system.

- `export-package-path = <path_for_export>`

Identifies the path to the directory where the export package is to be written.

For example, a configuration file used when exporting to the local file system might contain:

```
export-type = LOCAL
export-package-path = /mnt/dsk1/nosql_export_dir
```

Use `OBJECT_STORE` if the export utility is being used with Oracle Storage Cloud Services. In this case, the configuration file must contain the following information:

Note

To use the export utility with Oracle Storage Cloud Services, you must download and install Java jar files which provide necessary support. See [Installing the Cloud Storage JARs \(page 73\)](#) for details.

- `export-type = OBJECT_STORE`

Indicates that the export is to Oracle Storage Cloud Services.

- `container-name = <container_name>`

The name of the container in Oracle Storage Cloud Service where the exported data is stored. Upon export, the container must not currently exist. The export utility will automatically create the container for you.

- `service-name = <service_name>`

The service name associated with the Oracle Storage Cloud Service subscription.

- `user-name = <user_name>`

The user name associated with the Oracle Storage Cloud Service subscription.

- `password` is the password you use with the Oracle Storage Cloud Service subscription.

- `service-url = <service_url>`

The service URL associated with the Oracle Storage Cloud Service subscription.

For example, a configuration file used when exporting to Oracle Storage Cloud Service might contain:

```
export-type = OBJECT_STORE
container-name = TestContainer
service-name = Storage-nosqlldb
user-name = nosqlldb.Storageadmin
password = obj54KV!
service-url = https://storage-den2.oraclecorp.com
```

Schema Management

It is possible that your store's schema will change during a long-running export process. The export utility handles schema changes in the following way:

- If the schema evolves during the export process, the process uses the latest version available at the beginning of the process. In the event that this data is later reimported to the store, all the imported data will be compatible with this version of the schema.

In this event, the export utility emits a warning at the end of the export process which indicates that the schema changed during export. A metadata diff is provided to identify how the schema changed.

- If a table is removed during the export process, the process will continue without complaint. In this event, the export utility emits a warning at the end of the export process which indicates that the table, or tables, were deleted during the export.
- If a new table is added to the store during the export process, it is ignored. Only those tables which existed at the start of the export process are exported.

Export Exit Codes

Name	Code	Description
EXIT_OK	0	No errors found.
EXIT_USAGE	100	Illegal export command usage.
EXIT_NOPERM	101	Unauthorized access to the Oracle Cloud Storage Service.
EXIT_EXPSTR_NOCONNECT	102	The source store could not be accessed using the service connection parameters.
EXIT_NOCONNECT	103	The source store could not be connected using the given store name and helper host.
EXIT_UNEXPECTED	104	The utility experienced an unexpected error.
EXIT_NOWRITE	105	The export package has no write permissions.
EXIT_CONTAINER_EXISTS	107	The specified container already exists in the Object Store. Delete the existing container or use another container name.
EXIT_NO_EXPORT_FOLDER	108	Export folder with the given name does not exist.
EXIT_INVALID_EXPORT_STORE	109	Invalid export store type. Valid export types are LOCAL or OBJECT_STORE.
EXIT_SECURITY_ERROR	110	Error loading security file.
EXIT_NOSQL_PERM	111	User has no read permissions on the object.

generateconfig

```
java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar generateconfig [-verbose]
-host <hostname> -port <port> -sn <StorageNodeId> -target <zipfile>
```

Generates configuration files for the specified storage node. The generateconfig command creates the target zipfile which contains the required configuration to re-create the storage node. The top-level directory in the zipfile is the store's root directory.

help

```
java -Xmx256m -Xms256m \
```

```
-jar KVHOME/lib/kvstore.jar help <commandName>
```

Prints usage info. With no arguments the top-level shell commands are listed. With a command name, additional detail is provided.

import

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvtool.jar import -import-all | -table <table_names>  
-store <storeName> -helper-hosts <helper_hosts>  
[-status <status-file-name>] [-username <user>]  
[-security <security-file-path>]
```

This utility imports data to the identified Oracle NoSQL Database store. The data to be imported must have been created by the [export \(page 182\)](#) utility.

This utility runs synchronously. Also, this utility will not create an Oracle NoSQL Database store instance; the store must be installed and configured before this utility is run.

This utility can be used to:

1. Import all schema definitions and user data. Schema definitions include table definitions, avro schemas, and the index definitions. All schema is imported first, and then user data is imported to the store. Because schema is written first, it is possible to use this utility to populate a new, empty store.

Schema is imported only if the table or avro definition does not currently exist in the store. Index definitions are created after tables are created, but only if the tables are created by this utility. If the table is created using some other mechanism (DDL supplied using the Command Line Interface, for example), then the `import` utility will not create the indexes, even if they currently do not exist. Finally, if the targeted table somehow does not contain the field to be indexed, then that index creation is skipped.

After all schema has been imported, user data is imported. If the primary key definition of the data does not match the primary key definition in the table or avro schema definition, the corresponding table data is not imported.

If the non-key fields in the data do not match the non-key definition fields in the schema, then the table is still imported with the following behavior:

- If the schema calls for a non-key field, but the data does not provide this field, then the field's default value is used if one is available. If a default value has not been defined in the schema for that field, then NULL is used.
 - If the data provides a non-key field value that is not known to the table's schema, then that value is ignored.
2. Import a specific table from the exported dataset. In this case, the corresponding table schemas, index definitions, and table data are imported.
 3. The Time-To-Live (TTL) value of the table data is imported. If the TTL has already expired, then the data is not written to the store.

Write activity may be on-going against the store at the time of the import. In this regard, the `import` utility is simply another client writing to the store. In the case of a conflict when writing a table row or record, your store data will be in a state defined by which client last wrote the data.

Because `import` can take a long time, it is possible for you to track the progress of the import process. Use the `Import.log` file for this purpose. It is written to the same directory as is identified by the `export-package-path` configuration file parameter.

See [Using the Export and Import Utilities \(page 70\)](#) for usage information.

Import Utility Command Line Parameters

The `import` utility's command line parameters are:

- `-import-all` causes the entire store to be imported. If this option is specified, then `-table` cannot be specified.
- `-table` is the name of the table or tables you want to import. If you want to import multiple tables, then specify a comma-delimited list of table names.

If this parameter is specified, then `-import-all` cannot be specified.

- `-store` is the name of the Oracle NoSQL Database store you want to import data to. This parameter is required.
 - `-helper-hosts` is a list of hostname and registry port pairs in *hostname:port* format. Comma-delimit each item in this list. At least one helper host must be specified.
 - `-config` is the name of the configuration file to use. This parameter is required. See [Import Utility Configuration File \(page 189\)](#) for information on the configuration file for this utility.
 - `-status` is optional parameter that causes the status of the import operation to be saved in the named file. If the import fails part way, it can start where it left off by using the status file. The granularity of the status file is per file segment stored in the export package.
- If this parameter is not specified and there is a failure, then the import must start over from the beginning. In this case, the target store does not need to be re-created. Upon subsequent imports, existing records are skipped.
- `-username` is the name of the user you want to import data as. This parameter is required if your store is configured to require authentication.
 - `-security` is the client security configuration file. This parameter is required if your store is configured to require authentication. For information on the parameters contained in this file, see *Configuring SSL in the Oracle NoSQL Database Getting Started with the Table API for Java* guide. For example:

```
oracle.kv.auth.username=clientUID1
```

```
oracle.kv.auth.pwdfile.file=/home/nosql/login.pwd
oracle.kv.transport=ssl
oracle.kv.ssl.trustStore=/home/nosql/client.trust
```

If you are using Kerberos, then this file would look something like this:

```
oracle.kv.auth.kerberos.keytab = kerberos/mykeytab
oracle.kv.auth.username = krbuser@EXAMPLE.COM
oracle.kv.auth.external.mechanism=kerberos
oracle.kv.auth.kerberos.services=
node01:oraclenosql/node01.example.com@EXAMPLE.COM
oracle.kv.auth.kerberos.mutualAuth=false
```

Import Utility Configuration File

The import utility uses a plain-text configuration file which describes the import type and the location of the exported data. It is identified to the utility using the required `-config` command line parameter.

The contents of the configuration file differ depending on the value specified for the utility's `export-type` parameter.

If `LOCAL` is specified, then the configuration file contains the following information:

- `export-type = LOCAL`

Indicates that this export is stored on a local file system.

- `export-package-path = <path_for_export>`

Identifies the path to the directory where the export package can be located.

- `t1` is used for import only (see [import \(page 187\)](#) for details). This parameter is illegal if you are using it with the export utility. It must specify either absolute or relative.

If absolute, then the expiration timestamp on the data is observed without adjustment. This is the default.

If relative, then the expiration timestamp is adjusted relative to a date and time value provided using the `t1-relative-date` parameter.

- `t1-relative-date` is used only when the `t1` parameter is set to relative. It requires you to set a date and time value which is used to calculate the timeout value for the data. It is provided in `YYYY-MM-DD HH:MM:SS` format.

For example, a configuration file used when importing from the local file system might contain:

```
export-type = LOCAL
export-package-path = /mnt/dsk1/nosql_export_dir
t1 = absolute
```


Use `OBJECT_STORE` if the `import` utility is being used with Oracle Storage Cloud Services. In this case, the configuration file must contain the following information:

Note

To use the `import` utility with Oracle Storage Cloud Services, you must download and install Java jar files which provide necessary support. See [Installing the Cloud Storage JARs \(page 73\)](#) for details.

- `export-type = OBJECT_STORE`

Indicates that the export is located in Oracle Storage Cloud Services.

- `container-name = <container_name>`

The name of the container in Oracle Storage Cloud Service where the exported data is stored.

- `service-name = <service_name>`

The service name associated with the Oracle Storage Cloud Service subscription.

- `user-name = <user_name>`

The user name associated with the Oracle Storage Cloud Service subscription.

- `password` is the password you use with the Oracle Storage Cloud Service subscription.

- `service-url = <service_url>`

The service URL associated with the Oracle Storage Cloud Service subscription.

- `ttl` is used for import only (see [import \(page 187\)](#) for details). This parameter is illegal if you are using it with the export utility. It must specify either absolute or relative.

If absolute, then the expiration timestamp on the data is observed without adjustment. This is the default.

If relative, then the expiration timestamp is adjusted relative to a date and time value provided using the `ttl-relative-date` parameter.

- `ttl-relative-date` is used only when the `ttl` parameter is set to relative. It requires you to set a date and time value which is used to calculate the timeout value for the data. It is provided in `YYYY-MM-DD HH:MM:SS` format.

For example, a configuration file used when importing from Oracle Cloud Service Storage might contain:

```
export-type = OBJECT_STORE
container-name = TestContainer
service-name = Storage-nosqlldb
user-name = nosqlldb.Storageadmin
```

```
password = objs4KV!
service-url = https://storage-den2.oraclecorp.com
ttl = absolute
```

Import Exit Codes

Name	Code	Description
EXIT_OK	0	No errors found.
EXIT_USAGE	100	Illegal import command usage.
EXIT_NOPERM	101	Unauthorized access to the Oracle Cloud Storage Service.
EXIT_EXPSTR_NOCONNECT	102	The Oracle Cloud Storage Service could not be accessed using the service connection parameters.
EXIT_NOCONNECT	103	The source store could not be connected using the given store name and helper host.
EXIT_UNEXPECTED	104	The utility experienced an unexpected error.
EXIT_NOREAD	106	The import utility does not have permission to read the export package.
EXIT_INVALID_EXPORT_STORE	109	Invalid export store type. Valid export types are LOCAL or OBJECT_STORE.
EXIT_SECURITY_ERROR	110	Error loading security file.
EXIT_NOEXPPACKAGE	112	The export package required for import can not be found at the identified location. For Oracle Cloud Storage Service, the means the required container cannot be found.

load admin metadata

```
java -Xmx<javamxvalue> -Xms<javamxvalue> \
-jar KVHOME/lib/kvstore.jar load -store <storeName>
-host <hostname> -port <port> -load-admin
-source <admin-backup-dir> [-force]
[-username <user>] [-security <security-file-path>]
```

Loads the admin metadata from the snapshot to the new store. In this case the -source directory must point to the environment directory of the admin node from the snapshot. The store must not be available for use by users at the time of this operation.

where:

- `-load-admin` Specifies that only admin metadata will be loaded into the store.

Note

This option should not be used on a store unless that store is being restored from scratch. If `-force` is specified in conjunction with `-load-admin`, any existing metadata in the store, including tables and security metadata, will be overwritten. See [Using the Load Program \(page 63\)](#) for more information.

- `-host <hostname>` Identifies the host name of a node in your store.
- `-port <port>` Identifies the registry port in use by the store's Node.
- `-security <security-file-path>` Identifies the security file used to specify properties for login.
- `-source <admin-backup-dir>` The admin snapshot directory containing the contents of the admin metadata that is to be loaded into the store.
- `-store <storeName>` Identifies the new store which is the target of the load.
- `-username <user>` Identifies the name of the user to login to the secured store.

load store data

```
java -Xmx<javamxvalue> -Xms<javamxvalue> \  
-jar KVHOME/lib/kvstore.jar load [-verbose] \  
-store <storeName> -host <hostname> -port <port> \  
-source <shard-backup-dir>[, <shard-backup-dir>]* \  
[-checkpoint <checkpoint-files-directory>] \  
[-username <user>] [-security <security-file-path>]
```

Loads data into a store from backup directories. The bulk put API is used by this utility to load data into the target store. To recreate the complete contents of the store, you must specify one directory per shard for each shard associated with the store.

The load utility is highly parallelized. To further boost load performance, you can choose to run multiple concurrent invocations of the load utility on different machines, and assign each invocation a non-overlapping subset of the shard directories, using the `-source` argument. The use of these additional machine resources could significantly decrease overall elapsed load times.

Note

Creating multiple processes on the same machine is unlikely to be beneficial and could be detrimental, since the two processes are likely to be contending for the same CPU and network resources.

where:

- `-checkpoint <checkpoint-files-directory>` The utility used this directory to checkpoint its progress on a periodic basis. If the load process is interrupted for some reason, the progress checkpoint information is used to skip data that had already been loaded when the load utility is subsequently re-executed with the same arguments. If the `-checkpoint` flag is not specified, progress will not be checkpointed and all the data in the partitions that were already loaded will be reread.
- `-host <hostname>` Identifies the host name of a node in your store.
- `-port <port>` Identifies the registry port in use by the store's node.
- `-security <security-file-path>` Identifies the security file used to specify properties for login.
- `-source <shard-backup-dir>[,<shard-backup-dir>]*` These backup directories typically represent the contents of snapshots created using the snapshot commands described at [Taking a Snapshot \(page 60\)](#).
- `-store <storeName>` Identifies the name of the store.
- `-username <user>` Identifies the name of the user to login to the secured store.

makebootconfig

```
java -Xmx256m -Xms256m
-jar KVHOME/lib/kvstore.jar makebootconfig [-verbose]
-root <rootDirectory> -host <hostname> -horange <startPort,endPort>
-port <port> [-config <configFile>]
[-store-security <none | configure | enable> ]
[-noadmin]
[-storagedir <directory path>] [-storagedirsize <directory size>]
[-capacity <n_rep_nodes>]
[-num_cpus <ncpus>][-memory_mb <memory_mb>]
[-servicerange <startPort,endPort>]
[-hahost <haHostname>]
[-secdir <security dir>] [-pwmgr {pwdfile | wallet | <class-name>}]
[-kspwd <password>]
[-external-auth {kerberos}]
  [-krb-conf <kerberos configuration>]
  [-kadmin-path <kadmin utility path>]
  [-instance-name <database instance name>]
  [-admin-principal <kerberos admin principal name>]
  [-kadmin-keytab <keytab file>]
  [-kadmin-ccache <credential cache file>]
  [-princ-conf-param <param=value>]*
[-security-param <param=value>]*
[-mgmt {jmx|none}]
[-dns-cachettl <time in sec>]
```

[-force]

where:

- `-capacity <n_rep_nodes>` The total number of Replication Nodes a Storage Node can support. The value defaults to "1".

If capacity is set to 0, then this Storage Node may be used to host Arbiter Nodes.

- `-config <configFile>` Only specified if more than one Storage Node Agent process will share the same root directory. This value defaults to "config.xml".
- `-dns-cachettl <time in sec>` Specifies the number of seconds that Replication Nodes should cache host name to IP address mappings. The default value is -1, which means mappings should be cached indefinitely. A value of 0 means mappings should not be cached. The value of this flag is used to set the `networkaddress.cache.ttl` and `networkaddress.cache.negative.ttl` security properties.
- `-external-auth {kerberos}` Specifies Kerberos as an external authentication service. If no keytab or credential cache has been specified on the command line, an interactive version of the `securityconfig` utility will run.

This flag is only permitted when the value of the `-store-security` flag is specified as `configure` or `enable`.

To remove Kerberos authentication from a running store, set the value of the `userExternalAuth` `security.xml` parameter to `NONE`.

For more information on Kerberos, see the *Oracle NoSQL Database Security Guide*.

where `-external-auth` can have the following flags:

- `-admin-principal <kerberos admin principal name>`

Specifies the principal used to login to the Kerberos admin interface. This is required while using `kadmin` keytab or password to connect to the admin interface.

- `-kadmin-ccache <credential cache file>`

Specifies the complete path name to the Kerberos credentials cache file that should contain a service ticket for the `kadmin/ADMINHOST`. `ADMINHOST` is the fully-qualified hostname of the admin server or `kadmin/admin` service.

If not specified, the user is prompted to enter the password for principal while logging to the Kerberos admin interface. This flag cannot be specified in conjunction with the `-kadmin-keytab` flag.

- `-kadmin-keytab <keytab file>`

Specifies the location of a Kerberos keytab file that stores Kerberos admin user principals and encrypted keys. The security configuration tool will use the specified keytab file to login to the Kerberos admin interface.

The default location of the keytab file is specified by the Kerberos configuration file. If the keytab is not specified there, then the system looks for the file `user.home/krb5.keytab`.

You need to specify the `-admin-principal` flag when using keytab to login to the Kerberos admin, otherwise the correct admin principal will not be recognized. This flag cannot be specified in conjunction with the `-kadmin-ccache` flag.

- `-kadmin-path <kadmin utility path>`

Indicates the absolute path of the Kerberos kadmin utility. The default value is `/usr/kerberos/sbin/kadmin`.

- `-krb-conf <kerberos configuration>`

Specifies the location of the Kerberos configuration file that contains the default realm and KDC information. If not specified, the default value is `/etc/krb5.conf`.

- `-princ-conf-param <param=value>*`

A repeatable argument that allows configuration defaults to be overridden.

Use the `krbPrincValidity` parameter to specify the expiration date of the Oracle NoSQL Database Kerberos service principal.

Use the `krbPrincPwdExpire` parameter to specify the password expiration date of the Oracle NoSQL Database Kerberos service principal.

Use the `krbKeysalt` parameter to specify the list of encryption types and salt types to be used for any new keys created.

- `-force` Optionally specified to force generating the boot configuration files even if boot config verification finds any invalid parameters.
- `-hahostname <hostname>` Can be used to specify a separate network interface for store replication traffic. This defaults to the hostname specified using the `-host` flag.
- `-harange <startPort,endPort>` A range of free ports which the Replication Nodes use to communicate among themselves. These ports should be sequential and there must be at least as many as the specified capacity for this node.
- `-host <hostname>` Identifies a host name associated with the node on which the command is run. This hostname identifies the network interface used for communication with this node.
- `-kspwd<password>` For script-based configuration you can use this option to allow tools to specify the keystore password on the command line. If it is not specified, the user is prompted to enter the password.
- `-memory_mb <memory_mb>` The total number of megabytes of memory that is available in the machine. If the value is 0, the store will attempt to determine the amount of memory

on the machine, but the value is only available when the JVM used is the Oracle Hotspot JVM. The default value is "0".

For best results, do not specify this parameter. Oracle NoSQL Database will determine the proper value by default. This parameter should be used sparingly, and only for exceptional situations.

- `-num_cpus <ncpus>` The total number of processors on the machine available to the Replication Nodes. If the value is 0, the system will attempt to query the Storage Node to determine the number of processors on the machine. This value defaults to "0".

For best results, do not specify this parameter. Oracle NoSQL Database will determine the proper value by default. This parameter should be used sparingly, and only for exceptional situations.

- `-port <port>` The TCP/IP port on which Oracle NoSQL Database should be contacted. Sometimes referred to as the registry port. This port must be free on the node on which this command is run.
- `-pwmgr [pwdfile | wallet]`

Indicates the password manager mechanism used to hold passwords that are needed for access to keystores, etc.

where `-pwmgr` can have the following options:

- `-pwmgr pwdfile`

Indicates that the password store is a read-protected clear-text password file. This is the only available option for Oracle NoSQL Database CE deployments. You can specify an alternate implementation.

- `-pwmgr wallet`

Specifies Oracle Wallet as the password storage mechanism. This option is only available in the Oracle NoSQL Database EE version.

- `-root <rootDirectory>` Identifies where the root directory should reside.
- `-secdir <security dir>`

Specifies the name of the directory within the KVROOT that will hold the security configuration. This must be specified as a name relative to the specified secroot. If not specified, the default value is "security".

- `-security-param <param=value>*`

A repeatable argument that allows configuration defaults to be overridden.

Use the `krbServiceName` parameter to specify the service name of the Oracle NoSQL Database Kerberos service principal.

Use the `krbServiceKeytab` parameter to specify the keytab file name in security directory of the Oracle NoSQL Database Kerberos service principal.

- `-servicerange <startPort,endPort>` A range of ports that may be used for communication among administrative services running on a Storage Node and its managed services. This parameter is optional and is useful when services on a Storage Node must use specific ports for firewall or other security reasons. By default the services use anonymous ports. The format of the value string is "startPort,endPort."
- `-storagedir <path>` Specify a path to the directory to be used for a Replication Node. This flag may be used more than once in the command to specify multiple storage directories, but the number should not exceed the capacity for the node. If no storage directory is specified, Replication Nodes use a directory under the root directory.

The use of the `-storagedir` argument must be coordinated with the use of the `capacity` argument. For example, if your Storage Node hosts four disks, you would specify a capacity of four and have four `-storagedir` arguments.

- `-storagedirsize <directory size>` Specifies the size of the directory specified in `-storagedir`. This parameter is optional; however, it is an error to specify this parameter for some, but not all, storage directories.

Use of this parameter is recommended for heterogeneous installation environments where some hardware has more storage capacity than other hardware. If this parameter is specified for all storage directories, then the store's topology will place more data on the shards that offer more storage space. If this parameter is not used, then data is spread evenly across all shards.

The value specified for this parameter must be a long, followed optionally by a unit string. Accepted unit strings are: KB, MB, GB, and TB, corresponding to 1024 , 1024^2 , 1024^3 , 1024^4 respectively. Acceptable strings are case insensitive. Valid delimiters between the long value and the unit string are " ", "-", or "_".

For example:

```
-storagedirsize 200 MB
-storagedirsize 4_tb
-storagedirsize 5000-Mb
```

- `-noadmin` Specifies to disable the bootstrap admin service for SNA.
- `-store-security [none | configure | enable]` Specifies if security will be used or not. If `-store-security none` is specified, no security will be used. If `-store-security configure` is specified, security will be used and the security configuration utility will be invoked as part of the `makebootconfig` process. If `-store-security enable` is specified, security will be used. You will need to configure security either by utilizing the security configuration utility or by copying a previously created configuration from another system.

Note

-store-security command is optional. Even if the user does not specify -store-security, it would be enabled by default. The user must run securityconfig utility to create the security folder before starting up the storage node agent.

Creates a configuration file used to start a not-yet-deployed Storage Node to be used in an instance of Oracle NoSQL Database. The file must not already exist. To create the initial "boot config" file used to configure the installation see [Installation Configuration \(page 3\)](#).

ping

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar ping [-verbose] [-json]  
-host <hostname> -port <port> or  
-helper-hosts <host:port>[,host:port]*>  
-username <user>  
-security <security-file-path>
```

Attempts to contact a store to get status of running services. This utility provides both a concise summary of the health of a store, as well as detailed information about the topology of the store. It can signal a red/yellow/green status, to let you know whether the store is in full health, whether the store has experienced some failures but is operational, or whether the store has critical problems. ping uses the nodes specified by the -helper-hosts or -host/-port arguments to locate topology metadata describing the store. Using that topology, ping contacts all the RNs, SNs, Arbiters, and Admin services associated with a store.

Specify the -helper-hosts flag as an alternative to the existing -host and -port flags. If multiple helper hosts are provided, this utility will have multiple nodes it can use to make an initial point of contact with the store, and will have a greater chance of success if some nodes of the store are unavailable.

Ping Command Line Parameters

The ping utility's command line parameters are:

- -host identifies the name of a specific host in the store. Use this option to check whether the SNA on that particular host can be contacted.

If this parameter is specified, then -port must also be specified. Further, if the -host and -port parameters are specified, then the -helper-hosts must not be specified.

- -port identifies the listening port for a specific host in the store. Use this parameter only if you are also using the -host parameter.
- -helper-hosts identifies a comma-separated list of one or more host:port pairs in the store. Use this parameter to check the health of the entire store.

If this parameter is specified, then -host and -port must not be specified.

If multiple helper hosts are provided, this utility will have multiple nodes it can use to make an initial point of contact with the store, and will have a greater chance of success if some nodes of the store are unavailable. For example:

```
-helper-hosts hst1:5000,hst2:5100,hst3:5100
```

- `-username` is the name of the user that you want to ping the store as. This parameter is required if your store is configured to require authentication. This user should have at least SYSVIEW access to the store. The built-in dbadmin role is sufficient.
- `-security` is the client security configuration file. This parameter is required if your store is configured to require authentication. For information on the parameters contained in this file, see *Configuring SSL in the Oracle NoSQL Database Getting Started with the Table API for Java* guide. For example:

```
oracle.kv.auth.username=clientUID1
oracle.kv.auth.pwdfile.file=/home/nosql/login.pwd
oracle.kv.transport=ssl
oracle.kv.ssl.trustStore=/home/nosql/client.trust
```

If you are using Kerberos, then this file would look something like this:

```
oracle.kv.auth.kerberos.keytab = kerberos/mykeytab
oracle.kv.auth.username = krbuser@EXAMPLE.COM
oracle.kv.auth.external.mechanism=kerberos
oracle.kv.auth.kerberos.services=
node01:oraclenosql/node01.example.com@EXAMPLE.COM
oracle.kv.auth.kerberos.mutualAuth=false
```

- `-verbose` is optional. It causes the ping utility to provide additional information about the utility's current actions.
- `-json` causes the ping utility to write its output in JSON format.

Ping Exit Codes

The following exit codes can be returned by this utility. Exit codes can be returned both as a process exit code, and as part of the JSON output.

Name	Code	Description
EXIT_OK	0	All services in the store could be located and are in a known, good state (for example, RUNNING).
EXIT_OPERATIONAL	1	One or more services in the store could not be reached, or are in an unknown or not usable state. In this case the store should support all data operations across all shards, as well as all

Name	Code	Description
		administrative operations, but may be in a state of degraded performance. Some action should be taken to find and fix the problem before part of the store becomes unavailable.
EXIT_NO_ADMIN_QUORUM	2	The Admin Service replication group does not have quorum or is not available at all, and it is not possible to execute administrative operations which modify store configuration. The store supports all normal data operations despite the loss of admin quorum, but this state requires immediate attention to restore full store capabilities.
EXIT_NO_SHARD_QUORUM	3	One or more of the shards does not have quorum and either cannot accept write requests, or is completely unavailable. This state requires immediate attention to restore store capabilities. The exit code takes precedence over EXIT_NO_ADMIN_QUORUM, so if this exit code is used, it is possible that the administrative capabilities are also reduced or unavailable.
EXIT_USAGE	100	Illegal ping command usage.
EXIT_TOPOLOGY_FAILURE	101	ping was unable to find a topology in order to operate. This could be a store problem, a network problem, or it could be a usage problem with the parameters passed to ping. For example, the specified -host/-port pair are not part of the store, or none of the hosts specified

Name	Code	Description
		on -helper-hosts can be contacted.
EXIT_UNEXPECTED	102	The utility has experienced an unexpected error.

Note

Exit codes 1 through 3 may indicate a network connectivity issue that should be checked first before concluding that any services have a problem.

Ping Report Text Output

By default, the ping utility reports store health in human readable format. For example:

Note

Extra line breaks have been introduced to allow this output to fit in the available space.

```
$ java -jar <KVHOME>/lib/kvstore.jar ping -host nodeA -port 1310
Pinging components of store mystore based upon topology sequence #108
100 partitions and 3 storage nodes
Time: 2016-03-11 04:21:04 UTC   Version: 12.1.4.0.1
Shard Status: healthy:1 writable-degraded:0 read-only:0 offline:0
Admin Status: healthy
Zone [name=MyDC id=zn1 type=PRIMARY allowArbiters=false]
RN Status: online:3 offline:0 maxDelayMillis:0 maxCatchupTimeSecs:0
Storage Node [sn1] on nodeA:13100
Zone: [name=MyDC id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING   Ver: 12cR1.4.0.3 2016-03-10 09:33:21 UTC
Build id: 238b56a47a00+
    Admin [admin1]           Status: RUNNING,MASTER
    Rep Node [rg1-rn1]       Status: RUNNING,MASTER
    sequenceNumber:227 haPort:13117
Storage Node [sn2] on nodeB:13200
Zone: [name=MyDC id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING   Ver: 12cR1.4.0.3 2016-03-10 09:33:21 UTC
Build id: 238b56a47a00+
    Admin [admin2]           Status: RUNNING,REPLICA
    Rep Node [rg1-rn2]       Status: RUNNING,REPLICA
    sequenceNumber:227 haPort:13217 delayMillis:0
    catchupTimeSecs:0
Storage Node [sn3] on nodeC:13300
Zone: [name=MyDC id=zn1 type=PRIMARY allowArbiters=false]
Status: RUNNING   Ver: 12cR1.4.0.3 2016-03-10 09:33:21 UTC
Build id: 238b56a47a00+
    Admin [admin3]           Status: RUNNING,REPLICA
    Rep Node [rg1-rn3]       Status: RUNNING,REPLICA
    sequenceNumber:227 haPort:13317 delayMillis:0
```

```
catchupTimeSecs:0
```

Ping Report JSON Output

When the `-json` command line parameter is specified, this utility provides its report in JSON formatting.

Note

Extra line breaks have been introduced to allow this output to fit in the available space.

```
bash-3.2$ java -jar dist/lib/kvstore.jar ping -host nodeA \
-port 13100 -json
{
  "topology" : {
    "storeName" : "mystore",
    "sequenceNumber" : 108,
    "numPartitions" : 100,
    "numStorageNodes" : 3,
    "time" : 1457670762500,
    "version" : "12.1.4.0.1"
  },
  "adminStatus" : "healthy",
  "shardStatus" : {
    "healthy" : 1,
    "writable-degraded" : 0,
    "read-only" : 0,
    "offline" : 0
  },
  "zoneStatus" : [ {
    "resourceId" : "zn1",
    "name" : "MyDC",
    "type" : "PRIMARY",
    "allowArbiters" : false,
    "rnSummaryStatus" : {
      "online" : 3,
      "offline" : 0,
      "hasReplicas" : true,
      "maxDelayMillis" : 0,
      "maxCatchupTimeSecs" : 0
    }
  } ],
  "snStatus" : [ {
    "resourceId" : "sn1",
    "hostname" : "nodeA",
    "registryPort" : 13100,
    "zone" : {
      "resourceId" : "zn1",
      "name" : "MyDC",
```

```

    "type" : "PRIMARY",
    "allowArbiters" : false
  },
  "serviceStatus" : "RUNNING",
  "version" : "12cR1.4.0.3 2016-03-10 09:33:21 UTC
    Build id: 238b56a47a00+",
  "adminStatus" : {
    "resourceId" : "admin1",
    "status" : "RUNNING",
    "state" : "MASTER",
    "authoritativeMaster" : true
  },
  "rnStatus" : [ {
    "resourceId" : "rg1-rn1",
    "status" : "RUNNING",
    "state" : "MASTER",
    "authoritativeMaster" : true,
    "sequenceNumber" : 227,
    "haPort" : 13117
  } ],
  "anStatus" : [ ]
}, {
  "resourceId" : "sn2",
  "hostname" : "nodeB",
  "registryPort" : 13200,
  "zone" : {
    "resourceId" : "zn1",
    "name" : "MyDC",
    "type" : "PRIMARY",
    "allowArbiters" : false
  },
  "serviceStatus" : "RUNNING",
  "version" : "12cR1.4.0.3 2016-03-10 09:33:21 UTC
    Build id: 238b56a47a00+",
  "adminStatus" : {
    "resourceId" : "admin2",
    "status" : "RUNNING",
    "state" : "REPLICA"
  },
  "rnStatus" : [ {
    "resourceId" : "rg1-rn2",
    "status" : "RUNNING",
    "state" : "REPLICA",
    "sequenceNumber" : 227,
    "haPort" : 13217,
    "networkRestoreUnderway" : false,
    "delayMillis" : 0,
    "catchupTimeSecs" : 0,
    "catchupRateMillisPerMinute" : 0
  } ]
}

```

```

    } ],
    "anStatus" : [ ]
  }, {
    "resourceId" : "sn3",
    "hostname" : "nodeC",
    "registryPort" : 13300,
    "zone" : {
      "resourceId" : "zn1",
      "name" : "MyDC",
      "type" : "PRIMARY",
      "allowArbiters" : false
    },
    "serviceStatus" : "RUNNING",
    "version" : "12cR1.4.0.3 2016-03-10 09:33:21 UTC
      Build id: 238b56a47a00+",
    "adminStatus" : {
      "resourceId" : "admin3",
      "status" : "RUNNING",
      "state" : "REPLICA"
    },
    "rnStatus" : [ {
      "resourceId" : "rg1-rn3",
      "status" : "RUNNING",
      "state" : "REPLICA",
      "sequenceNumber" : 227,
      "haPort" : 13317,
      "networkRestoreUnderway" : false,
      "delayMillis" : 0,
      "catchupTimeSecs" : 0,
      "catchupRateMillisPerMinute" : 0
    } ],
    "anStatus" : [ ]
  } ],
  "operation" : "ping",
  "return_code" : 5000,
  "description" : "No errors found",
  "exit_code" : 0

```

restart

```

java -Xmx256m -Xms256m \
-jar KVHOME/lib/kvstore.jar restart
[-disable-services] [-verbose]
-root <rootDirectory> [-config <bootstrapFileName>]

```

Stops and then starts the Oracle NoSQL Database Storage Node Agent and services related to the root directory.

To disable all services associated with a stopped SNA use the `-disable-services` flag. For more information, see [Disabling Storage Node Agent Hosted Services \(page 84\)](#)

runadmin

```
java -Xmx<javamxvalue> -Xms<javamxvalue> \  
-jar KVHOME/lib/kvstore.jar runadmin  
-host <hostname> -port <port> [-store <storeName> ]  
[-admin-host <adminHost> -admin-port <adminPort> ]  
[-username <user>] [-security <security-file-path>]  
[-admin-username <adminUser>]  
[-admin-security <admin-security-file-path>]  
[-timeout <timeout ms>]  
[-consistency <NONE_REQUIRED(default) | ABSOLUTE |  
    NONE_REQUIRED_NO_MASTER>]  
[-durability <COMMIT_SYNC(default) | COMMIT_NO_SYNC |  
    COMMIT_WRITE_NO_SYNC>]  
[single command and arguments]
```

Runs a utility which provides a command line interface (CLI). It is used to perform store configuration.

Use the timeout, consistency and durability flags to override the default connect configuration.

where:

- **-timeout**
Specifies the store request timeout in milliseconds.
- **-consistency**
Specifies the store request consistency. The default value is NONE_REQUIRED.
- **-durability**
Specifies the store request durability. The default value is COMMIT_SYNC.

start

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar start  
[-disable-services] [-verbose]  
-root <rootDirectory> [-config <bootstrapFileName>]
```

Starts the Oracle NoSQL Database Storage Node Agent (and if configured, store) in the root directory.

To disable all services associated with a stopped SNA use the **-disable-services** flag. For more information, see [Disabling Storage Node Agent Hosted Services \(page 84\)](#)

status

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar status
```



```
-jar KVHOME/lib/kvstore.jar status  
-root <rootDirectory> [-config <bootstrapFileName>]  
[-verbose] [-disable-services]
```

Attempts to connect to a running Oracle NoSQL Database Storage Node Agent and prints out its status.

For example:

```
java -Xmx256m -Xms256m -jar KVHOME/lib/kvstore.jar \  
status -root KVR00T  
SNA Status : RUNNING
```

stop

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar stop  
[-disable-services] [-verbose]  
-root <rootDirectory> [-config <bootstrapFileName>]
```

Stops the Oracle NoSQL Database Storage Node Agent and services related to the root directory.

To disable all services associated with a stopped SNA use the `-disable-services` flag. For more information, see [Disabling Storage Node Agent Hosted Services \(page 84\)](#)

version

```
java -Xmx256m -Xms256m \  
-jar KVHOME/lib/kvstore.jar version
```

Prints version.

Appendix D. Initial Capacity Planning

To deploy a store, the user must specify a replication factor, the desired number of partitions, and the Storage Nodes on which to deploy the store. The following sections describe how to calculate these values based upon the application's requirements and the characteristics of the hardware available to host the store.

The resource estimation is a two step process:

1. Determine the storage and I/O throughput capacity of a representative shard, given the characteristics of the application, the disk configuration on each machine, and disk throughput. The amount of physical memory required by each machine and its network throughput capacity is also estimated as part of this step.
2. Use the shard level storage and I/O throughput capacities as a basis for extrapolating throughput from one shard to the required number of shards and machines, given the storewide application requirements.

There is an accompanying spreadsheet that should be used in the planning process. You can find the spreadsheet in your Oracle NoSQL Database distribution here: <KVHOME>/doc/misc/InitialCapacityPlanning.xls.

The sections in this appendix correspond to named sections in the spreadsheet. Column A of the spreadsheet lists cell names that are associated with the values in column B. Cell names in red represent values that must be provided as input. Column C describes the value or the computation associated with the value in column B. The sections: [Application Characteristics \(page 208\)](#), [Hardware Characteristics \(page 209\)](#), and [Machine Physical Memory \(page 211\)](#) contain required inputs. Green cell names denote optional inputs; the default values supplied in the spreadsheet should be adequate for most estimates. All other cells are computed by the spreadsheet using the formulas described below.

After filling in the required inputs, the cell *StoreMachines* value will tell you how many Storage Nodes should be available in the storage node pool. The *StorePartitions* value will tell you how many partitions should be specified when creating the store.

Please keep in mind that the computations below yield estimates. The underlying model used as a basis for the estimation makes simplifying assumptions since it's hard to come up with a simple single underlying model that will work well under a wide range of application requirements. So these estimates should only be used as the basis for an initial starting point and refined under simulated or actual load.

Shard Capacity

To determine the shard capacity first determine the application and hardware characteristics described in this section. Having determined these characteristics, enter them into the

accompanying spreadsheet. The spread sheet will then calculate the capacity of a shard on the basis of the supplied application and hardware characteristics.

Application Characteristics

Replication Factor

In general, a *Primary Replication Factor* of 3 is adequate for most applications and is a good starting point, because 3 replicas allow write availability if a single primary zone fails. It can be refined if performance testing suggests some other number works better for the specific workload. Do not select a *Primary Replication Factor* of 2 because doing so means that even a single failure results in too few sites to elect a new master. This is not the case if you have an Arbiter Node, as a new master can still be elected if the Replication Factor is two and you lose a Replication Node. However, if you have multiple failures before both Replication Nodes are caught up, you may not be able to elect a new master. A *Primary Replication Factor* of 1 is to be avoided in general since Oracle NoSQL Database has just a single copy of the data; if the storage device hosting the data were to fail the data could be lost.

Larger *Primary Replication Factors* provide two benefits:

1. Increased durability to better withstand disk or machine failures.
2. Increased read request throughput, because there are more nodes per shard available to service those requests.

However, the increased durability and read throughput has costs associated with it: more hardware resources to host and serve the additional copies of the data and slower write performance, because each shard has more nodes to which updates must be replicated.

Note

Only the Primary Replication Factor affects write availability, but both Primary and Secondary Replication Factors, and therefore the Store Replication Factor, have an effect on read availability.

The *Primary Replication Factor* is defined by the cell *RF*.

Average Key Size

Use knowledge of the application's key schema and the relative distributions of the various keys to arrive at an average key length. The length of a key on disk is the number of UTF-8 bytes needed to represent the components of the key, plus the number of components, minus one.

This value is defined by the cell *AvgKeySize*.

Average Value Size

Use knowledge of the application to arrive at an average serialized value size. The value size will vary depending upon the particular serialization format used by the application.

This value is defined by the cell *AvgValueSize*.

Read and Write Operation Percentages

Compute a rough estimate of the relative frequency of store level read and write operations on the basis of the KVS API operations used by the application.

At the most basic level, each KVS `get()` call results in a store level read operation and each `put()` operation results in a store level write operation. Each KVS multi key operation (`KVStore.execute()`, `multiGet()`, or `multiDelete()`) can result in multiple store level read/write operations. Again, use application knowledge about the number of keys accessed in these operations to arrive at an estimate.

Express the estimate as a read percentage, that is, the percentage of the total operations on the store that are reads. The rest of the operations are assumed to be write operations.

This value is defined by the cell *ReadOpsPercent*.

Estimate the percentage of read operations that will likely be satisfied from the file system cache. The percentage depends primarily upon the application's data access pattern and the size of the file system cache. [Sizing Advice \(page 211\)](#) contains a discussion of how this cache is used.

This value is defined by the cell *ReadCacheHitPercent*.

Hardware Characteristics

Determine the following hardware characteristics based on a rough idea of the type of the machines that will be used to host the store:

- The number of disks per machine that will be used for storing KV pairs. This value is defined by the cell *DisksPerMachine*. The number of disks per machine typically determines the Storage Node Capacity as described in [Storage Node Parameters \(page 94\)](#).
- The usable storage capacity of each disk. This value is defined by the cell *DiskCapacityGB*.
- The IOPs capacity of each disk. This information is typically available in the disk spec sheet as the number of sustained random IO operations/sec that can be delivered by the disk. This value is defined by the cell *DiskIopsPerSec*.

The following discussion assumes that the system will be configured with one RN per disk.

Shard Storage and Throughput Capacities

There are two types of capacity that are relevant to this discussion: 1) Storage Capacity 2) Throughput Capacity. The following sections describe how these two measures of capacity are calculated. The underlying calculations are done automatically by the attached spreadsheet based upon the application and hardware characteristics supplied earlier.

Shard Storage Capacity

The storage capacity is the maximum number of KV pairs that can be stored in a shard. It is calculated by dividing the storage actually available for live KV pairs (after accounting for the

storage set aside as a safety margin and cleaner utilization) by the storage (including a rough estimation of Btree overheads) required by each KV pair.

The KV Storage Capacity is computed by the cell: *MaxKVPairsPerShard*.

Shard I/O Throughput capacity

The throughput capacity is a measure of the read and write ops that can be supported by a single shard. In the calculations below, the logical throughput capacity is derived from the disk IOPs capacity based upon the percentage of logical operations that actually translate into disk IOPs after allowing for cache hits. The [Machine Physical Memory \(page 211\)](#) section contains more detail about configuring the caches used by Oracle NoSQL Database.

For logical read operations, the shard-wide IOPs is computed as:

```
(ReadOpsPercent * (1 - ReadCacheHitPercent))
```

Note that all percentages are expressed as fractions.

For logical write operations, the shard-wide IOPs is computed as:

```
((1 - ReadOpsPercent) / WriteOpsBatchSize) * RF)
```

The writeops calculations are very approximate. Write operations make a much smaller contribution to the IOPs load than do the read ops due to the sequential writes used by the log structured storage system. The use of WriteOpsBatchSize is intended to account for the sequential nature of the writes to the underlying JE log structured storage system. The above formula does not work well when there are no reads in the workload, that is, under pure insert or pure update loads. Under pure insert, the writes are limited primarily by acknowledgement latency which is not modeled by the formula. Under pure update loads, both the acknowledgement latency and cleaner performance play an important role.

The sum of the above two numbers represents the percentage of logical operations that actually result in disk operations (the *DiskIopsPercent* cell). The shard's logical throughput can then be computed as:

```
(DiskIopsPerSec * RF) / DiskIopsPercent
```

and is calculated by the cell *OpsPerShardPerSec*.

Memory and Network Configuration

Having established the storage and throughput capacities of a shard, the amount of physical memory and network capacity required by each machine can be determined. Correct configuration of physical memory and network resources is essential for the proper operation of the store. If your primary goal is to determine the total size of the store, skip ahead to [Estimate total Shards and Machines \(page 214\)](#) but make sure to return to this section later when it is time to finalize the machine level hardware requirements.

Note

You can also set the memory size available for each Storage Node in your store, either through the `memory_mb` parameter of the `makebootconfig` utility or through

the `memorymb Storage Node` parameter. For more information, see [Installation Configuration \(page 3\)](#) and [Storage Node Parameters \(page 94\)](#) respectively.

Machine Physical Memory

The shard storage capacity (computed by the cell `MaxKVPairsPerShard`) and the average key size (defined by the cell `AvgKeySize`) can be used to estimate the physical memory requirements of the machine. The physical memory on the machine backs up the caches used by Oracle NoSQL Database.

Sizing the in-memory cache correctly is essential for meeting store's performance goals. Disk I/O is an expensive operation from a performance point of view; the more operations that can be serviced from the cache, the better the store's performance.

Before continuing, it is worth noting that there are two caches that are relevant to this discussion:

1. The JE cache. The underlying storage engine used by Oracle NoSQL Database is Berkeley DB Java Edition (JE). JE provides an in-memory cache. For the most part, this is the cache size that is most important, because it is the one that is simplest to control and configure.
2. The file system (FS) cache. Modern operating systems attempt to improve their I/O subsystem performance by providing a cache, or buffer, that is dedicated to disk I/O. By using the FS cache, read operations can be performed very quickly if the reads can be satisfied by data that is stored there.

Sizing Advice

JE uses a Btree to organize the data that it stores. Btrees provide a tree-like data organization structure that allows for rapid information lookup. These structures consist of interior nodes (INs) and leaf nodes (LNs). INs are used to navigate to data. LNs are where the data is actually stored in the Btree.

Because of the very large data sets that an Oracle NoSQL Database application is expected to use, it is unlikely that you can place even a small fraction of the data into JE's in-memory cache. Therefore, the best strategy is to size the cache such that it is large enough to hold most, if not all, of the database's INs, and leave the rest of the node's memory available for system overhead (negligible) and the FS cache.

Both INs and LNs can take advantage of the FS cache. Because INs and LNs do not have Java object overhead when present in the FS cache (as they would when using the JE cache), they can make more effective use of the FS cache memory than the JE cache memory.

Of course, in order for the FS cache to be truly effective, the data access patterns should not be completely random. Some subset of your key-value pairs must be favored over others in order to achieve a useful cache hit rate. For applications where the access patterns are not random, the high file system cache hit rates on LNs and INs can increase throughput and decrease average read latency. Also, larger file system caches, when properly tuned, can help reduce the number of stalls during sequential writes to the log files, thus decreasing

write latency. Large caches also permit more of the writes to be done asynchronously, thus improving throughput.

Determine JE Cache Size

To determine an appropriate JE cache size, use the `com.sleepycat.je.util.DbCacheSize` utility. This utility requires as input the number of records and the size of the application keys. You can also optionally provide other information, such as the expected data size. The utility then provides a short table of information. The number you want is provided in the Cache Size column, and in the Internal nodes and leaf nodes: MAIN cache row.

For example, to determine the JE cache size for an environment consisting of 100 million records, with an average key size of 12 bytes, and an average value size of 1000 bytes, invoke `DbCacheSize` as follows:

```
java -Xmx256m -Xms256m \
-d64 -XX:+UseCompressedOops -jar je.jar DbCacheSize \
-key 12 -data 1000 -records 100000000 -replicated \
-je.rep.preserveRecordVersion true -offheap
```

=== Environment Cache Overhead ===

3,164,485 minimum bytes

To account for JE daemon operation, record locks, HA network connections, etc, a larger amount is needed in practice.

=== Database Cache Size ===

Number of Bytes	Description
3,885,284,944	Internal nodes only: MAIN cache
0	Internal nodes only: OFF-HEAP cache
3,885,284,944	Internal nodes and leaf nodes: MAIN cache
104,002,733,216	Internal nodes and leaf nodes: OFF-HEAP cache

Please make note of the following jvm arguments (they have a special meaning when supplied to `DbCacheSize`):

1. The `-d64` argument is used to ensure that cache sizes account for a 64-bit JVM. Only 64-bit JVMs are supported by NoSQL DB.
2. The `-XX:+UseCompressedOops` causes cache sizes to account for CompressedOops mode, which is used by NoSQL DB by default. This mode uses more efficient 32 bit pointers in a 64-bit JVM thus permitting better utilization of the JE cache.
3. The `-replicated` is used to account for memory usage in a JE ReplicatedEnvironment, which is always used by NoSQL DB.
4. The `-je.rep.preserveRecordVersion` accounts for cache storage of record versions, which are always preserved in NoSQL DB. Versions are used in operations such as "put if version",

"delete if version", etc. This feature performs best when the cache is sized large enough to hold the record versions.

5. The `-offheap` is specified to use a JE off-heap cache, which is configured by default in NoSQL DB. This causes `DbCacheSize` to print values for the main (in-heap) cache and off-heap cache separately.

These arguments when supplied to Database Cache Size serve as an indication that the JE application will also be supplied these arguments and Database Cache Size adjusts its calculations appropriately. The arguments are used by Oracle NoSQL Database when starting up the Replication Nodes which uses these caches.

The output indicates that a cache size of 3.6 GB is sufficient to hold all the internal nodes representing the Btree in the JE cache. With a JE cache of this size, the IN nodes will be fetched from the JE cache and the LNs will be fetched from the off-heap cache or the disk.

For more information on using the `DbCacheSize` utility, see this Javadoc page: http://docs.oracle.com/cd/E17277_02/html/java/com/sleepycat/je/util/DbCacheSize.html. Note that in order to use this utility, you must add the `<KVHOME>/lib/je.jar` file to your Java classpath. `<KVHOME>` represents the directory where you placed the Oracle NoSQL Database package files.

Having used `DbCacheSize` to obtain the JE cache size, the heap size can be calculated from it. To do this, enter the number obtained from `DbCacheSize` into the cell named `DbCacheSizeMB` making sure to convert the units from bytes to MB. The heap size is computed by the cell `RNHeapMB` as below:

$$(DbCacheSizeMB / RNCachePercent)$$

where `RNCachePercent` is the percentage of the heap that is used for the JE cache. The computed heap size should not exceed 32GB, so that the java VM can use its efficient CompressedOops format to represent the java objects in memory. Heap sizes with values exceeding 32GB will appear with a strikethrough in the `RNHeapMB` cell to emphasize this requirement. If the heap size exceeds 32GB, try to reduce the size of the keys to reduce the JE cache size in turn and bring the overall heap size below 32GB.

The heap size is used as the basis for computing the memory required by the machine as below:

$$(RNHeapMB * DisksPerMachine) / SNRNHeapPercent$$

where `SNRNHeapPercent` is the percentage of the physical memory that is available for use by the RN's hosted on the machine. The result is available in the cell `MachinePhysicalMemoryMB`.

Machine Network Throughput

We need to ensure that the NIC attached to the machine is capable of delivering the application I/O throughput as calculated earlier in [Shard I/O Throughput capacity \(page 210\)](#), because otherwise it could prove to be a bottleneck.

The number of bytes received by the machine over the network as a result of write operations initiated by the client is calculated as:

$$(\text{OpsPerShardPerSec} * (1 - \text{ReadOpsPercent}) * (\text{AvgKeySize} + \text{AvgValueSize})) * \text{DisksPerMachine}$$

and is denoted by *ReceiveBytesPerSec* in the spreadsheet. Note that whether a node is a master or a replica does not matter for the purposes of this calculation; the inbound write bytes come from the client for the master and from the masters for the replicas on the machine.

The number of bytes received by the machine as a result of read requests is computed as:

$$((\text{OpsPerShardPerSec} * \text{ReadOpsPercent}) / \text{RF}) * (\text{AvgKeySize} + \text{ReadRequestOverheadBytes}) * \text{DisksPerMachine}$$

where *ReadRequestOverheadBytes* is a fixed constant overhead of 100 bytes.

The bytes sent out by the machine over the network as a result of the read operations has two underlying components:

1. The bytes sent out in direct response to application read requests and can be expressed as:

$$((\text{OpsPerShardPerSec} * \text{ReadOpsPercent}) / \text{RF}) * (\text{AvgKeySize} + \text{AvgValueSize}) * \text{DisksPerMachine}$$

2. The bytes sent out as replication traffic by the masters on the machine expressed as:

$$(\text{OpsPerShardPerSec} * (1 - \text{ReadOpsPercent}) * (\text{AvgKeySize} + \text{AvgValueSize}) * (\text{RF} - 1)) * \text{MastersOnMachine}$$

The sum of the above two values represents the total outbound traffic denoted by *SendBytesPerSec* in the spreadsheet.

The total inbound and outbound traffic must be comfortably within the NIC's capacity. The spreadsheet calculates the kind of network card, GigE or 10GigE, which is required to support the traffic.

Estimate total Shards and Machines

Having calculated the per shard capacity in terms of storage and throughput, the total number of shards and partitions can be estimated on the basis of the maximum storage and throughput required by the store as a whole using a simple extrapolation. The following inputs must be supplied for this calculation:

1. The maximum number of KV pairs that will stored in the initial store. This value is defined by the cell *MaxKVPairs*. This initial maximum value can be increased subsequently by using the topology transformation commands described in [Transform the Topology Candidate \(page 36\)](#).
2. The maximum read/write mixed operation throughput expressed as operations/sec for the entire store. The percentage of read operations in this mix must be the same as that supplied earlier in the *ReadOpsPercent* cell. This value is defined by the cell *MaxStorewideOpsPerSec*.

The required number of shards is first computed on the basis of storage requirements as below:

$$\text{MaxKVPairs} / \text{MaxKVPairsPerShard}$$

This value is calculated by the cell *StorageBasedShards*.

The required number of shards is then computed again based upon IO throughput requirements as below:

$$\text{MaxStorewideOpsPerSec} / \text{OpsPerShardPerSec}$$

This value is calculated by the cell named *OpsBasedShards*.

The maximum of the shards computed on the basis of storage and throughput above is sufficient to satisfy both the total storage and throughput requirements of the application.

The value is calculated by the cell *StoreShards*. To highlight the basis on which the choice was made, the smaller of the two values in *StorageBasedShards* or *OpsBasedShards* has its value crossed out.

Having determined the number of required shards, the number of required machines is calculated as:

$$\text{MAX}(\text{RF}, (\text{StoreShards} * \text{RF}) / \text{DisksPerMachine})$$

Number of Partitions

Every shard in the store must contain at least one partition, but it is best to configure the store so that each shard always contains more than one partition. The records in the KVStore are spread evenly across the KVStore partitions, and as a consequence they are also spread evenly across shards. The total number of partitions that the store should contain is determined when the store is initially created. This number is static and cannot be changed over the store's lifetime, so it is an important initial configuration parameter.

The number of partitions must be more than the largest number of shards the store will contain. It is possible to add shards to the store, and when you do, the store is re-balanced by moving partitions between shards (and with them, the data that they contain). Therefore, the total number of partitions is actually a permanent limit on the total number of shards your store is able to contain.

Note that there is some overhead in configuring an excessively large number of partitions. That said, it does no harm to select a partition value that provides plenty of room for growing the store. It is not unreasonable to select a partition number that is 10 times the maximum number of shards.

The number of partitions is calculated by the cell *StorePartitions*.

$$\text{StoreShards} * 10$$

Appendix E. Tuning

The default tuning parameters available for the Oracle NoSQL Database software should in general be acceptable for production systems, and so do not require any tuning. However, the underlying operating system will have default values for various kernel parameters which require modification in order to achieve the best possible performance for your store's installation.

This appendix identifies the kernel parameters and other system tuning that you should manage when installing a *production* store. By this, we mean any store whose performance is considered critical. Evaluation systems installed into a lab environment probably do not need this level of tuning unless you are using those systems to measure the store's performance.

Note

Oracle NoSQL Database is most frequently installed on Linux systems, and so that is what this appendix focuses on.

Turn off the swap

For best performance on a dedicated Oracle NoSQL Database server machine, turn off the swap on the machine. Oracle NoSQL Database processes are careful in their management of the memory they use to ensure that they do not exceed the RAM available on the machine.

The performance gains come from two sources:

1. The I/O overhead due to swap is eliminated. This is especially important if the disk normally used for swap also holds the store's log files used to persist data.
2. Reduces the CPU overhead associated with kswapd.

To turn off the swap, do not mount any swap partitions at boot time. You do this by eliminating all swap related mount entries from `/etc/fstab`. These are all the rows with the entry "swap" in their mount point (column 2) and file system type (column 3) entries.

You can verify that no swap space is being used by running the `free` command. Do this after the `/etc/fstab` has been modified and the machine has been rebooted:

```
-bash-4.1$ free -m
```

	total	used	free	shared	buffers	cached
Mem:	72695	72493	202	0	289	2390
-/+ buffers/cache:		69813	2882			
Swap:	0	0	0			

The Swap/total cell in the above table should read 0.

Linux Page Cache Tuning

Tune your page cache to permit the OS to write asynchronously to disk whenever possible. This allows background writes, which minimize the latency resulting from serial write operations

such as `fsync`. This also helps with write stalls which occur when the file system cache is full and needs to be flushed to disk to make room for new writes. We have observed significant speedups (15-20%) on insert-intensive benchmarks when these parameters are tuned as described below.

Place the following commands in `/etc/sysctl.conf`. Run

```
sysctl -p
```

to load the new settings so they can take effect without needing to reboot the machine.

```
# Set vm.dirty_background_bytes to 10MB to ensure that
# on a 40MB/sec hard disk a fsync never takes more than 250ms and takes
# just 125ms on average. The value of vm.dirty_background_bytes
# should be increased on faster SSDs or I/O subsystems with higher
# throughput. You should increase this setting by the same proportion
# as the relative increase in throughput. For example, for a typical SSD
# with a throughput of 160MB/sec, vm.dirty_background_bytes should be set
# to 40MB so fsync takes ~250ms. In this case, the value was increased by
# a factor of 4.
vm.dirty_background_bytes=10485760

# IO calls effectively become synchronous(waiting for the underlying
# device to complete them). This setting helps minimize the
# possibility of a write request stalling in JE while holding the
# write log latch.
vm.dirty_ratio=40

# Ensures that data does not hang around in memory longer than
# necessary. Given JE's append-only style of writing, there is
# typically little benefit from having an intermediate dirty page
# hanging around, because it is never going to be modified. By
# evicting the dirty page earlier, its associated memory is readily
# available for reading or writing new pages, should that become
# necessary.
vm.dirty_expire_centisecs=1000
```

Earlier versions of the Linux kernel may not support `vm.dirty_background_bytes`. On these older kernels you can use `vm.dirty_background_ratio` instead. Pick the ratio that gets you closest to 10MB. On some systems with a lot of memory this may not be possible due to the large granularity associated with this configuration knob. A further impediment is that a ratio of 5 is the effective minimum in some kernels.

```
vm.dirty_background_ratio=5
```

Use `sysctl -a` to verify that the parameters described here are set as expected.

OS User Limits

When running a large Oracle NoSQL Database store, the default OS limits may be insufficient. The following sections list limits that are worth reviewing.

File Descriptor Limits

Use `ulimit -n` to determine the maximum number of files that can be opened by a user. The number of open file descriptors may need to be increased if the defaults are too low. It's worth keeping in mind that each open network connection also consumes a file descriptor. Machines running clients as well as machines running RNs may need to increase this limit for large stores with 100s of nodes.

Add entries like the ones below in `/etc/security/limits.conf` to change the file descriptor limits:

```
$username soft nofile 10240
$username hard nofile 10240
```

where `$username` is the username under which the Oracle NoSQL Database software runs.

Note that machines hosting multiple replication nodes; that is, machines configured with a capacity > 1; will need larger limits than what is identified here.

Process and Thread Limits

Use `ulimit -u` to determine the maximum number of processes (threads are counted as processes under Linux) that the user is allowed to create. Machines running clients as well as machines running RNs may need to increase this limit to accommodate large numbers of concurrent requests.

Add entries like the ones below in `/etc/security/limits.conf` to change the thread limits:

```
$username soft nproc 8192
$username hard nproc 8192
```

where `$username` is the username under which the Oracle NoSQL Database software runs.

Note that machines hosting multiple replication nodes; that is, machines configured with a capacity > 1; will need larger limits than what is identified here.

Linux Network Configuration Settings

Before continuing, it is worth checking that the network interface card is configured as expected during the initial setup of each SN, because it is harder to debug these problems later when such configuration problems show up under load.

Use the following command to determine which network interface is being used to access a particular subnet on each host. This command is particularly useful for machines with multiple NICs:

```
$ ip addr ls to 192.168/16
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast
    state UP qlen 1000
    inet 192.168.1.19/24 brd 192.168.1.255 scope global eth0
```

Use the following command to get information about the configuration of the NIC:

```
$ ethtool -i eth2
driver: enic
```

```
version: 2.1.1.13
firmware-version: 2.0(2g)
bus-info: 0000:0b:00.0
```

Use the following command to get information about the NIC hardware:

```
$ lspci -v | grep "Ethernet controller"
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit
Ethernet Controller (rev 02)
```

Use the following command to get information about the network speed. Note that this command requires sudo:

```
$ sudo ethtool eth0 | grep Speed
Speed: 1000Mb/s
```

You may want to consider using 10 gigabit Ethernet, or other fast network implementations, to improve performance for large clusters.

Server Socket Backlog

The typical default maximum server socket backlog, typically set at 128, is too small for server style loads. It should be at least 1K for server applications and even a 10K value is not unreasonable for large stores.

Set the `net.core.somaxconn` property in `sysctl.conf` to modify this value.

Isolating HA Network Traffic

If the machine has multiple network interfaces, you can configure Oracle NoSQL Database to isolate HA replication traffic on one interface, while client request traffic uses another interface. Use the `-hahost` parameter to the `makebootconfig` command to specify the interface to be used by HA as in the example below:

```
java -Xmx256m -Xms256m \
-jar kvstore.jar makebootconfig -root /disk1/kvroot \
-host sn10.example.com -port 5000 -h.arange 5010,5020 \
-storagedir /disk2/kv -hahost sn10-ha.example.com
```

In this example, all client requests will use the interface associated with `sn10.example.com`, while HA traffic will use the interface associated with `sn10-ha.example.com`.

Receive Packet Steering

When multiple RNs are located on a machine with a single queue network device, enabling Receive Packet Steering (RPS) can help performance by distributing the CPU load associated with packet processing (soft interrupt handling) across multiple cores. Multi-queue NICs provide such support directly and do not need to have RPS enabled.

Note that this tuning advice is particularly appropriate for customers using Oracle Big Data Appliance.

You can determine whether a NIC is multi-queue by using the following command:

```
sudo ethtool -S eth0
```

A multi-queue NIC will have entries like this:

```
rx_queue_0_packets: 271623830
rx_queue_0_bytes: 186279293607
rx_queue_0_drops: 0
rx_queue_0_csum_err: 0
rx_queue_0_alloc_failed: 0
rx_queue_1_packets: 273350226
rx_queue_1_bytes: 188068352235
rx_queue_1_drops: 0
rx_queue_1_csum_err: 0
rx_queue_1_alloc_failed: 0
rx_queue_2_packets: 411500226
rx_queue_2_bytes: 206830029846
rx_queue_2_drops: 0
rx_queue_2_csum_err: 0
rx_queue_2_alloc_failed: 0
...
```

For a 32 core Big Data Appliance using Infiniband, use the following configuration to distribute receive packet processing across all 32 cores:

```
echo ffffffff > /sys/class/net/eth0/queues/rx-0/rps_cpus
```

where ffffffff is a bit mask selecting all 32 cores.

For more information on RPS please consult:

1. http://docs.oracle.com/cd/E37670_01/E37355/html/ol_about_uek.html
2. <http://lwn.net/Articles/361440/>

Managing the Off-heap Cache

Each Replication Node in the store divides the memory available to it between memory containing store objects, memory used by the host operation system (which includes the file system cache), and the in-memory cache used to contain frequently accessed store data. The amount of memory used by the cache is configurable using the `rnHeapPercent` parameter. This is expressed as a percentage of the total memory available to the Replication Node (which is, in turn, determined by the amount of memory made available to the Java VM). By default, 70% of the memory available to the Replication Node is reserved for the in-memory cache.

However, this can and probably will fill up. When that happens, objects are evicted from the cache based on a Least-Recently-Used (LRU) algorithm which guarantees that the most commonly accessed objects will remain in the cache.

It is possible to configure your Replication Node so that the in-memory cache is very large, and therefore is less likely to overflow. However, several drawbacks occur when the cache becomes too large. The most important of these is that Java Garbage Collection performance can decrease, which will have an adverse impact on your Replication Node's overall performance. *Therefore, it is in general a good idea to keep your heap size below 32 GB.* Doing so limits your in-memory cache size to about 22.4 GB.

Note

Be aware that Oracle NoSQL Database limits your maximum heap size to a default value of 32 GB so as to prevent accidentally creating an excessively large cache. This value is managed using the `rnHeapMaxMB`, which is described in greater detail later in this section.

When your Replication Node's heap is sized lower, it is possible to configure the system such that any memory unused by the heap will be used for the operating system and file system cache. A large file system cache has performance benefits, but it also has drawbacks:

1. There is a significant redundancy between the main cache and the file system cache because all data and Btree information that is logged (written) by the Replication Node appears in the file system and may also appear in the main cache.
2. It is not possible for dirty Btree information to be placed in the file system cache without logging it. This logging may be otherwise unnecessary, and the logging creates additional work for internal cleaner threads.

To avoid the problems caused by excessively large in-memory and file system caches, your Replication Node is by default configured to use an *off-heap cache*. The off-heap cache is used to hold record data and Btree nodes when these are evicted from the "main cache" because it overflows. When the off-heap cache overflows, eviction occurs according to the same LRU algorithm used by the main cache.

Note

You should engage in performance testing before modifying the caches in use by your production store.

Configuring the Off-heap Cache

You do not directly control the amount of memory available to the off-heap cache. Instead, you make memory available to it mainly by limiting the amount of memory available to the operating system. You might also need to control the size of the Java heap, which in turn controls the size of the in-memory cache. Any Replication Node memory that is left over once the heap and operating system requirements are met is used for the off-heap cache. If no memory is left over, the off-heap cache is not used. This is the only way to turn off the off-heap cache.

The parameters you use to (indirectly) configure the off-heap cache are:

1. `systemPercent`

This defines the percentage of memory available to the Storage Node that is available for operating system use *after* the heap requirement is subtracted. By default, this value is 10%. Configuring this value to a number that is greater than 10% but less than 100% might leave room for the off-heap cache (depending on the memory on your Storage Node and the value chosen for this parameter). If room is available for the off-heap cache, it will be turned on.

For most production systems, if you are using the off-heap cache, then the default value of 10% for this parameter should be sufficient.

2. rnHeapMaxMB

This is the maximum amount of memory available for the Java heap. (The heap is where the in-memory cache is contained.) The size of your heap will be the lesser of this number, or the size arrived at using the rnHeapPercent parameter value:

$$\text{total SN memory} * \text{rnHeapPercent} = \text{Heap Size}$$

rnHeapPercent is by default 85%. So if your Storage Node has 32GB memory, then the heap size will be $32 * 0.85 = 27.2$ GB. However, if you set your rnHeapMaxMB to 25,600 (25*1024), then your heap size will be 25GB instead.

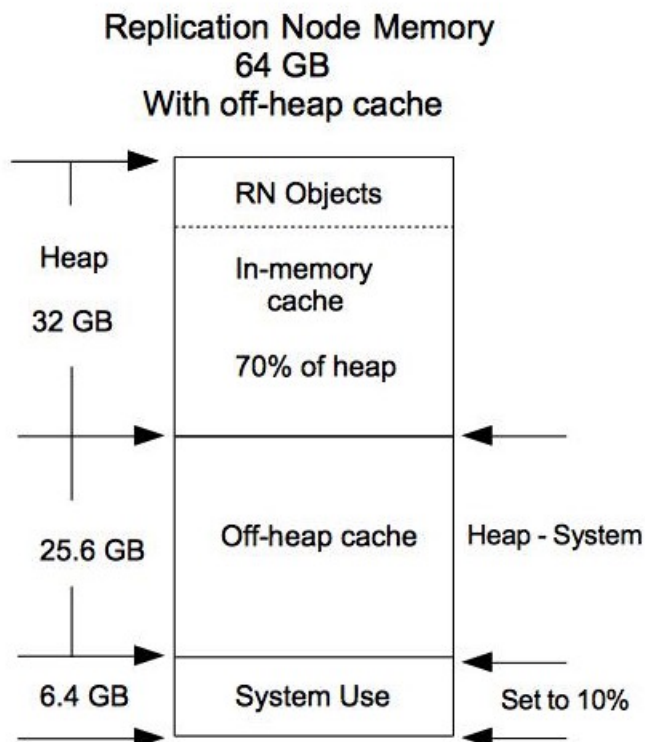
Remember that the heap size is not the same as the in-memory cache size. The in-memory cache size is expressed as a percentage of the heap size. By default, this is 70% (configurable using the rnCachePercent parameter). So if your heap size is 27.2 GB, then your in-memory cache size ends up being 19.04 GB ($27.2 * 0.7$).

Note

Regardless of the values provided to the parameters described here, and the actual memory available for the heap, your heap size is limited to a maximum size of 32 GB.

For example, if your Storage Node has 64GB of memory, and just one Replication Node, then by default:

- The heap size is 32GB. ($64 * .85 = 54.4$ which is greater than the 32GB maximum.)
- The in-memory cache size is 22.4 GB ($32 * 0.7$).
- A system memory size of 6.4 GB. ($64 * .1$)
- An off-heap cache size of 25.6 GB. This is the amount of memory left over after the heap and system requirements have been met.

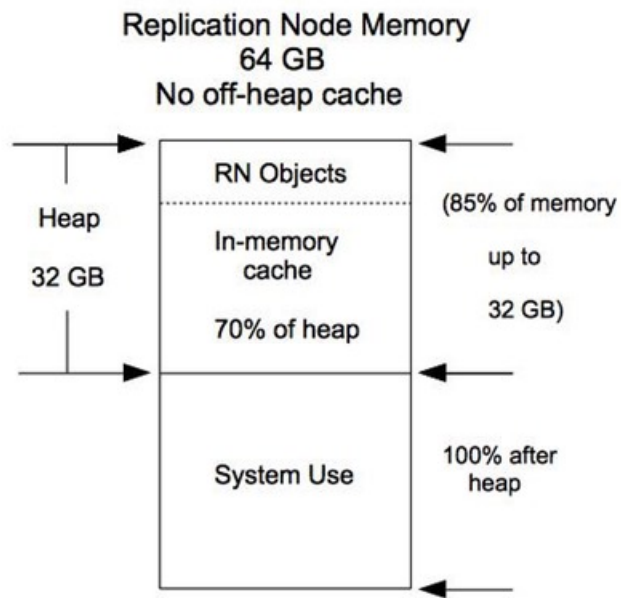


If you want to eliminate the off-heap cache, then set system memory to 100%. Do this for each Storage Node in your store. Be aware that doing this causes your Storage Node to restart:

```
kv-> change-policy -params systemPercent=100 change-parameters \
-svc service sn1 -wait -params systemPercent=100
Executed plan 5, waiting for completion...
Plan 5 ended successfully
kv->
```

This yields:

- A heap size of 32 GB and in-memory cache size of 22.4 GB. Nothing has changed from the default configuration.
- The system memory is 32 GB. System memory is 100% of what is left over when the heap is taken away. 64 GB (total available) - 32 GB (heap size) = 32 GB for the operating system and file system cache.



Appendix F. Solid State Drives (SSDs)

If you are planning on using Solid State Drives (SSDs) for your Oracle NoSQL Database deployment, a special consideration should be taken. Because of how SSDs work, I/O latency can become an issue with SSDs over time. Correct configuration and use of `trim` can help minimize these latency issues.

Trim requirements

In general, for TRIM to be effective, the following requirements must be met:

- The SSD itself must support trim.
- Linux-kernel 2.6.33 or later.
- Filesystem ext4 (ext3 does not support trim).

Enabling Trim

The `trim` support must be explicitly enabled for the ext4 file system. You should mount the file system with trim enabled.

Appendix G. Diagnostics Utility

In order to catch configuration errors early, you can use this tool when troubleshooting your KVStore. Also, you can use this tool to package important information and files to send them to Oracle Support, for example.

The usage for the utility is:

```
>java -jar KVHOME/lib/kvstore.jar diagnostics {setup | collect} [args]
```

Setting up the tool

You should first run the `diagnostics setup` command in order to setup the tool. This command generates the configuration file `sn-target-list` with the Storage Node target list, which contains the IP/hostname, registry ports, and root directory of SNAs in the remote machines.

The usage of this command is:

```
diagnostics setup {-add |  
-list |  
-delete |  
-clear} [args]
```

where:

- -add

Adds the specified information of each SNA to the `sn-target-list`. The usage is:

```
setup -add -store <store name>  
-sn <SN name>  
-host <host>  
-rootdir <kvroot directory>  
[-sshusername <SSH username>]  
[-configdir <directory of configuration>]
```

In the `sn-target-list`, the SNA information has the following format:

```
<store name>|<sn name>|<SSH username@host>|<root directory>
```

For example:

```
mystore|sn3|lroot@localhost|/scratch/tests/kvroot
```

Note

You can also create and edit the `sn-target-list` manually in your preferred text editor to add or delete any SNA information.

- -list

Lists and tests the SNAs information of the `sn-target-list`. The usage is:

```
setup -list [-configdir <configuration file directory>]
           [-sshusername <SSH username>]
```

This command checks if:

- The host name is reachable or not.
- The root directory exists or not.
- `-delete`

Specified to delete the information of the specified SNA from the `sn-target-list`.

The usage of this command is:

```
diagnostics setup -delete
[-store <store name>]
[-sn <SN name>]
[-host <host>]
[-rootdir kvroot directory>]
[-sshusername <SSH username>]
[-configdir <configuration file directory>]
```

- `-clear`

Specified to clear all the SNA information in the `sn-target-list`.

The usage of this command is:

```
diagnostics setup -clear [-configdir <configuration file directory>]
```

- `-configdir`

Optionally specified to change the default directory where the `sn-target-list` file is saved. If the flag is not specified, the default directory is the working directory.

Packaging information and files

After completing the `diagnostics setup`, you can use the `diagnostics collect` tool to package important information and files to be able to send them to Oracle Support, for example.

The usage of this command is:

```
diagnostics collect -logfiles
[-host <host name of a SN in topology>]
[-port <registry port of a SN in topology>]
[-sshusername <SSH username>]
[-username <store username>]
[-security <security-file-path>]
```

```
[ -configdir <location of Storage Node target file> ]  
[ -savedir <destination directory for log files> ]  
[ -nocompress ]
```

where:

- -host

Specifies the host of a Storage Node. If specified, it detects a running topology in order to update the `sn-target-list` without having to run `diagnostics setup` first. It needs to be specified with `-port`.

- -port

Specifies the host of a Storage Node. If specified, it detects a running topology in order to update the `sn-target-list` without having to run `diagnostics setup` first. It needs to be specified with `-host`.

- -sshusername

Specifies a SSH username to log on as in a Storage Node.

- -username

Specifies a username to log on as in a secure deployment.

- -security

In a secured deployment, specifies a path to the security file. If not specified in a secure store, updating the `sn-target-list` will fail.

- -configdir

Specifies the directory which contains the `sn-target-list`. If the flag is not specified, the default directory is the working directory.

- -logfiles

Specified to gather log files of KVStore and pack them up into a compressed file. The log files are all files in the root directory of SNAs(excluding database files `jdb` files). Available disk space in all the hosting machines and the client machine is required. If available disk space is not enough, an error message is prompted. Log files are helpful to analyze some sophisticated issues.

- -nocompress

Specifies that log files should be copied directly instead of being compressed. If the log files size is large, copying can take a while. You should use `-nocompress` if the remote servers do not have an unzip tool or if compress mode encounters errors.

- -savedir

Optionally used to specify the path of the directory to contain all the log files. If the flag is not specified, the default directory is the working directory.

Verifying Storage Node configuration

You can use the `diagnostics verify` tool to verify the configuration of the specified Storage Nodes. You can also check if the configuration of each Storage Node is consistent with other members of the cluster.

The usage of this command is:

```
diagnostics verify { -checkLocal | -checkMulti }  
[-host <host name of a SN in topology>]  
[-port <registry port of a SN in topology>]  
[-sshusername <SSH username>]  
[-username <store username>]  
[-security <security-file-path>]  
[-configdir <location of Storage Node target file>]
```

where:

- `-checkLocal`

If specified, verifies the configuration of the specified Storage Nodes.

- `-checkMulti`

If specified, verifies that the configuration of each Storage Node is consistent with other members of the cluster.

- `-host`

Specifies the host of a Storage Node. If specified, it detects a running topology in order to update the `sn-target-list` without having to run `diagnostics setup` first. It needs to be specified with `-port`.

- `-port`

Specifies the host of a Storage Node. If specified, it detects a running topology in order to update the `sn-target-list` without having to run `diagnostics setup` first. It needs to be specified with `-host`.

- `-sshusername`

Specifies a SSH username to log on as in a Storage Node.

- `-username`

Specifies a username to log on as in a secure deployment.

- `-security`

In a secured deployment, specifies a path to the security file. If not specified in a secure store, updating the `sn-target-list` will fail.

- `-configdir`

Specifies the directory which contains the `sn-target-list`. If the flag is not specified, the default directory is the working directory.

Key Distribution Statistics Utility

If enabled, your KVStore automatically gathers key distribution statistics.

Oracle NoSQL Database uses four system tables to store key distribution data. System tables are internally managed and maintained by Oracle NoSQL Database. They are read-only when security is enabled on the store. Regardless of security, the schema for system tables is immutable. The name of system tables is defined with the prefix `SYS$`. You are not allowed to create any other table name using this reserved prefix.

The four system tables used to store key distribution data are:

- `SYS$IndexStatsLease`
- `SYS$PartitionStatsLease`
- `SYS$TableStatsIndex`
- `SYS$TableStatsPartition`

`SYS$TableStatsPartition` stores the distribution of primary keys and table `SYS$TableStatsIndex` stores the distribution of index keys. All four tables are forbidden to modify, delete and insert.

To enable statistics gathering you need to set the `rnStatisticsEnabled` parameter to true:

```
plan change-parameters -wait -all-rns  
-params "rnStatisticsEnabled=true"
```

Then, you can query any of the four tables to get key distribution data or review the gathering process.

To modify the behavior of the utility, use the following parameters:

- `rnStatisticsEnabled`

Used to enable or disable the statistics gathering. The default value is true, which enables statistics gathering.

- `rnStatisticsGatherInterval`

Specifies the interval time between updates of table level statistics. The default value is 24 hours.

- `rnStatisticsLeaseDuration`

Specifies the duration of a lease. A Replication Node must hold a lease associated with a partition or a shard-index before it can update the associated statistics. The default value is 10 minutes.

- `rnStatisticsLowActivePeriod`

Specifies the period for which activity must be below the threshold defined by `rnStatisticsRequestThreshold` before statistics gathering activity is initiated. The default value is 2 minutes.

- `rnStatisticsRequestThreshold`

Specifies the threshold number of requests used to initiate statistics gathering. Statistics gathering is initiated if the sampled number of requests is below this threshold over the period defined by `rnStatisticsLowActivePeriod`. The default value is 2 requests.

Appendix H. Third Party Licenses

All of the third party licenses used by Oracle NoSQL Database are described in the LICENSE.txt file, which you can find in your KVHOME directory.