HP Network Automation Software

For the Windows®, Linux, and Solaris operating systems

Software Version: 9.20 Patch 1 (9.20.01)

Disaster Recovery Configuration Guide

Document Release Date: August 2012
Software Release Date: August 2012

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

Intel and Intel Itanium are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, after product installation see the `$NA_HOME/server/license` directory (or the `%NA_HOME%\server\license` directory on Windows systems) on the NA application server.

Acknowledgements

This product includes software developed by the Apache Software Foundation.
(http://www.apache.org)

Parts of this software Copyright © 2003-2008 Enterprise Distributed Technologies Ltd. All Rights Reserved.
(http://www.enterprisedt.com)

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 NA Disaster Recovery Concepts

This guide describes the recommended disaster recovery architecture for HP Network Automation Software (NA). This guide describes the procedure for configuring NA for disaster recovery. It also describes the procedures for switching over to the disaster recovery location and switching back from the disaster recovery location.

What is Disaster Recovery?

Disaster recovery planning provides for minimizing the business disruption should a significant event affect an entire data center. Possible uses for the disaster recovery configuration include the following:

- Unexpected unavailability of a data center due to natural disaster or acts of war. In this case, any lag in data replication results in lost data at the disaster recovery location.
- Anticipated unavailability of a data center due to natural events (for example, a forecasted hurricane), facilities maintenance, or data center movement. In this case, it might be possible to avoid data loss by waiting until the NA database in the disaster recovery location is completely synchronized with the NA database in the primary location before switching over to the disaster recovery location.

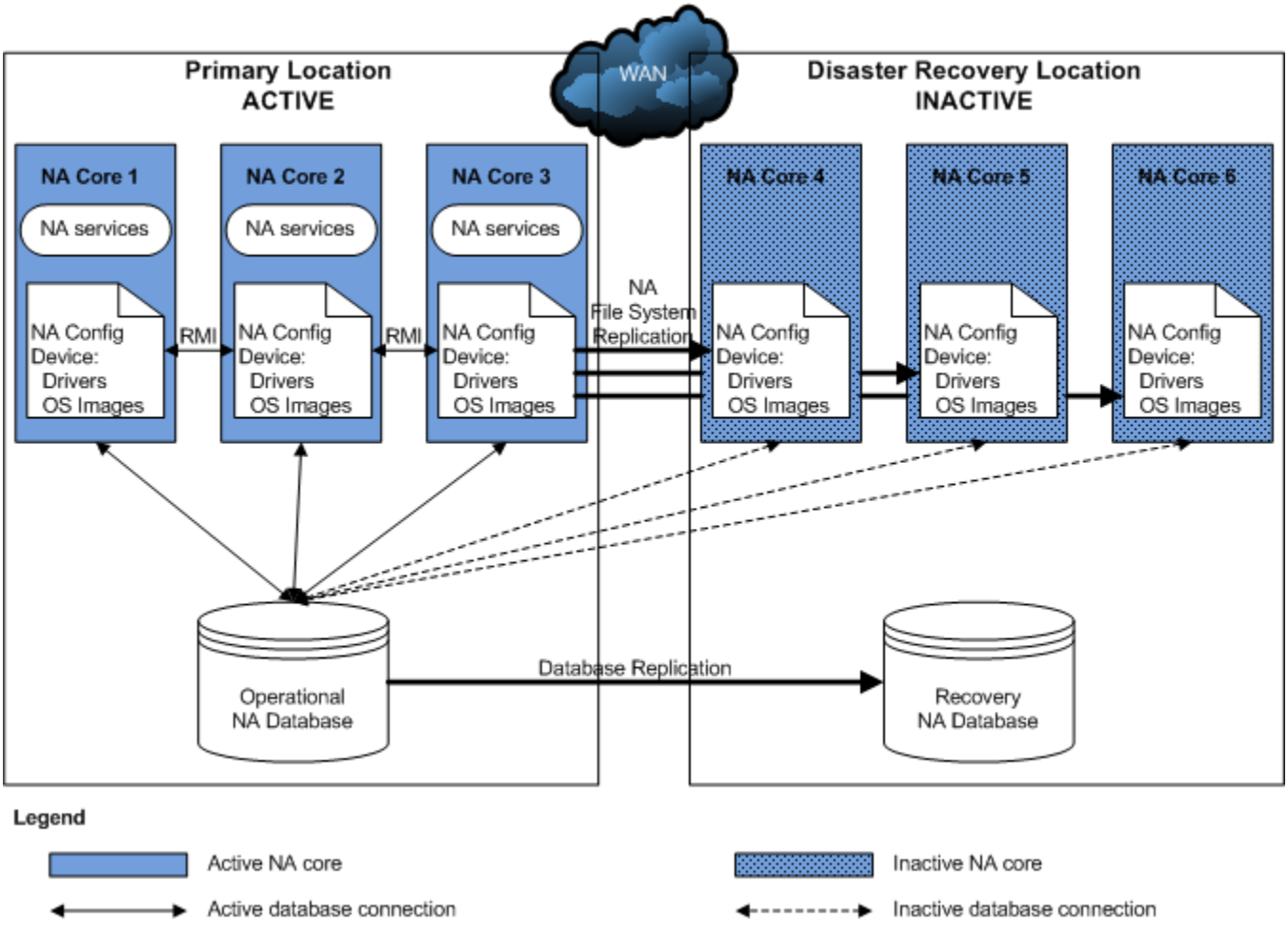
Disaster recovery is different from high availability in that with disaster recovery, down time is expected. Generally, disaster recovery configuration includes both of the following processes:

1. Setting up redundant hardware and software at a disaster recovery location that is remote to the primary, operational location.
2. Providing for one-way replication of application data to the disaster recovery location.

Disaster Recovery Architecture

For NA, disaster recovery configuration involves duplicating the NA environment running in a data center in the primary location to a remote data center in the disaster recovery location. Figure 1 shows this duplication for a three NA core Horizontal Scalability environment. (An NA core is a physical or virtual server on which the NA services and supporting configuration are installed.) Horizontal Scalability provides load sharing, high availability, and fault tolerance. The disaster recovery configuration provides continuity after a disaster.

Figure 1 Example NA Disaster Recovery Architecture



Note the following:

- Each location includes one NA database. This database could be implemented as a standalone database server or as a database cluster using a technology such as Oracle Real Application Clusters (RAC).
- At any point in time, only one NA database is actively used by the NA cores. The second database must be running to receive database updates; however, no NA cores connect to the second database.

  The recommended NA disaster recovery scenario includes one-way database replication.
- One to five active NA cores connect to the operational NA database using Horizontal Scalability. The server for each NA core has a unique IP address and hostname, so the switchover and switchback procedures include updating any configuration that connects to the NA servers. For best performance of the overall solution, it is recommended that each NA server be located in the same data center as the database server to which it is most likely to connect.

  When multiple NA cores are active simultaneously, Java remote method invocation (RMI) calls synchronize the NA-specific file systems across the active NA cores. RMI calls also manage schedules for running tasks across the active NA cores.

- During disaster recovery configuration, all NA cores connect to the operational NA database. The NA cores in the disaster recovery location are then set to the inactive state. While an NA core is inactive, the following conditions apply:
  - That NA core does not run tasks.
  - Users should *not* log on to the NA console.
  - Users might connect to the NA command-line interface through telnet or SSH *only* for the purpose of setting the NA core state during switchover or switchback.
- The maximum number of active NA cores in a Horizontal Scalability environment is five. The maximum number of active and inactive NA cores in a Horizontal Scalability environment is nine, which means that the maximum number of NA cores in a disaster recovery scenario is five active NA cores at the primary location and four inactive NA cores at the disaster recovery location.

  During disaster recovery configuration, all nine NA cores might be active at one time; however, no device management occurs on the NA cores in the disaster recovery location.
- If the primary location includes one or more core gateways, the disaster recovery location must include at least one core gateway. The disaster recovery location could include up to one core gateway per NA core. The number of core gateways in the disaster recovery location need not match the number of core gateways in the primary location.
- This guide assumes that satellite gateways are located at facilities other than the primary and disaster recovery locations; therefore, it does not discuss disaster recovery configuration for satellite gateways.
- As of NA 9.20 patch 1, NA task management in the Horizontal Scalability environment includes the following behavior:
  - If NA tasks for a given device are bound to only one NA core (the default behavior; Horizontal Scalability topologies 1, 3, or 4), when an NA administrator reassigns the sites from one NA core to another NA core, NA moves the tasks associated with that site to the receiving NA core.
  - If all NA tasks for all devices are distributed in round-robin fashion across all NA cores (Horizontal Scalability topology 2), when an NA administrator sets an NA core to the inactive state, all tasks scheduled to run on that NA core are distributed to the remaining active NA cores.
- This disaster recovery configuration is licensed as follows:
  - One production license for the total number of managed devices for one NA core in the primary location.
  - One non-production license for the total number of managed devices for *each* additional NA core in the primary and disaster recovery locations.
  - One production license for each core gateway in the primary location.
  - One non-production license for each core gateway in the disaster recovery location.

2 NA Disaster Recovery Initial Setup

You can configure HP Network Automation Software (NA) in a disaster recovery any time after NA is configured and running satisfactorily in the primary location. The approach described in this document requires NA Horizontal Scalability functionality. For information about the supported database versions for NA Horizontal Scalability, see “Databases for Horizontal Scalability” in the *NA Support Matrix*.

This guide assumes NA database replication in an operation–recovery configuration. The recovery database server contains a copy of the NA database. The replication technology monitors the database transactions on the operational database and periodically replicates them to the recovery database. This configuration requires that the recovery database server be powered on and running continuously. Select a database replication technology appropriate to your database type and business needs. For information about the tested database replication technologies, see “Disaster Recovery” in the *NA Support Matrix*.

Setting up NA for Disaster Recovery

To perform initial setup of an NA disaster recovery configuration, follow this general outline:

- Task 1: Prepare the Primary Location for Disaster Recovery Configuration on page 11
- Task 2: Configure Database Replication on page 13
- Task 3: Install and Configure NA in the Disaster Recovery Location on page 13
- Task 4: Finish the Disaster Recovery Configuration on page 15

Task 1: Prepare the Primary Location for Disaster Recovery Configuration

1 In the primary location, start with a running NA deployment. This deployment can be a single NA core or a Horizontal Scalability environment containing up to five NA cores. This deployment can also include NA satellite functionality.

NA must be version 9.20 patch 1 or later.

For information about installing a single NA core, see the *NA Installation and Upgrade Guide*.

For information about adding NA cores to create a Horizontal Scalability environment, see the *NA Horizontal Scalability Guide*.

2 *Optional*. Consider the risk that if the primary location is not accessible during switchover to the disaster recovery location, the NA cores in the primary location cannot be deactivated. In this case, two NA cores (one each in the primary and disaster recovery locations) might run the same task. To mitigate this risk, on each NA server in the primary location, disable automatic starting of the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, click **Properties**, and then set Startup Type to **Disabled**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *Linux*:

  ```
  mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
  ```
- *Solaris*:

  ```
  mv /etc/rc2.d/S99truecontrol /etc/S99truecontrol
  ```

3 Prepare to stop NA in the primary location.

a Notify users to log out.

b Log on to the NA console for one of the NA cores in the primary location.

c Pause tasks scheduled to start during the disaster recovery configuration process (until Task 4, step 1 on page 15). Include time for the currently running tasks to complete. Also include time for database synchronization. For example:

- On the Search for Task page (**Reports > Search For > Tasks**), for the Schedule Date field, set since to **`Now`** and until to **`4 hours later`**.
- On the Task Search Results page, pause each listed task.

d On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

If any critical tasks are running, wait for them to complete before continuing with step 4, next.

4 Stop all NA services on all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  ```
  /etc/init.d/truecontrol stop
  ```

Task 2: Configure Database Replication

1. If the NA database in the primary location, was created for the SYSTEM user (Oracle) or the SA user (SQL Server), move the NA database to a custom user with the privileges described in the *NA Installation and Upgrade Guide*. Do the following:
   a. Create a new tablespace or database instance dedicated to NA on the database server in the primary location.
   b. Use database tools to copy the NA schema to the new tablespace or database instance.
2. Use database tools to create a copy of the operational NA database in the disaster recovery location.

   Note the following:

   - The NA database user in the disaster recovery location must have the same name and permissions as the NA database user in the primary location.
   - Copy the NA schema tables only.
   - For Oracle or Oracle RAC, the SID or service name should be different between the two database servers.

     One SID *cannot* be a subset of the other SID, for example NARp and NARpBU. Instead, use SIDs that stand alone, for example NARp1 and NARp2.
   - For Microsoft SQL Server, the database name should be different between the two database servers.

   For example, you might follow this process:

   a. Install the database software.
   b. Create a database user with the same name and permissions as the NA database user for the operational database in the primary location.
   c. Export the NA database from the operational database in the primary location.
   d. Import the NA database to the recovery database in the disaster recovery location.
3. Configure one-way database replication from the operational database in the primary location to the recovery database in the disaster recovery location.

   Use a database replication technology appropriate to your database type and business needs. Follow the documentation for that technology.

Task 3: Install and Configure NA in the Disaster Recovery Location

1. In the disaster recovery location, install the NA cores as additional NA cores connected (through Horizontal Scalability) to the operational database in the primary location.

   For information, see “Adding Additional NA Cores” in the *NA Horizontal Scalability Guide* for NA 9.20 patch 1 or later.

If you reached this step from a switchback procedure, complete the script edits to account for having removed one or more NA cores from the Horizontal Scalability environment.

Connecting the NA cores in the disaster recovery location to the NA database in the primary location ensures that the databases remain synchronized. These NA cores will be stopped later in this procedure.

This use of Horizontal Scalability over the WAN is for disaster recovery configuration only. Daily use of Horizontal Scalability over the WAN is not supported.

2 *Optional*. Perform any NA core-specific tuning. Restart the NA services as needed.

3 *Optional*. Configure the managed devices to send syslog messages to one NA core in the disaster recovery location.

4 If the primary location includes NA Satellite functionality, do the following:

a In the disaster recovery location install one or more core gateways.

Install at least one core gateway in the disaster recovery location to continue communication with the existing gateway mesh. Optionally install additional core gateways, up to one core gateway per NA core. During installation, configure each core gateway in the disaster recovery location as follows:

— Use the same Gateway Crypto Data file as for the core gateways in the primary location.

— Assign the same realm name, typically Default Realm, to each core gateway.

For information, see the *NA Satellite Guide*.

b For each satellite in the gateway mesh, update the satellite configuration to enable communication with a core gateway in the disaster recovery location.

Edit the remote gateway configuration file:

`<gateway_install_dir>/opswgw-<gateway_name>/opswgw.properties`
(The default value of `<gateway_install_dir>` is `/etc/opt/opsware`.)

In the remote gateway configuration file, do the following:

— Add an `opswgw.TunnelSrc` entry that points to a core gateway in the disaster recovery location.

Configure this secondary connection with a higher route cost so it is used only when the core gateway in the primary location is unavailable. For example:

```
opswgw.TunnelSrc=<core_gateway1_IP>:2001:100:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem
```

```
opswgw.TunnelSrc=<core_gateway2_IP>:2001:200:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem
```

— Update the `opswgw.EgressFilter` entry to match the following:

```
opswgw.EgressFilter=tcp:*:443:127.0.0.1:*,tcp:*:22:NAS:,tcp:
*:23:NAS:,tcp:*:513:NAS:,tcp:*:443:NAS:,tcp:*:80:NAS:
```

c Restart each remote core gateway.

With this configuration, no additional work is needed to enable the core gateways during switchover or switchback.

This guide expects that the satellites are remote to the primary and disaster recovery locations. If necessary, set up additional satellites in the gateway mesh for redundancy.

5 Deactivate the NA cores in the disaster recovery location.

a Connect as an NA administrator to the NA proxy on one of the NA cores in the disaster recovery location.

b Run the following command:

```
list core
```

c From the `list core` command output, determine the core IDs of the new NA cores, and then run the following command for each core ID:

```
core status -status standby -coreid <coreid>
```

6 Stop all NA services on all NA cores in the disaster recovery location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

Task 4: Finish the Disaster Recovery Configuration

1 In the primary location, start all NA services on all active NA cores.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

2 Resume the tasks that were paused in Task 1, step 3 on page 12.

a Log on to the NA console for one of the NA cores in the primary location.

b On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **`Paused`**.

c On the Task Search Results page, resume each listed task.

3 Notify users to resume use of the NA console on the NA cores in the primary location.

4 Configure replication of the NA file system from one of the active NA cores to the inactive NA cores (or an intermediate server) as described in Files to Synchronize Across NA Cores on page 16.

5 *Optional*. If you chose to synchronize the NA files to an intermediate server, to conserve resources, power down the NA servers in the disaster recovery location.

6 *Optional*. If the database replication technology supports reverse replication from the database in the disaster recovery location to the database in the primary location, prepare for, but *do not enable*, reverse replication.

Files to Synchronize Across NA Cores

While most NA data is stored in the NA database, some files on the NA core support the NA console and NA functions. A complete disaster recovery scenario must include replication of these files. Table 1 lists the files to consider for replication among the NA cores.

Configure file replication using tools appropriate to your environment. Maintain file ownership and permissions during replication.

Set up a regularly scheduled server-level job to copy the files listed in Table 1 from one of the active NA cores (in the primary location) to all of the inactive NA cores in the disaster recovery location. This copy could be initiated by an active NA core (push) or by each inactive NA core (pull).

Alternatively, the script might copy files from an active NA core to an intermediate server. This approach is useful if you want to leave the inactive NA cores powered off until they are needed. In this case, the procedure for switching over to the disaster recovery location includes copying the files from the intermediate server to each inactive NA core.

Example file replication script

For example, the following script pulls files from an active NA core. It uses the `rsync` command, which compares the versions of a file on each server and copies only those files that have changed. This script would be located on each inactive NA core. It copies files from the active NA core whose core ID is `core1`.

```
C1=core1
rsync -avz $C1:/opt/NA/jre/site_options.rcx /opt/NA/jre
rsync -avz $C1:/opt/NA/jre/logging.rcx /opt/NA/jre
rsync -avz $C1:/opt/NA/jre/adjustable_options.rcx /opt/NA/jre
rsync -avz $C1:/opt/NA/jre/distribution.rcx /opt/NA/jre
rsync -avz $C1:/opt/NA/jre/securityfilter_additional_init.rcx /opt/NA/
jre
rsync -avz $C1:/opt/NA/server/lib/drivers/ /opt/NA/server/lib/drivers
rsync -avz $C1:/opt/NA/server/images/ /opt/NA/server/images
```

Table 1 Files to Synchronize Across NA Cores

Category	Files
RCX files, which are located in the following directory: • *Windows*: `%NA_HOME%/jre` • *UNIX*: `$NA_HOME/jre`	Specifically, at least the following files: • `site_options.rcx` (NA server behavior) • `logging.rcx` (NA logging levels) • `adjustable_options.rcx` (Customer-specified configuration options) • `distribution.rcx` (Distribution settings) • `securityfilter_additional_init.rcx` (Customer-specified filters for URL strings) Also include other RCX files that have been customized. **NOTE**: Do *not* include the `appserver.rcx` file, which contains paths to the local system. If this file has been modified, copy the changed blocks to the `adjustable_options.rcx` file for synchronization across all NA cores.
HP-developed device drivers (`*.rdp`), which are located in a directory as specified by the `driver/dir` option in the `site_options.rcx` file, typically: • *Windows*: `%NA_HOME%\server\lib\drivers` • *UNIX*: `$NA_HOME/server/lib/drivers`	Synchronize all files in the `drivers` directory.
Device drivers developed outside of HP, which are located in a directory as specified by the `driver/extension/dir` option in the `site_options.rcx` file.	Synchronize all files in the identified directory.
Device operating system images, which are located in a directory as specified by the `deploy/repository/root` option in the `site_options.rcx` file, typically: • *Windows*: `%NA_HOME%\server\images` • *UNIX*: `$NA_HOME/server/images`	Synchronize all files in the `images` directory.

Verifying the Disaster Recovery Configuration

To verify the initial setup of an NA disaster recovery configuration, the database administrator (DBA) can follow this general outline:

1. Verify that database replication works correctly.

   Use database tools to confirm that the numbers of tables and records in the two NA databases are the same.

2. Check the database replication logs.

   - Are there any replication errors?
   - Is there a problem with any of the NA tables?
   - Are there errors regarding the primary key?

3. Examine the replication lag, which is the time difference between when a transaction is recorded in the primary and disaster recovery database.

   If the lag is unacceptably large, tune database replication. For information, see the documentation for your database replication technology.

   For Oracle GoldenGate, consider tuning the `TCPBUFSIZE`, `TCPFLUSHBYTES`, and `COMPRESS` arguments to the `RMTHOST` parameter.

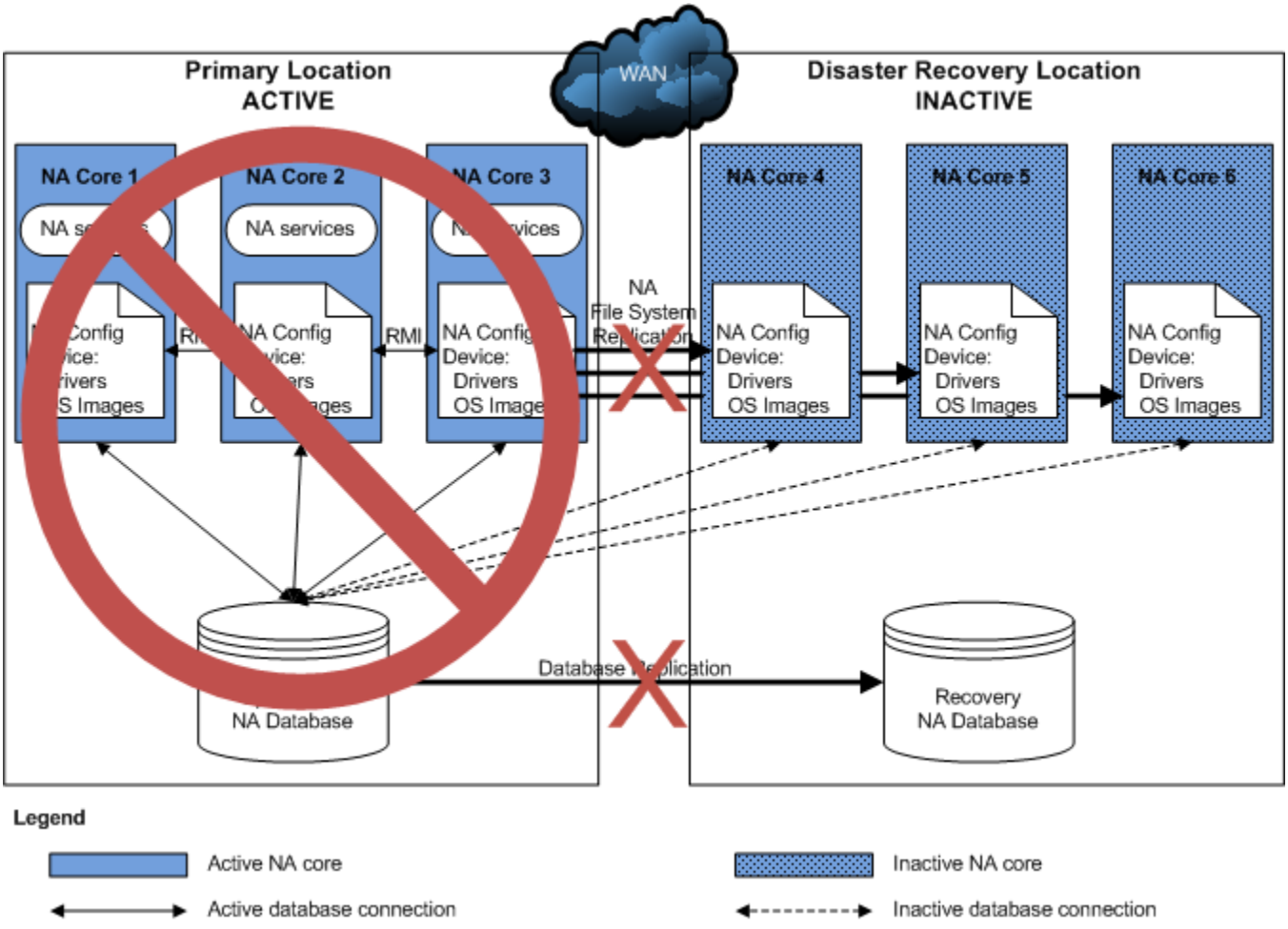
4. Set up a schedule for performing regular trimming of the replication log files.
5. Verify NA file system replication by comparing the file sizes and timestamps in the primary and disaster recovery locations.

3 Switchover

When the primary location becomes unavailable, an administrator can follow the procedure described in this chapter to switch use of HP Network Automation Software (NA) over to the disaster recovery location. In the case of an unplanned disaster event, NA will be unavailable until switchover is complete and the most recent database updates might be lost. In the case of a planned unavailability, replication can be fully completed before switchover begins, and NA downtime can be very short with no data loss.

Figure 2 shows the state of the disaster recovery configuration immediately after an event has occurred. The primary location is unavailable, and the disaster recovery has not yet gone live.

Figure 2 After a Disaster Event, Before Switchover



If the primary location is *not* accessible, to switch over from the primary location to the disaster recovery location, complete the following tasks in order:

- Task 1: Plan to Disable NA in the Primary Location on page 20
- Task 3: Enable Use of the Database in the Disaster Recovery Location on page 22
- Task 4: Enable NA in the Disaster Recovery Location on page 23
- Task 5: Finish Switchover on page 25

If the primary location is accessible, to switch over from the primary location to the disaster recovery location, complete the following tasks in order:

- Task 2: Disable NA in the Primary Location on page 20
- Task 3: Enable Use of the Database in the Disaster Recovery Location on page 22
- Task 4: Enable NA in the Disaster Recovery Location on page 23
- Task 5: Finish Switchover on page 25

Task 1: Plan to Disable NA in the Primary Location

If the primary location is not currently accessible, make plans to disable NA functionality in the primary location as soon as that location becomes accessible. These plans might include any or all of the following:

- Disabling automatic starting of the NA services (as described in step on page 12)
- Physical changes to the NA server (for example, disconnecting the power source or the network cable)

Continue with Task 3 on page 22.

Task 2: Disable NA in the Primary Location

If the primary location is accessible, disable NA by completing the steps in this task. If you anticipate losing connectivity to the primary location, complete as many of these steps as possible while connectivity remains. If you are unable to complete this task before losing connectivity to the primary location, also consider the information in Task 1: Plan to Disable NA in the Primary Location.

1 On each NA server in the primary location, disable automatic starting of the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, click **Properties**, and then set Startup Type to **Disabled**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *Linux*:

```
mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
```

- *Solaris*:

```
mv /etc/rc2.d/S99truecontrol /etc/S99truecontrol
```

2 Prepare to stop NA in the primary location.

a Notify users to log out.

b Log on to the NA console for one of the NA cores in the primary location.

c Pause tasks scheduled to start during the switchover process (until Task 4, step 5 on page 24). Include time for the currently running tasks to complete. For example:

— On the Search for Task page (**Reports > Search For > Tasks**), for the Schedule Date field, set since to **`Now`** and until to **`2 hours later`**.

— On the Task Search Results page, pause each listed task.

d On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

If any critical tasks are running, wait for them to complete before continuing with step 3, next.

3 Stop all NA services on all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

Ensure that the NA services on the NA cores in the primary location remain stopped until directed otherwise in the switchback procedure.

4 Wait for NA file system replication from the primary location to complete.

Verify completeness by comparing the file sizes and timestamps in the primary and disaster recovery locations.

5 Wait for all database updates to replicate from the database in the primary location to the database in the disaster recovery location.

6 On the primary location database server, disable database replication to the database in the disaster recovery location.

Task 3: Enable Use of the Database in the Disaster Recovery Location

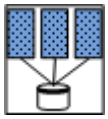
1. On the disaster recovery location database server, disable database replication from the database in the primary location.

2. *Optional*. In the case of a planned switchover, if the database replication technology supports reverse replication from the database in the disaster recovery location to the database in the primary location, enable reverse replication.

If the down time of the primary location is expected to be less that the time in which the database transaction logs fill, reverse replication can be a good way to prepare the database in the primary location for switchback. If the database transaction logs fill before the primary database becomes available, reverse replication becomes ineffective. In this case, you will need to do a complete database copy as part of switching back to the primary location.

3. If necessary, power on the NA servers in the disaster recovery location.
4. If automatic starting of the NA services is enabled, stop all NA services on all NA cores in the disaster recovery location.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *UNIX*: Run the following command:

     ```
     /etc/init.d/truecontrol stop
     ```



5. Connect the NA cores in the disaster recovery location to the local database (the database in the disaster recovery location).

   On each NA server in the disaster recovery location, in a text editor such as WordPad or vi, edit following file:

   - *Windows*:

     ```
     <NA_HOME>\server\ext\jboss\server\default\deploy\db_ds.xml
     ```

   - *UNIX*:

     ```
     <NA_HOME>/server/ext/jboss/server/default/deploy/db_ds.xml
     ```

   This file contains two lines defining the `JdbcUrl` attribute. For example:

   - Oracle:

     ```
     <attribute name="JdbcUrl">jdbc:oracle:thin:@db.example.com:
     1521:nadb</attribute>
     ```

   - SQL Server:

     ```
     <attribute name="JdbcUrl">jdbc:sqlserver://db.example.com:
     1433;DatabaseName=NA;SendStringParametersAsUnicode=false
     </attribute>
     ```

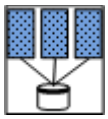
   For each `JdbcUrl` attribute, replace the database server name (`db.example.com` in the example) with the fully-qualified domain name or IP address of the database server in the disaster recovery location.

For Oracle, also replace the database SID or service name (**nadb** in the example) with the database SID or service name for the NA database in the disaster recovery location.

For SQL Server, also replace the database name (**NA** in the example) with the database name for the NA database in the disaster recovery location.

This step replaces the connection between these NA cores and the database in the primary location with a connection to the database in the disaster recovery location.

Task 4: Enable NA in the Disaster Recovery Location



To enable NA in the disaster recovery location, follow these steps:

1. If necessary, copy the NA server files from the intermediate location to the correct locations on the NA servers in the disaster recovery location. Maintain file ownership and permissions.
2. Activate the NA cores in the disaster recovery location.
   a. On *one* NA core in the disaster recovery location, start all NA services.
      — *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:

      TrueControl ManagementEngine

      TrueControl FTP Server

      TrueControl SWIM Server

      TrueControl Syslog Server

      TrueControl TFTP Server

      — *UNIX*: Run the following command:

      ```
      /etc/init.d/truecontrol restart
      ```

   b. Using telnet or SSH, connect as an NA administrator to the NA proxy on that NA core.
   c. Run the following command:

      ```
      list core
      ```

   d. From the `list core` command output, determine the core IDs of the NA cores in the disaster recovery location, and then run the following command for each core ID:

      ```
      core status -status normal -coreid <coreid>
      ```

This step changes the NA core status in the NA database in the disaster recovery location only. Unless reverse replication is running, the NA database in the primary location still shows these cores as inactive.

3 If NA is configured with tasks for a given device bound to only one core (the default Horizontal Scalability configuration), do the following:

a On the *one* running NA core in the disaster recovery location, restart all NA services.

— *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

TrueControl ManagementEngine

TrueControl FTP Server

TrueControl SWIM Server

TrueControl Syslog Server

TrueControl TFTP Server

— *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

b Log on to the NA console for the running NA core in the disaster recovery location.

c Update the site assignments. In the NA console, open the **Site Reassignment** page (**Admin > Distributed > Site Reassignment**), and then assign all partitions to NA cores in the disaster recovery location.

4 Deactivate the NA cores in the primary location.

a Connect as an NA administrator to the NA proxy on the *one* running NA core in the disaster recovery location.

b Run the following command:

```
list core
```

c From the `list core` command output, determine the core IDs of the NA cores in the primary location, and then run the following command for each core ID:

```
core status -status standby -coreid <coreid>
```

This step changes the NA core status in the NA database in the disaster recovery location only. Unless reverse replication is running, the NA database in the primary location still shows these cores as active.

5 Start (or restart) all NA services on all NA cores in the disaster recovery location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

The NA services on the primary NA cores must remain stopped.

6 Resume the tasks that were paused in Task 2, step 2 on page 21.

a Log on to the NA console for one of the NA cores in the primary location.

b On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **`Paused`**.

c On the Task Search Results page, resume each listed task.

Task 5: Finish Switchover

1 Configure any applications that integrate with NA to connect to the working NA cores in the disaster recovery location.

2 Notify users to connect to the NA console on the NA cores in the disaster recovery location.

3 *Optional*. Configure the managed devices to send syslog messages to one NA core in the disaster recovery location.

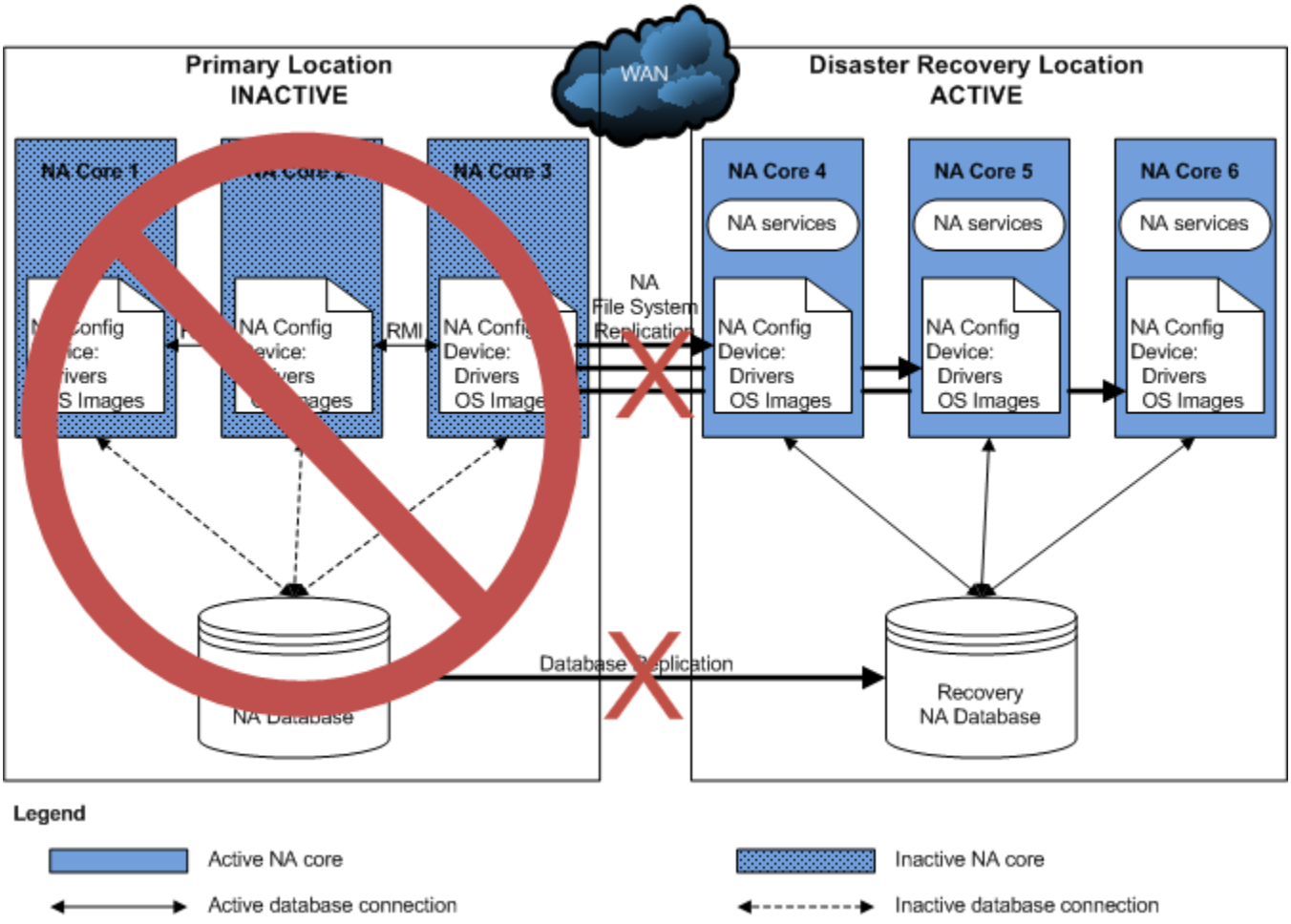
Without syslog messages, NA will detect configuration changes at the next scheduled snapshot.

Figure 3 shows the results of switching over to the disaster recovery location.

The **Allow this core to run all tasks created on it locally** setting on the NA cores in the primary location does not affect the distribution of tasks to the NA cores in the disaster recovery location. The following CLI command can be used to move a task to a different NA core:

```
mod task -id <Task ID> -coreid <Core ID>
```

Figure 3 After Switchover



4 Switchback

Switchback involves synchronizing application data from the disaster recovery location to the primary location. Switchback can be scheduled for a time with the least impact.

This chapter describes the following switchback scenarios:

- When the primary location again becomes available, an administrator can follow the procedure described in Switching Back to the Original Servers in the Primary Location on page 27 to switch the use of HP Network Automation Software (NA) back to the primary location.
- If the systems in the primary location cannot be recovered, configure new servers in the primary location or a new primary location, and then follow the process in Switching Back to Different NA and Database Servers on page 33 to switch NA to that location.
- Alternatively, you can run the disaster recovery location as the new primary location and configure a new disaster recovery location as described in Creating a New Disaster Recovery Location on page 42.

Switching Back to the Original Servers in the Primary Location

When the NA servers are available, switching back from the disaster recovery location to the primary location involves the following general process:

- Task 1: Disable NA in the Disaster Recovery Location on page 27
- Task 2: Enable the Use of the Database in the Primary Location on page 28
- Task 3: Enable NA in the Primary Location on page 30
- Task 4: Finish Switchback on page 31

Task 1: Disable NA in the Disaster Recovery Location

This task assumes that all NA services are stopped on all NA cores in the primary location.

To disable NA in the disaster recovery location, follow these steps:

1. Prepare to stop NA in the disaster recovery location. Do the following:
   a. Notify users to log out.
   b. Log on to the NA console for one of the NA cores in the disaster recovery location.
   c. Pause tasks scheduled to start during the switchback process (Task 3, step 5 on page 31). Include time for the currently running tasks to complete. Also include time for database synchronization. For example:
      — On the Search for Task page (**Reports > Search For > Tasks**), for the Schedule Date field, set since to **`Now`** and until to **`4 hours later`**.
      — On the Task Search Results page, pause each listed task.

d On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

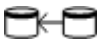
If any critical tasks are running, wait for them to complete before continuing with step 2, next.

2 Stop all NA services on all NA cores in the disaster recovery location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

Task 2: Enable the Use of the Database in the Primary Location

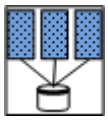


1 Synchronize the database in the primary location with the database in the disaster recovery location. Possible approaches include the following:

- Use database tools to copy the NA database from the disaster recovery location to the primary location. Copy the NA schema tables only.

  For example, you might follow this process:
  - Export the NA database from the recovery database server in the disaster recovery location.
  - Wipe the NA database from the database server in the primary location.
  - Import the NA database to the database server in the primary location.
- If reverse replication from the database in the disaster recovery location to the database in the primary location is running, analyze the reverse replication transaction logs.
  - If the transaction logs have overflowed, reverse replication becomes ineffective. In this case, disable reverse replication to the database in the primary location, and then use database tools to copy the NA database from the disaster recovery location to the primary location. Copy the NA schema tables only.
  - If the transaction logs are within bounds, wait for all database updates to replicate to the database in the primary location. After replication is complete, disable reverse replication to the database in the primary location.

2 Re-enable database replication from the primary location to the disaster recovery location.



3 Connect the NA cores in the disaster recovery location to the database in the primary location.

On each NA server in the disaster recovery location, in a text editor, edit following file:

- *Windows*:

  `<NA_HOME>\server\ext\jboss\server\default\deploy\db_ds.xml`

- *UNIX*:

  `<NA_HOME>/server/ext/jboss/server/default/deploy/db_ds.xml`

This file contains two lines defining the `JdbcUrl` attribute. For example:

- Oracle:

  ```
  <attribute name="JdbcUrl">jdbc:oracle:thin:@db.example.com:
  1521:nadb</attribute>
  ```

- SQL Server:

  ```
  <attribute name="JdbcUrl">jdbc:sqlserver://db.example.com:
  1433;DatabaseName=NA;SendStringParametersAsUnicode=false
  </attribute>
  ```

For each `JdbcUrl` attribute, replace the database server name (`db.example.com` in the example) with the fully-qualified domain name or IP address of the database server in the primary location.

For Oracle, also replace the database SID or service name (**`nadb`** in the example) with the database SID or service name for the NA database in the primary location.

For SQL Server, also replace the database name (**`NA`** in the example) with the database name for the NA database in the primary location.

This step replaces the connection between these NA cores and the database in the disaster recovery location with a connection to the database in the primary location.

4 Ensure that the NA servers in the primary location are powered on.

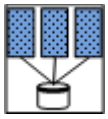
5 If automatic starting of the NA services is enabled, stop all NA services on all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

  `/etc/init.d/truecontrol stop`

6 Verify that the NA cores in the primary location are connected to the local database (the database in the primary location) as described in step 3.

Task 3: Enable NA in the Primary Location



To enable NA in the primary location, follow these steps:

1. If the configuration of the NA cores in the disaster recovery location has changed since switchover, update the NA core files on each NA server in the primary location. Maintain file ownership and permissions. See Table 1 on page 17.

   You will restart the NA services in step 5 on page 31. You do not need to do so now.

2. Activate the NA cores in the primary location.
   a. On *one* NA core in the primary location, start all NA services.
      — *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:

      TrueControl ManagementEngine

      TrueControl FTP Server

      TrueControl SWIM Server

      TrueControl Syslog Server

      TrueControl TFTP Server

      — *UNIX*: Run the following command:

      ```
      /etc/init.d/truecontrol restart
      ```

   b. Using telnet or SSH, connect as an NA administrator to the NA proxy on that NA core.
   c. Run the following command:

      ```
      list core
      ```

   d. From the `list core` command output, determine the core IDs of the NA cores in the primary location, and then run the following command for each core ID:

      ```
      core status -status normal -coreid <coreid>
      ```

   This step changes the NA core status in the NA database in the primary location. Because replication is running, the NA database in the disaster recovery location also shows these cores as active.

3. If NA is configured with tasks for a given device bound to only one core (the default Horizontal Scalability configuration), do the following:
   a. On the *one* running NA core in the primary location, restart all NA services.
      — *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

      TrueControl ManagementEngine

      TrueControl FTP Server

      TrueControl SWIM Server

      TrueControl Syslog Server

      TrueControl TFTP Server

      — *UNIX*: Run the following command:

      ```
      /etc/init.d/truecontrol restart
      ```

   b. Log on to the NA console for the running NA core in the primary location.

c Update the site assignments. In the NA console, open the **Site Reassignment** page (**Admin > Distributed > Site Reassignment**), and then assign all partitions to NA cores in the primary location.

4 Deactivate the NA cores in the disaster recovery location.

a Connect as an NA administrator to the NA proxy on the *one* running NA core in the primary location.

b Run the following command:

```
list core
```

c From the `list core` command output, determine the core IDs of the NA cores in the disaster recovery location, and then run the following command for each core ID:

```
core status -status standby -coreid <coreid>
```

This step changes the NA core status in the NA database in the primary location. Because replication is running, the NA database in the disaster recovery location also shows these cores as inactive.

5 Start (or restart) all NA services for all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

6 Resume the tasks that were paused in Task 1, step 1 on page 27.

a Log on to the NA console for one of the NA cores in the primary location.

b On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **Paused**.

c On the Task Search Results page, resume each listed task.

Task 4: Finish Switchback

1 Configure any applications that integrate with NA to connect to the working NA cores in the primary location.

2 Notify users to connect to the NA console on the NA cores in the primary location.

3 Re-enable file system replication from the primary location to the disaster recovery location.

4 *Optional*. If you chose to synchronize the NA files to an intermediate server, to conserve resources in the disaster recovery location, power down the NA servers in the disaster recovery location.

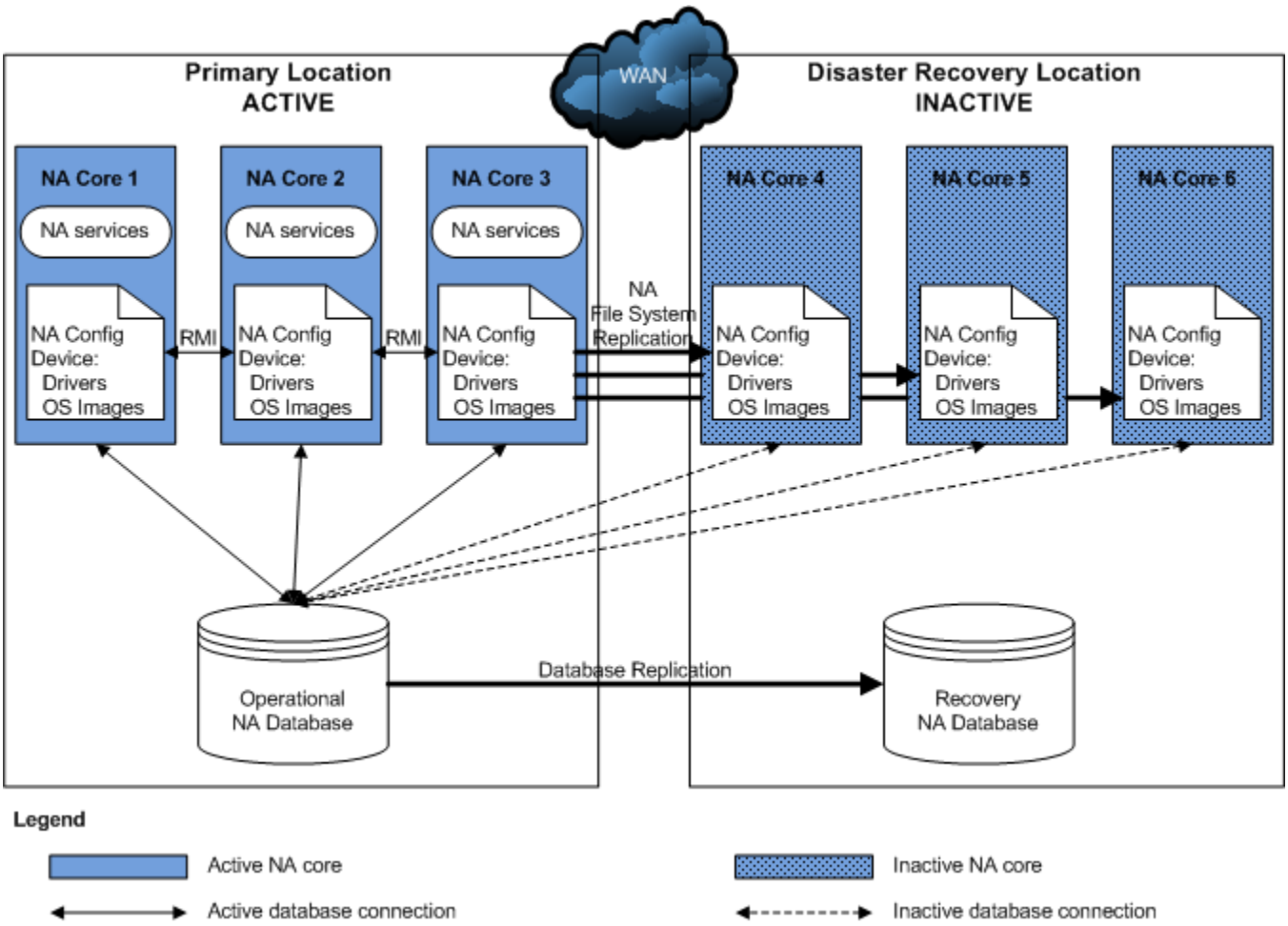
5 *Optional*. Configure the managed devices to send syslog messages to one NA core in the primary location and to no NA cores in the disaster recovery location.

Figure 4 shows the results of switching back to the primary location.

The **Allow this core to run all tasks created on it locally** setting on the NA cores in the primary location does not affect the distribution of tasks to the NA cores in the disaster recovery location. The following CLI command can be used to move a task to a different NA core:

```
mod task -id <Task ID> -coreid <Core ID>
```

Figure 4 After Switchback



Switching Back to Different NA and Database Servers

This section describes how to switch back to different primary servers than those from which the switchover to the disaster recovery location occurred. This situation applies to the following cases:

- New hardware has been provisioned in the original primary location. Any or all of the NA cores could be running on newly-provisioned servers. Additionally, the NA database might be running on a newly-provisioned server.
- The original primary location is no longer available, so a different site is now being used as the primary location. All NA servers and the database server are newly-provisioned.

In this procedure, the following terms apply:

- The primary location is the data center that will receive the NA deployment switched back from the disaster recovery location. This location could be the original primary location data center with newly-provisioned servers, or it could be a different data center with newly-provisioned servers.
- The existing NA cores are NA cores in the original primary location data center that are still available for switchback.
- The new NA cores are NA cores running on newly-provisioned servers in the primary location.
- The disaster recovery location is data center currently hosting the existing NA deployment.

Switching back from the disaster recovery location to one or more new servers in the primary location involves the following general process:

- Task 1: Disable NA in the Disaster Recovery Location on page 33
- Task 2: Enable the Use of the Database in the Primary Location on page 34
- Task 3: Enable NA in the Primary Location on page 37
- Task 4: Finish Switchback on page 40

Task 1: Disable NA in the Disaster Recovery Location

This task assumes that all NA services are stopped on all NA cores in the primary location.

To disable NA in the disaster recovery location, follow these steps:

1. Determine the core IDs of the NA cores in the original primary location that are no longer available.
   a. Connect as an NA administrator to the NA proxy on an NA core running in the disaster recovery location.
   b. Run the following command:

      ```
      list core
      ```

   c. Note the core ID for each unavailable NA server.

2 Prepare to stop NA in the disaster recovery location. Do the following:

a Notify users to log out.

b Log on to the NA console for one of the NA cores in the disaster recovery location.

c Pause tasks scheduled to start during the switchback process (Task 3, step 9 on page 40). Include time for the currently running tasks to complete. Also include time for database synchronization. For example:

— On the Search for Task page (**Reports > Search For > Tasks**), for the Schedule Date field, set since to **`Now`** and until to **`4 hours later`**.

— On the Task Search Results page, pause each listed task.

d On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

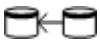
If any critical tasks are running, wait for them to complete before continuing with step 3, next.

3 Stop all NA services on all NA cores in the disaster recovery location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

Task 2: Enable the Use of the Database in the Primary Location



1 If the database server is newly-provisioned, create the NA schema on that database server.

Note the following:

- The NA database user in the disaster recovery location must have the same name and permissions as the NA database user in the primary location.
- Copy the NA schema tables only.
- For Oracle or Oracle RAC, the SID or service name should be different between the two database servers.

  One SID *cannot* be a subset of the other SID, for example NARp and NARpBU. Instead, use SIDs that stand alone, for example NARp1 and NARp2.
- For Microsoft SQL Server, the database name should be different between the two database servers.

For example, you might follow this process:

a Install the database software.

b Create a database user with the same name and permissions as the NA database user for the database in the disaster recovery location.

2 Synchronize the database in the primary location with the database in the disaster recovery location. Possible approaches include the following:

- Use database tools to copy the NA database from the disaster recovery location to the primary location. Copy the NA schema tables only.

  For example, you might follow this process:

  — Export the NA database from the recovery database server in the disaster recovery location.

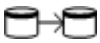
  — Wipe the NA database from the database server in the primary location.

  — Import the NA database to the database server in the primary location.

- If reverse replication from the database in the disaster recovery location to the database in the new primary location is running, analyze the reverse replication transaction logs.

  — If the transaction logs have overflowed, reverse replication becomes ineffective. In this case, disable reverse replication to the database in the primary location, and then use database tools to copy the NA database from the disaster recovery location to the primary location. Copy the NA schema tables only.

  — If the transaction logs are within bounds, wait for all database updates to replicate to the database in the primary location. After replication is complete, disable reverse replication to the database in the primary location.



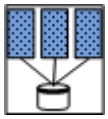
3 Configure database replication as follows:

- If the NA database server is newly-provisioned, update database replication as follows:

  — On the disaster recovery location database server, remove the configuration for database replication from the original primary location database server.

  — Configure one-way database replication from the database in the primary location to the recovery database in the disaster recovery location.

- If the NA database server is *not* newly-provisioned, re-enable database replication from the primary location to the disaster recovery location.



4 Connect the NA cores in the disaster recovery location to the database in the primary location.

On each NA server in the disaster recovery location, in a text editor, edit following file:

- *Windows*:

  `<NA_HOME>\server\ext\jboss\server\default\deploy\db_ds.xml`

- *UNIX*:

  `<NA_HOME>/server/ext/jboss/server/default/deploy/db_ds.xml`

This file contains two lines defining the `JdbcUrl` attribute. For example:

- Oracle:

  ```
  <attribute name="JdbcUrl">jdbc:oracle:thin:@db.example.com:
  1521:nadb</attribute>
  ```

- SQL Server:

```
<attribute name="JdbcUrl">jdbc:sqlserver://db.example.com:
1433;DatabaseName=NA;SendStringParametersAsUnicode=false
</attribute>
```

For each `JdbcUrl` attribute, replace the database server name (`db.example.com` in the example) with the fully-qualified domain name or IP address of the database server in the primary location.

For Oracle, also replace the database SID or service name (**`nadb`** in the example) with the database SID or service name for the NA database in the primary location.

For SQL Server, also replace the database name (**`NA`** in the example) with the database name for the NA database in the primary location.

This step replaces the connection between these NA cores and the database in the disaster recovery location with a connection to the database in the primary location.

5 Ensure that all existing NA servers in the primary location are powered on.

6 If automatic starting of the NA services is enabled for the existing NA cores, stop all NA services on all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

7 Connect the existing NA cores in the primary location to the local database (the database in the primary location) as follows:

- If the NA database server is newly-provisioned, update the `db_ds.xml` file as described in step 4.
- If the NA database server is *not* newly-provisioned, verify the `db_ds.xml` file as described in step 4.

8 In the primary location database, remove the unavailable NA servers from the NA database.

a Locate the list of core IDs for the unavailable NA servers, as determined in Task 1, step 1 on page 33.

b For each unavailable NA server in the original primary location, delete the entry for that NA server from the RN_CORE table of the NA database.

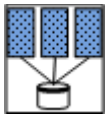
For example on Oracle:

```
DELETE FROM RN_CORE WHERE CoreID = <coreid>;
COMMIT;
```

For example on SQL Server:

```
DELETE FROM RN_CORE WHERE CoreID = <coreid>;
```

Task 3: Enable NA in the Primary Location



To enable NA in the primary location, follow these steps:

1. If the configuration of the NA cores in the disaster recovery location has changed since switchover, update the NA core files on each existing NA server in the primary location. See Table 1 on page 17.

   You will restart the NA services in step 9 on page 40. You do not need to do so now.

2. Verify that you have the *NA Horizontal Scalability Guide* for NA 9.20 patch 1 or later.

   If necessary, download the most recent version from:

   http://h20230.www2.hp.com/selfsolve/manuals

   For more information, see Documentation Updates on page 3.

3. In the primary location, install the new NA cores as additional NA cores connected (through Horizontal Scalability) to the database in the primary location.

   For information, see "Adding Additional NA Cores" in the *NA Horizontal Scalability Guide* for NA 9.20 patch 1 or later.

   Complete the script edits to account for having removed one or more NA cores from the Horizontal Scalability environment.

4. Configure the new NA cores as follows:

   a. Stop all NA services on the new NA cores.

      — *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:

      TrueControl ManagementEngine

      TrueControl FTP Server

      TrueControl SWIM Server

      TrueControl Syslog Server

      TrueControl TFTP Server

      — *UNIX*: Run the following command:

      ```
      /etc/init.d/truecontrol stop
      ```

   b. Put into place any modified files from those listed in Table 1 on page 17. Options include:

      — Copy the files from one of the NA servers in the disaster recovery location.

      — Retrieve the files from a backup.

c Start all NA services on the new NA cores.

— *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:

TrueControl ManagementEngine

TrueControl FTP Server

TrueControl SWIM Server

TrueControl Syslog Server

TrueControl TFTP Server

— *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

d *Optional*. Perform any NA core-specific tuning. Restart the NA services as needed.

5 If the NA environment includes NA Satellite functionality, do the following:

a If necessary, in the primary location install one or more core gateways.

Install at least one core gateway in the primary location to continue communication with the existing gateway mesh. Optionally install additional core gateways, up to one core gateway per NA core. During installation, configure each core gateway in the primary location as follows:

— Use the same Gateway Crypto Data file as for the core gateways in the original primary location.

— Assign the same realm name, typically Default Realm, to each core gateway.

For information, see the *NA Satellite Guide*.

b If necessary, in the primary location reconnect each core gateway installed on a system other than an NA server to an NA core.

For each core gateway that remains from the original primary location configuration and is not installed on an NA server, connect that core gateway with an NA server as described in "Configuring NA to Communicate with the Core Gateway" of the *NA Satellite Guide*.

c For each satellite in the gateway mesh, update the satellite configuration to enable communication with a core gateway in the primary location.

Edit the remote gateway configuration file:

`<gateway_install_dir>/opswgw-<gateway_name>/opswgw.properties`
(The default value of `<gateway_install_dir>` is `/etc/opt/opsware`.)

In the remote gateway configuration file, modify the `opswgw.TunnelSrc` entry that points to a core gateway in the original primary location to now point to a core gateway in the new primary location.

For example, change:

```
opswgw.TunnelSrc=<core_gateway1_IP>:2001:100:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem

opswgw.TunnelSrc=<core_gateway2_IP>:2001:200:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem
```

To:

```
opswgw.TunnelSrc=<core_gateway11_IP>:2001:100:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem

opswgw.TunnelSrc=<core_gateway2_IP>:2001:200:0:/var/opt/
opsware/crypto/opswgw-RemoteGw/opswgw.pem
```

d Restart each remote core gateway.

6 Activate the existing NA cores in the primary location.

a Connect as an NA administrator to the NA proxy on an NA core running on a newly-provisioned NA server.

b Run the following command:

```
list core
```

c From the `list core` command output, determine the core IDs of the original NA cores in the primary location, and then run the following command for each core ID:

```
core status -status normal -coreid <coreid>
```

This step changes the NA core status in the NA database in the primary location. Because replication is running, the NA database in the disaster recovery location also shows these cores as active.

7 If NA is configured with tasks for a given device bound to only one core (the default Horizontal Scalability configuration), do the following:

a On *one* running NA core in the primary location, restart all NA services.

— *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Restart**:

TrueControl ManagementEngine

TrueControl FTP Server

TrueControl SWIM Server

TrueControl Syslog Server

TrueControl TFTP Server

— *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

b Log on to the NA console for the NA core that was just restarted in the primary location.

c Update the site assignments. In the NA console, open the **Site Reassignment** page (**Admin > Distributed > Site Reassignment**), and then assign all partitions to NA cores in the primary location.

8 Deactivate the NA cores in the disaster recovery location.

a Connect as an NA administrator to the NA proxy on the NA core that was recently restarted in the primary location.

b Run the following command:

```
list core
```

c From the `list core` command output, determine the core IDs of the NA cores in the disaster recovery location, and then run the following command for each core ID:

```
core status -status standby -coreid <coreid>
```

This step changes the NA core status in the NA database in the primary location. Because replication is running, the NA database in the disaster recovery location also shows these cores as inactive.

9 Start (or restart) all NA services for all NA cores in the primary location.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Start**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol restart
```

10 Resume the tasks that were paused in Task 1, step 2 on page 34.

a Log on to the NA console for one of the NA cores in the primary location.

b On the Search for Task page (**Reports > Search For > Tasks**), for the Task Status field, select **Paused**.

c On the Task Search Results page, resume each listed task.

Task 4: Finish Switchback

1 Configure any applications that integrate with NA to connect to the working NA cores in the primary location.

2 Notify users to connect to the NA console on the NA cores in the primary location.

3 Configure replication of the NA file system from one of the active NA cores to the inactive NA cores (or an intermediate server) as described in Files to Synchronize Across NA Cores on page 16.

4 *Optional*. If you chose to synchronize the NA files to an intermediate server, to conserve resources in the disaster recovery location, power down the NA servers in the disaster recovery location.

5 *Optional*. Configure the managed devices to send syslog messages to one NA core in the primary location and to no NA cores in the disaster recovery location.

6 *Optional*. For the NA cores on the newly-provisioned NA servers, consider the risk that if the primary location is not accessible during switchover to the disaster recovery location, the NA cores in the primary location cannot be deactivated. In this case, two NA cores (one each in the primary and disaster recovery locations) might run the same task. To mitigate this risk, on each NA server in the primary location, disable automatic starting of the NA services.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, click **Properties**, and then set Startup Type to **Disabled**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *Linux*:

  ```
  mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
  ```
- *Solaris*:

  ```
  mv /etc/rc2.d/S99truecontrol /etc/S99truecontrol
  ```

Figure 4 on page 32 shows the results of switching back to the new primary location.

The **Allow this core to run all tasks created on it locally** setting on the NA cores in the primary location does not affect the distribution of tasks to the NA cores in the disaster recovery location. The following CLI command can be used to move a task to a different NA core:

```
mod task -id <Task ID> -coreid <Core ID>
```

Creating a New Disaster Recovery Location

This section describes how to set the current (original) disaster recovery location to be the new primary location with a new disaster recovery location.

In this procedure, the following terms apply:

- The original primary location is the data center that is no longer available.
- The new primary location is the data center hosting the existing NA deployment. This location is the original disaster recovery location.
- The new disaster recovery location is the data center that will receive the new NA deployment.

This configuration involves the following process:

1. *Optional*. Consider the risk that if the new primary location is not accessible during switchover to the disaster recovery location, the NA cores in the primary location cannot be deactivated. In this case, two NA cores (one each in the primary and disaster recovery locations) might run the same task. To mitigate this risk, on each NA server in the primary location, disable automatic starting of the NA services.
   - *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, click **Properties**, and then set Startup Type to **Disabled**:
     - **TrueControl ManagementEngine**
     - **TrueControl FTP Server**
     - **TrueControl SWIM Server**
     - **TrueControl Syslog Server**
     - **TrueControl TFTP Server**
   - *Linux*:

     ```
     mv /etc/rc.d/rc5.d/S99truecontrol /etc/S99truecontrol
     ```
   - *Solaris*:

     ```
     mv /etc/rc2.d/S99truecontrol /etc/S99truecontrol
     ```
2. Determine the core IDs of the NA cores in the original primary location that are no longer available.
   a. Connect as an NA administrator to the NA proxy on an NA core running in the disaster recovery location.
   b. Run the following command:

      ```
      list core
      ```
   c. Note the core ID for each unavailable NA server.
3. *Optional*. Perform any tuning needed to prepare the NA cores in the new primary location for daily use. Restart the NA services as needed.
4. *Optional*. Configure the managed devices to send syslog messages to one NA core in the new primary location.

5 Prepare to stop NA in the new primary location.

a Notify users to log out.

b Log on to the NA console for one of the NA cores in the new primary location.

c Pause tasks scheduled to start during the disaster recovery configuration process (until Task 4, step 1 on page 15). Include time for the currently running tasks to complete. Also include time for database synchronization. For example:

— On the Search for Task page (**Reports > Search For > Tasks**), for the Schedule Date field, set since to **`Now`** and until to **`4 hours later`**.

— On the Task Search Results page, pause each listed task.

d On the Running Tasks page (**Tasks > Running Tasks**), examine the list of running tasks.

If any critical tasks are running, let them run to completion before continuing with step 6.

6 In the new primary location, stop all NA services on all NA cores.

- *Windows*: Open the **Services** control panel. In the list of services, right-click each of the following services, and then click **Stop**:
  - **TrueControl ManagementEngine**
  - **TrueControl FTP Server**
  - **TrueControl SWIM Server**
  - **TrueControl Syslog Server**
  - **TrueControl TFTP Server**
- *UNIX*: Run the following command:

```
/etc/init.d/truecontrol stop
```

7 Clean up database replication as follows:

a On the new primary location database server, remove the configuration for database replication from the original primary location database server.

b If reverse replication from the database in the original disaster recovery location to the database in the original primary location was configured, remove that configuration.

8 In the new primary location database, remove the unavailable NA servers from the NA database.

a Locate the list of core IDs for the unavailable NA servers, as determined in step 2 on page 42.

b For each unavailable NA server in the original primary location, delete the entry for that NA server from the RN_CORE table of the NA database.

For example on Oracle:

```
DELETE FROM RN_CORE WHERE CoreID = <coreid>;
COMMIT;
```

For example on SQL Server:

```
DELETE FROM RN_CORE WHERE CoreID = <coreid>;
```

9 Remove any remaining configuration for replication of the NA file system from one of the NA cores in the original primary location to the original disaster recovery NA cores (or an intermediate server).

10 Verify that you have the *NA Horizontal Scalability Guide* for NA 9.20 patch 1 or later.

If necessary, download the most recent version from:

http://h20230.www2.hp.com/selfsolve/manuals

For more information, see Documentation Updates on page 3.

11 Beginning with Task 2: Configure Database Replication on page 13 and through the end of Chapter 2, NA Disaster Recovery Initial Setup, complete the process for setting up NA for disaster recovery.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NA 9.20 Patch 1 (9.20.01)

Document title: *NA Disaster Recovery Configuration Guide, August 2012*

Feedback: