High Availability (HA) Setup

*** Draft ***
Revised: Jan 22, 2006

Introduction

HA provides load balancing and failover for the sipX registration/redirect service (RR). See the HA spec for details. This document describes how to set up and configure HA, as an addendum to the standard sipX installation guide.

The release schedule for HA is uncertain. SIPxchange 3.2 may feature HA, but that's not guaranteed. We refer simply to “HA 1.0” in this document as the first release of SIPxchange that includes HA.

Before you begin

Verify Hardware Requirements

In an HA configuration, there are at least two types of Server:

- one Master Server (MS) running:
    - forking proxy
    - authentication proxy
    - registrar/redirect service
    - config service
    - VXML service with applications
    - publisher (status server)
    - presence
- one or more Distributed Servers (DS), each running:
    - forking proxy
    - authentication proxy
    - registrar/redirect service

For HA 1.0, only one configuration will be supported: one DS running only the proxies and registrar/redirect service, and one MS running all Services. The MS and DS should both conform to the standard hardware guidelines in the installation guide. However, only the MS hosts a VXML service and stores the associated voicemail. Therefore the DS does not need to budget disk for voicemail and can have a /var partition that is considerably smaller than the 40 GB recommended for the master. The DS runs fewer services than the MS, so it might be able to operate with reduced hardware resources, but we haven't yet done the measurements required to offer more specific guidance.

Establish Server Addresses

Select the fully qualified host names and IP addresses for your SIPxchange servers. “example.com” represents the local domain name throughout this document; replace it with the actual domain name for your installation. We recommend:

- `sipxchange1.example.com` for the MS
- `sipxchange2.example.com` for the DS

Prepare Installation Worksheets

Each machine must have a unique host name and IP address. Beyond that, they should be set up

identically, other than hard disk partitioning (see comments about /var above).

Verify browser requirements

After you install SIPxchange, you use a Web browser on a network PC to access the SIPxchange interface for administrators, which runs on top of the config service. The config service is installed only on the MS. You manage services (start/stop/restart/status) for both machines through the single config server instance. The registrations page shows only the registrations received by the MS. Since the registrations database is replicated between the two servers, each server has a complete database, and this is not a problem.

Installing a New SIPxchange System

Install Red Hat Enterprise

Same for both machines, except for the size of the /var partition as noted above.

Configuring DNS

In order to provide load sharing and failover, all SIP message routing to any redundant element in an HA configuration uses DNS SRV records. The following SRV records are required:

domain

In a single-system installation, an SRV record that maps the SIP domain name to the Server host name is recommended. In an HA installation, multiple SRV records for the SIP domain name are required, mapping to the Server names/ports that run the forking proxy service. There are domain SRV records specifying both TCP and UDP (with TCP given preference). For example:

```
$ORIGIN example.com.

_sip._tcp IN SRV   1 50 5060 sipxchange1
_sip._tcp IN SRV   1 50 5060 sipxchange2

_sip._udp IN SRV 101 50 5060 sipxchange1
_sip._udp IN SRV 101 50 5060 sipxchange2
```

registrar

The forwardingrules.xml for each forking proxy service specifies the registrar using an SRV name that maps first to the registrar instance on the same Server as the proxy (which is quicker to reach and more likely to be operational), and then to the registrar instance on the other Server (for failover). The registrar service SRV records specify only TCP, because TCP has better failure detection and performance characteristics and compatibility with User Agents is not required.

```
_sip._tcp.sipxregistrar1 IN SRV 1 50 5070 sipxchange1
_sip._tcp.sipxregistrar1 IN SRV 2 50 5070 sipxchange2

_sip._tcp.sipxregistrar2 IN SRV 1 50 5070 sipxchange2
_sip._tcp.sipxregistrar2 IN SRV 2 50 5070 sipxchange1
```

In the example above, the forking proxy on sipxchange1 would be configured to use sipxregistrar1, which preferentially routes to sipxchange1:5070 and fails

over to sipxchange2:5070. The forking proxy on sipxchange2 is configured to use sipxregistrar2, which uses the two Services in the reverse order.

authproxy

The forwardingrules.xml for each forking proxy service specifies the authorization proxy using a specialized SRV name configured similarly to the SRV name for the registrar. The authorization proxy SRV records specify both TCP and UDP, preferring TCP, but allowing UDP for compatibility with User Agents that require it. (The authorization proxy may be Record-Routed in dialogs.)

```
_sip._tcp.sipxauthproxy1 IN SRV   1 50 5080 sipxchange1
_sip._tcp.sipxauthproxy1 IN SRV   2 50 5080 sipxchange2
_sip._udp.sipxauthproxy1 IN SRV 101 50 5080 sipxchange1
_sip._udp.sipxauthproxy1 IN SRV 102 50 5080 sipxchange2

_sip._tcp.sipxauthproxy2 IN SRV   1 50 5080 sipxchange2
_sip._tcp.sipxauthproxy2 IN SRV   2 50 5080 sipxchange1
_sip._udp.sipxauthproxy2 IN SRV 101 50 5080 sipxchange2
_sip._udp.sipxauthproxy2 IN SRV 102 50 5080 sipxchange1
```

The selection technique used to create a preference order for registrars is also used for the authproxy, except that SRV records for UDP access are also provided, at lower priority than all the SRV records for TCP access.

Configuring DHCP

Set up DHCP on only one machine, whether it is a sipxchange machine or some other server.

Download and Install SIPxchange

Follow the same installation procedure for both machines, but disable all services on the DS except for:

- forking proxy
- authentication proxy
- registrar/redirect service

Do this by commenting out the right lines in ProcessDefinitions.xml, or some other way? Need to provide a detailed explanation here

SSL Key and Certificate Installation

Install SSL keys and certificates on both machines, following the standard procedure. Each machine needs its own unique certificate and key pairs. Both certificates should be signed by the same Certificate Authority.

The MS certificate needs to be installed on the DS and the DS certificate on the MS so that each machine can authenticate the other one for HA synchronization. What are the exact steps for cross-installation? Each machine should have the other machine's certificate but not its private key file.

Uninstall SIPxchange

Same for both machines