Control System Configuration

Introduction

The WSA Control System consists of the servers: WatchDog, Scheduler, and Dispatcher that need to be running for end-to-end connection provisioning and network auditing.

This chapter explains how to start, monitor, and stop the WSA Control System in the following sections:

Note   Prior to invoking the WSA Servers, ensure that the Network Access Points are defined for the network using the WSA System Administration GUI.

Starting the WSA Control System

Follow these steps to invoke the WSA Control System:

Step 1   Log in to the Solaris machine on which WSA is installed. Log in as **wsa**.

Step 2   Start WSA servers by entering the following command:

```
$ WSA_start
```

Note   A log of all actions is stored in the file **logfile** in the same directory from which the WSA_start script was invoked.

WSA_start is the main shell script that runs and configures the WSA control system server processes.

This script invokes the following three processes.

Note   You do not need to execute the following processes. They are described to clarify the behavior of the WSA servers.

1 Dispatcher process

WSA_Dispatcher -v &

This process talks to the network via a Control Processor Module. This process is responsible for network control message flow to and from WSA and from and to the network.

The **-v** flag indicates verbose mode such that all information is logged into a file **logfile** within the same directory.

2 Scheduler process

WSA_Scheduler -i -s +sched1 -c 30 &

This process sends tasks to the dispatcher at the appropriate date and time. This process also polls the dispatcher periodically for notification of task status and annotates the tasks in the WSA database.

The interval between task progress checks is 30 seconds, as supplied by the **-c** option.

3 WatchDog process

WSA_WatchDog -u -l -v -i 300 -z 180 &

When the WatchDog process is invoked with the previous flags, tasks are generated for connection provisioning and the task completion status is updated.

The interval between creating tasks is five minutes, as supplied by the **-i** option (default is 20 minutes).

The interval between task status updates is three minutes, as supplied by the **-z** option (default is five minutes).

The above options on the WatchDog process indicate that the WatchDog process runs every five minutes to pick up tasks to be provisioned and every three minutes to update any pending task status.

Monitoring the WSA Control System

Follow these steps to monitor a running WSA Control System:

Step 1   Log into the WSA Solaris server as **wsa**.

Step 2   Run the monitoring script.

```
$ /opt/CSCOwsa/bin/WSA_ps
```

This script displays all the WSA server processes.

The output should list at least one WSA_Scheduler, WSA_Dispatcher, and WSA_WatchDog process.

Stopping the WSA Control System

Follow these steps to perform a graceful shutdown of the WSA server processes:

Step 1   Log into the WSA Solaris server as **wsa**.

Step 2   Run the kill script to stop the WSA Control System.

```
$ /opt/CSCOwsa/bin/WSA_kill
```

⚠️ **Caution**   If the Solaris machine on which WSA servers are running is rebooted for any reason, the WSA servers need to be run again by re-executing the previous steps.

Starting and Stopping the WSA Discovery Server

The WSA Discovery Server runs on the SV+ Solaris Server and starts requests from WSA for discovering SV+ managed networks. This server, **wsadisc**, needs to be running for WSA_Probe, WSA_Loader, and WSA_Audit to work.

Starting the WSA Discovery Server

To start the WSA Discovery Server, telnet to the SV+ Solaris server as user **svplus**.

Then execute the following:

```
ps -ef | grep wsadisc
```

If the output from the previous command contains the words **scotty wsadisc** at the end, as shown next, then the WSA Discovery Server is running on that machine.

```
svplus  1007   984  0 14:23:19 pts/6    0:00 scotty wsadisc
```

If you do not see the previous line, then you need to start the WSA Discovery Server as follows:

```
cd ~svplus/wsa
source .wsarc
cd bin
wsadisc
```

The following message appears:

WSA Discovery Server: Setting Server port to 5000
****
*   WSA Discovery Server 1.1   *
*   (c) Cisco Systems Inc. 1998, 1999   *
****

Note   If wsadisc fails to start with a message **libresolv.so.2 not found**, ensure that the SV+ Solaris server includes Solaris patches recommended for SV+ 9.1.06.

Stopping the WSA Discovery Server

To stop the WSA Discovery Server, telnet to the SV+ Solaris server and kill the **scotty wsadisc** process by either interrupting (**Ctrl-C**) or using the UNIX **kill** command.

Discovering SV+ Networks

To discover one or more networks managed by SV+ using WSA, do the following steps:

Step 1   Log in as user **wsa** on the WSA Solaris server.

Step 2   Ensure that WSA Discovery Server **wsadisc** is running on the SV+ Solaris server.

Step 3   On the WSA Solaris server, execute WSA_Probe (refer to section WSA_Probe on page 6-11 for more details).

For example, to generate the network probe file from Network **Network1** using **ultra30qa** as the SV+ database host with user name **svplus** and password **svplus**, run WSA_Probe as follows:

```
WSA_Probe -n Network1 -a ultra30qa -u svplus -p svplus -R public -W
private -o probe.dat
```

Option	Description
-a<*ip address*>	Hostname of machine on which SV+ is running (**ultra30qa**, in this example).
-L <*sev*>[:<*lev*>[<*sev*>[:<*lev*>]]] where: <*sev*> <*lev*>	Log messages at or above both of these severity levels INFO, WARN, ERR, or SEV 0 to 10 <*sev*>:<*lev*> is for **stderr** <*sev*>:<*lev*> is for **logfile**
-n<*netname*>	What to name the network (**Network1** in this example)
-o<*filename*>	Name of file in which the probe data is dumped (**probe.dat**, in this example). Note: WSA_Probe creates the **probe.dat.Network1** file containing the Network data. The network name is appended to the file name.
-p<*password*>	SV+ user password (**svplus**, in this example).
-R<*snmp read*>	snmp read community string (**public**, in this example).
-u<username>	SV+ user name (**svplus**, in this example).
-v	Verbose mode, also show software build, version, and initialization status
-W<*snmp write*>	snmp write mode
-x	Command usage explanation

Note The file generated by WSA_Probe is in a Cisco proprietary format.

Loading Networks

WSA allows users to load a network from a file created by WSA_Probe or directly from a network using an SV+ database. The following information is loaded: nodes, cards within nodes, ports, trunks, and connections.

Loading a Network from a File

To load a network from a file, do the following:

Step 1 Log in as user **wsa** on the WSA Solaris server.

Step 2 Change the directory to the one containing the probe file **probe.dat.Network1** as generated by WSA_Probe in section Discovering SV+ Networks on page 5-5.

Step 3 Execute WSA_Loader, as follows (refer to section WSA_Loader on page 6-8 for more details):

```
WSA_Loader  -i probe.dat.Network1
```

If you supply a network name using the **-n** option, then all network data entries contained in the probe file are mapped to the new network name within the WSA database.

Launch the WSA Administration application on the PC and authorize yourself to view the network and region created by WSA_Loader. Then, launch the WSA Explorer application to view the loaded network.

Loading a Network from a Live Network

To load a network from a live network using a SV+ database, do the following:

Step 1 Log in as user **wsa** on the WSA Solaris server.

Step 2 Ensure Network Access Points are set up using the WSA Administration application. This is an important step, because WSA_Loader tries to load networks as defined by the Network Access Points.

Step 3 Ensure that the WSA Discovery Server **wsadisc** is running on the SV+ Solaris server (refer to section Starting and Stopping the WSA Discovery Server on page 5-4 for more details).

Step 4 Execute WSA_Loader, as follows (refer to section WSA_Loader on page 6-8 for more details):

WSA_Loader

Launch the WSA Administration application on the PC and authorize yourself to view the network and region created by WSA_Loader. Then, launch the WSA Explorer application to view the loaded network.