

HP



Data Center Automation Appliance

DCAA Satellite Guide

Express & Premium Edition

Software Version: 1.00

Release Date: June 2015

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 Notice

© Copyright 2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation. UNIX® is a registered trademark of The Open Group.

The OpenStack® Word Mark and the Square O Design, together or apart, are trademarks or registered trademarks marks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission.

Adobe™ is a trademark of Adobe Systems Incorporated.

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

The OpenStack® Word Mark and the Square O Design, together or apart, are trademarks or registered trademarks marks of OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission.

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

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document 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

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 online support 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 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 register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is <http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Chapter 1 DCAA Satellite Guide.....	7
Chapter 2 Advanced DCAA Architecture	8
Overview and Architecture	8
The SA Core	12
DCAA Server Agents.....	12
The Core Components	13
DCAA Core Component Bundling	13
DCAA Gateways.....	14
SA Topology for DCAA	14
Single Host Core	14
Facilities and Realms.....	14
Facilities.....	14
Realms	15
Satellite Topology Examples	16
A Simple DCAA Core to Satellite Link.....	16
A Two Satellite to Single DCAA Core Link.....	17
Chapter 3 DCAA Satellite Installation	18
Satellite Installation Basics	18
Satellite Installation Phases	18
Satellite Installation Requirements	18
DCAA Satellite - Installation Procedure.....	20
Phase 1: Prerequisites	20
Phase 2: Preparation	20
Phase 3: Installation Procedure: Install the Satellite.....	20
Phase 4: Post-installation Tasks.....	22
Uninstalling Satellites	22
Chapter 4 Satellite Administration	25
Starting/Restarting a Satellite	25
Stopping a Satellite.....	25
Verifying Satellite Communication with the Primary Core.....	25
Permissions Required for Managing Satellites.....	26
Viewing Satellite Information	26
Viewing Satellite Facilities and Realms	26
Viewing the Realm of a Satellite Managed Server	26
Viewing and Managing Satellite Gateway Information	27
Viewing Gateway Diagnostic and Debugging Information.....	28

Identifying the Source IP Address and Realm for a Connection	29
Changing the Bandwidth Usage or Link Cost Between Gateways	29
Viewing the Gateway Log or Change the Log Level	30
Restarting or Stopping a Gateway Process	30
Appendix A: Parameter Reference	31
Appendix B: HP DCAA Doc Library	34
Appendix C: HP SA Doc Library	35

Chapter 1 DCAA Satellite Guide

This *DCAA Satellite Guide* provides information about the how DCAA manages supported satellite operations.

DCAA has two editions:

- The Premium Edition of the HP Data Center Automation Appliance (DCAA-PE).
- The Express Edition of Data Center Automation Appliance (DCAA-EE).

The DCAA Satellite Guide works identically for both editions of DCAA.

In brief, DCAA is a virtual appliance used to provision and manage servers. DCAA bundles HP Operations Orchestration (HP OO) and HP Server Automation (HP SA) to enable you to automate Data Center management activities such as:

- Day 1 server provisioning
- Day 2 audit and compliance, software management, virtualization management, satellite setup, and more

You can leverage out-of-the-box user interface flows for day 1 and day 2 management activities and can also tap into the rich capabilities of HP OO and HP SA for more complex management use cases.

For more information about the **HP DCAA Premium Edition** or the **HP DCAA Express Edition**, see the *HP DCAA Release Notes*, *DCAA Installation and Administration Guide*, and the *HP DCAA Premium Edition User Guide*.

Please reference [Appendix B: DCAA Documentation Library](#) in this document to easily locate these guides online.

DCAA Satellites

A DCAA Satellite installation can be a solution for remote sites that do not have a large enough number of potentially Managed Servers to justify a full DCAA installation. A Satellite installation allows you to install only the minimum necessary Core Components on the Satellite host which then accesses the appliance's database and other services through an SA Gateway connection.

A Satellite installation can also relieve bandwidth problems for remote sites that may be connected to a primary facility through a limited network connection. You can cap a Satellite's use of network bandwidth to a specified bit rate limit. This allows you to ensure that Satellite network traffic will not interfere with your other critical systems network bandwidth requirements on the same pipe.

A Satellite installation typically consists of, at minimum, a Satellite Gateway and a Software Repository Cache and still allows you to fully manage servers at a remote facility. The Software Repository Cache contains local copies of software packages to be installed on Managed Servers in the Satellite while the Satellite Gateway handles communication with the Primary Core. You can optionally install the SA Provisioning Boot Server and Media Server on the Satellite host to support remote SA Provisioning. Installing other components on the Satellite host is not supported.

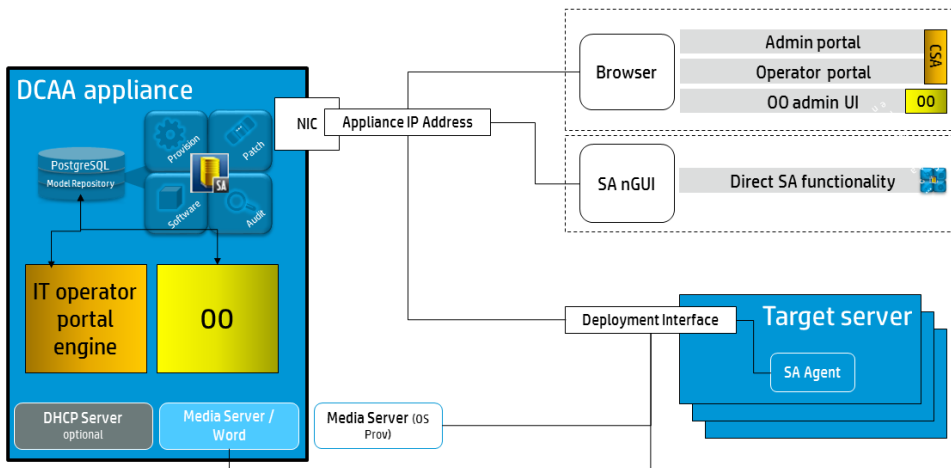
For more information about SA Satellite installations, see Chapter 7 in the *HP SA 10.2 Installation Guide*, which you can access using the [Appendix C: SA Documentation Library](#) in this guide.

Chapter 2 Advanced DCAA Architecture

Overview and Architecture

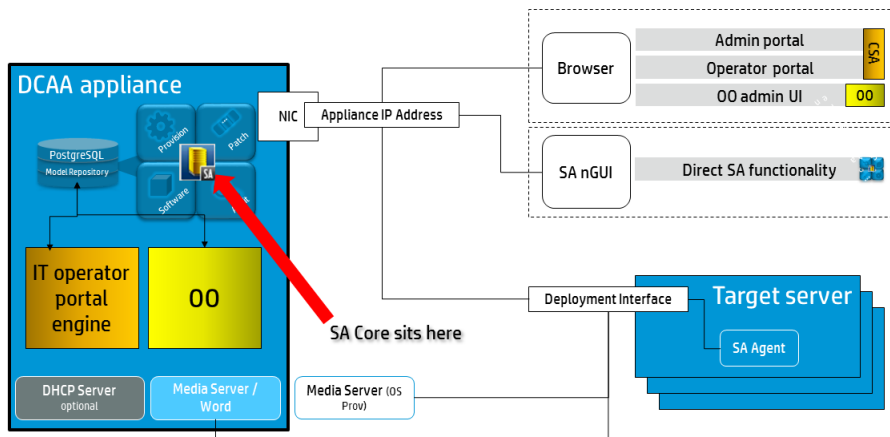
This section is intended for those users who want a more in-depth understanding of DCAA architecture. You will learn about the DCAA Core and its Core Components and the relationship between the core, Server Agents, and Satellites.

Figure A. DCAA Architecture



DCAA uses the PostgreSQL database for its Model Repository. The integrated SA Core, DCAA IT Operator portal engine, Operations Orchestration (OO), and metadata all use the PostgreSQL database, shown here in [Figure A](#). The optional DHCP Server and the Media Server handles OS Provisioning. DCAA uses a single NIC and single Appliance IP Address. A Browser accesses the DCAA Admin portal, the IT Operator portal, and also the Admin UI for OO. You can use the SA nGUI to get back to the Direct SA functionality.

Figure B. DCAA Architecture (detail)

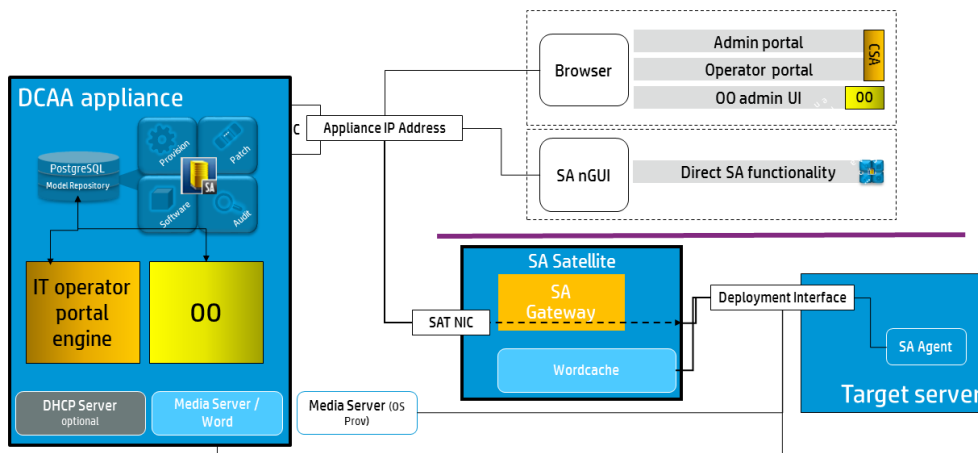


DCAA comes embedded with a ready to use **SA Core**; see Figure B. The SA Core is a set of components that perform the actions requested by the user to manage their registered datacenter(s).

Please see the [SA Core](#) section in this document for further details on the SA Core.

Now let's look at a view of the DCAA architecture with a single satellite added. Figure C (below) shows the structure of the Satellite, which consists of an SA Gateway, the Software Repository Cache (Wordcache), and the SA Agent connecting through the Satellite gateway to the SA Core running on the DCAA appliance and downloading data from the Satellite Wordcache.

Figure C. DCAA Architecture with single satellite



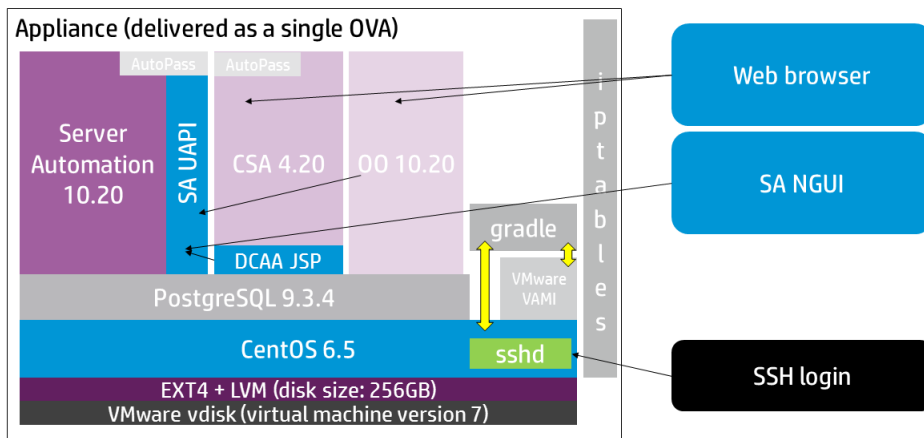
Optionally, one may install one or more satellites connected to the DCAA appliance. A satellite has a small subset of components installed and cannot function independently from a SA Core. They can be used to manage small remote sites from the DCAA appliance or to reduce bandwidth consumption between networks for tasks such as software installation or provisioning operating systems on servers.

If you are familiar with how SA runs satellites, much of the remaining guide will look familiar. Fundamentally, the SA Core manages satellites in DCAA using the same methods and approach as it does in SA Ultimate Edition.

For more information about SA Satellites, please see Chapter 3, Advanced SA Architecture in the *HP SA 10.2 Overview and Architecture Guide*, which you can access using the [Appendix C: SA Documentation Library](#) in this guide.

NOTE: Please note that the SA Multimaster Mesh is not supported in DCAA 1.00.

Figure D. DCAA Technology Stack



Looking at the technology stack in Figure D, starting at the bottom going to top of the stack, DCAA is delivered as an OVA running on a VMware vdisk version 7 virtual machine formatted using the EXT4 star system plus Logical Volume Management (LVM) which is ideal for managing large disk volumes and extending disk space easily. The Operating System is CentOS 6.5, and has a number of important security updates. The repository runs PostgreSQL 9.3.4, and manages the three main integrated products: Server Automation 10.20, Cloud Service Automation (CSA) 4.20 and Operations Orchestration (OO) 10.20. A standard web browser accesses CSA and OO components, whereas you can use the SA nGUI to access the SA UAPI on SA.

DCAA is AutoPass license enabled. The free trial edition will allow for 45 days unlimited use, after which the appliance will stop working.

Three integrated, open-source components that are used by DCAA are Gradle, VMware’s VAMI, and IPTables.

- Gradle is used for First Time Setup (FTS), and additional automation procedures.
- VMware’s VAMI (Virtual Appliance Management Instrumentation) is used for managing components built using VMware’s VM Studio.
- Security is run on the appliance using the IPTables firewall. Note that once the appliance is deployed and ready to run, only the ports which allow access to the integrated products are open; no other ports are usable on the appliance.

Also, DCAA now provides SSH login capabilities, which is a change from SAVA. The product is more open, easier to login with fewer constraints on initial startup.

Installation and initial setup of the DCAA Satellite will be different, however Administration of the satellite is very similar to how it is handled in SA since the DCAA Satellite is run by an SA Core. Thus, from this point forward, much of this guide will be

referring directly to SA topics from the *SA Overview and Architecture Guide* as they relate to Administration and Management issues of a satellite, since these are virtually unchanged.

The SA Core

A DCAA appliance is fundamentally an SA Core. For the remainder of this document, SA Core, DCAA Core and DCAA appliance can and will be used interchangeably and refer to the same component bundle.

The SA Core is a set of *Core Components* that work together to allow you to discover servers on your network, add those servers to a Managed Server Pool, and then provision, configure, patch, monitor, audit, and maintain those servers from a centralized DCAA Client interface. The DCAA Client provides a single interface to all the information and management capabilities of DCAA.

The servers that the Core Components are installed on are called *Core Servers*. The DCAA appliance *is* an SA Core server.

Core Components can all be installed on a single host or distributed across several hosts, however, a DCAA appliance has all SA Core components installed on the single appliance host. No other configuration is supported.

In order to communicate and perform certain server management activities, DCAA installs *Server Agents* on each Managed Server and communicates with the Managed Servers through Gateways that are part of the SA Core Components. Server Agents also perform certain actions on Managed Servers as directed by user input from the DCAA Client or DCAA IT Operator UI.

DCAA Server Agents

A DCAA Server Agent is intelligent software that is installed on all servers that you want DCAA to manage. After an agent is installed on an agentless server, the agent registers the server with the DCAA Core which then adds that server to its pool of Managed Servers. The DCAA Agent also receives user initiated commands from the Core and takes the appropriate action on the server it is installed on, such as software installation and removal, software and hardware configuration, server status reporting, auditing, and so on.

During agent registration, DCAA assigns each server a unique ID (the Machine ID (MID)) and stores this ID in the Model Repository. Servers can also be uniquely identified by their MAC Address (the network interface card's unique hexadecimal hardware identifier, which is used as the device's physical address on the network).

For more information on running the DCAA Manage Servers component, see the ***DCAA Installation and Administration Guide***, which you can access using the [Appendix B: DCAA Documentation Library](#) in this guide.

For more information on installing and managing Server Agents see the ***SA Users Guide: Server Automation*** section, which you can access using the [Appendix C: SA Documentation Library](#) in this guide.

The Core Components

The Core Components are the heart of the DCAA Core, making it possible to monitor and manage servers. When you retrieve vital information about network servers, provision servers, apply patches, take servers on and off line, configure and audit servers, and more, this interaction is controlled by the Core Components. The following section describes the DCAA Core Components and interfaces.

DCAA Core Component Bundling

All DCAA Core Components are *bundled* together and have been installed as a *unit*.

Table 1 shows the DCAA component bundle and their constituent components:

Table 1 DCAA Core Components

Model Repository	Infrastructure Components	DCAA Provisioning Components	Slice Components
Model Repository	Management Gateway Primary Data Access Engine Model Repository Multimaster Component (*) Software Repository Store (can be located on another host)	Media Server Boot Server	Core Gateway/ Agent Gateway Command Center Global File System Web Services Data Access Engine Secondary Data Access Engine Build Manager (*) Command Engine Software Repository HP Live Network (HPLN) DCML Exchange Tool (DET) Software Repository Accelerator (tsunami) Memcache



The *Boot Agent* is unrelated to Server Agents and operates as part of DCAA Provisioning.
(*) Not supported in DCAA.

DCAA Gateways

DCAA Gateways manage communication between Managed Servers and a DCAA Core, and between Satellite installations and a DCAA Core. Satellite installations are discussed in [Satellite Installation](#) on page 17.

There are several types of gateways:

- [Management Gateway](#)

This gateway manages communication between DCAA Cores and Satellites.

- [Core Gateway/Agent Gateway](#)

These gateways work together to facilitate communication between the DCAA Core and DCAA Agents on managed servers.

- [Satellite Gateway](#)

This gateway communicates with the DCAA Core through the Management Gateway or the Core Gateway depending on your configuration.

SA Topology for DCAA

Single Host Core

The DCAA appliance contains a single, complete SA Core.

Facilities and Realms

SA Gateways use two constructs that facilitate routing network traffic and eliminate the possibility of IP address conflicts: [Facilities](#) and [Realms](#).

Facilities

A *Facility* is a construct that typically represents a collection of servers that a single SA Core manages through the data about the managed environment stored in its Model Repository. A facility typically represents a specific geographical location, such as Sunnyvale, San Francisco, or New York, or, commonly, a specific data center.

A Facility is a permissions boundary within SA, that is, a user's permissions in one Facility do not carry over to another. Every Managed Server is assigned to a single facility. When a device initially registers with the SA Core, it is assigned to the facility associated with the gateway through which it is registering.

For example, Admin A works in Sunnyvale and is in charge of maintaining server patches. In a Facility

framework, Admin A is bound to the Sunnyvale Facility as a user. When Admin A views servers, only those servers that are also bound to the Sunnyvale Facility are displayed. He will not see servers for any other Facility.

There are two types of facilities:

1) **Core Facilities**

There is one Core Facility for every SA Core installation.

2) **Satellite Facilities**

A default Facility created when you install a Satellite.

Realms

Realms are an SA construct that allow SA to manage servers on different networks in the same Facility without fear of IP address conflicts. A realm is a unique identifier, appended to the IP address of a device in a Facility's network, which allows SA Gateways to uniquely identify devices on different networks in a Multimaster Mesh that may have conflicting IP addresses.

A Realm is a logical entity that defines an IP namespace *within which* all Managed Server IP addresses must be unique. However, servers that are assigned to *different Realms* can have duplicate IP addresses and still be uniquely identified within SA by their Realm membership.

Realms are interconnected by gateways in what can be described as a *gateway mesh* — a single interconnected network of SA Gateways.

When you create and name a new Facility during installation, a *default* Realm is also created with the same name as the Facility. For example, when you create the Facility, *Datacenter*, the installation also creates a Realm named *Datacenter*. Subsequent Realms in that facility could be named *Datacenter001*, *Datacenter002*, and so on. Managed servers in each realm are uniquely identified by the combination of the Realm name and the IP address.

A connection within the mesh has an ingress (or source) realm, where the connection enters the mesh, and an egress (or destination) realm, where the connection exits the mesh.

All SA managed devices are assigned to exactly one realm. Which realm they are assigned to can change dynamically (though it typically will not change). Whenever a device registers with the core, the core looks up the ingress realm for the registration using a gateway identity server, and then assigns the device to that realm.

If the registration occurs using a direct connection, the device is assigned to the *transitional realm*. The transitional realm may be thought of as a non-realm. It exists merely to denote devices which register themselves with a core using a direct connection.

With the exception of the transitional realm, realms do not span facilities (that is, every realm has a relationship to exactly one facility except for the transitional realm).

Within the mesh, there are two categories of realms:

- Root Realms
- Non-root Realms

Existing in the mesh are one or more realms which are at the “center” of the mesh. These realms are known as *root realms*. When a gateway is asked to route a connection, if that connection does not specify

a destination realm, the connection will be routed to the “closest” root realm, where “closest” refers to whichever root realm is reachable at the least network cost.

Root realms also have a special relationship in SA to facilities. Whenever an SA Core is installed, a facility is created. At the same time, a root realm is created which has a 1:1 relationship with the new facility.

Satellite Topology Examples

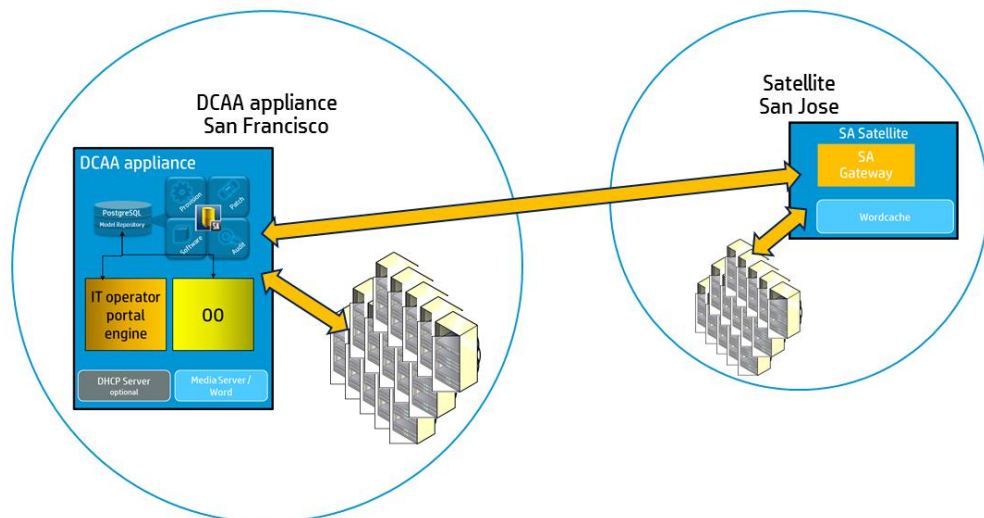
A Simple DCAA Core to Satellite Link

Figure E shows a single Satellite linked to a Single DCAA Core. In this example, the main facility is in San Francisco, and a smaller remote facility is in San Jose.

The San Francisco DCAA Core consists of several components, including the Software Repository, the Model Repository, an Agent gateway and a Management Gateway. For simplicity, this figure does not show all required Core Components, such as the Command Engine.

The San Jose Satellite consists of a Software Repository Cache, a Satellite Gateway, and an optional SA Provisioning Boot server and Media Server.

Figure E Satellite with the Single Core



The San Jose Satellite’s Software Repository Cache contains local copies of software packages to be installed on Managed Servers in that facility.

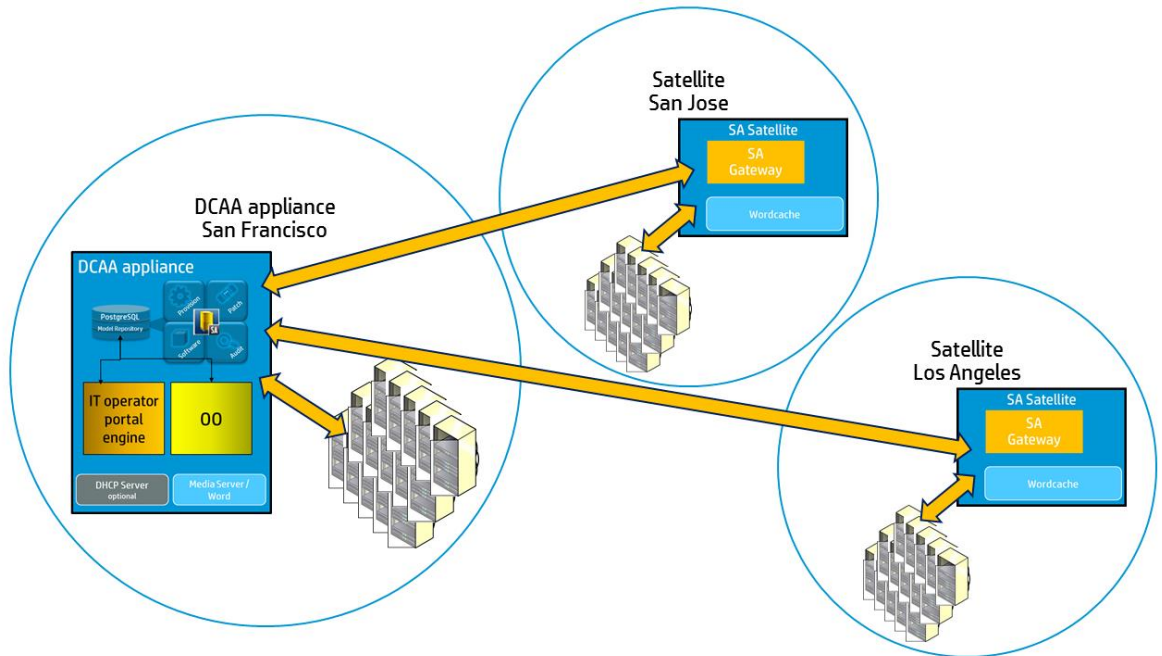
The Server Agents installed on managed servers at the San Jose facility connect to the San Francisco core through the San Jose Satellite Gateway which communicates with the San Francisco Management Gateway, ultimately connecting through the San Francisco Core gateway with the required Core Components.

Return communication reverses that path. The Server Agents installed on managed servers in the San Francisco facility communicate with the Core Components through the San Francisco facility's Agent and Core Gateways.

A Two Satellite to Single DCAA Core Link

Figure F shows two Satellites linked to a Single DCAA Core. In this example, San Francisco is the main facility, Los Angeles and San Jose are Satellite facilities.

Figure F Two Satellites with a Single Core



For detailed information about more SA related topics relevant to DCAA, see the *SA Documentation Reference Table* in the *HP DCAA Installation and Administration Guide*.

Chapter 3 DCAA Satellite Installation

This section provides an overview of Satellites and Satellite installation requirements as well as instructions for installing a Satellite and post-installation tasks.

Satellite Installation Basics

A Satellite installation can be a solution for remote sites that do not have a large enough number of potential Managed Servers to justify a full SA Core installation by allowing you to install only the necessary Core Components for the remote site to function as a Satellite.

If you are unsure of what a Satellite is, see the *SA Product Overview and Architecture* guide for an introduction to Satellites.

Satellite Installation Phases

This section provides a summary of the Satellite installation process. You can use the right-hand column on [Table 2](#) to indicate that a phase is completed:

Table 2 Satellite Installation Phases

Phase	Description	Complete
1	Requirements and Prerequisites	
2	Preparation	
3	Installation Procedure: Install the Satellite	
4	Post-Installation Tasks	

Satellite Installation Requirements

Before you install a Satellite, verify that you meet following requirements

- If you plan to install the optional SA Provisioning Boot Server and Media Server components in the Satellite, you must adhere to the requirements in *SA Provisioning: DHCP Proxying* on page 50 of the SA 10.2 Installation Guide.
- The required packages listed in *Required Linux Packages for SA Satellites* in this section must be installed on the Satellite server.
- The SA Core that will provide core component services to the Satellite must be running and accessible during Satellite installation and the Satellite server must have network connectivity to that Core's Management Gateway.
- You must be a member of the *System Administrators* group as well as a member of any user group that has Manage Gateway permissions.
- You must have root access to the DCAA appliance from which you need to copy the cryptographic material and security configuration file to the Satellite server.
- The Satellite server uses UTC. The Satellite server's system time **must** be synchronized with the DCAA appliance.

- If you plan to locate the Satellite's Software Repository Cache on a network storage device, the network storage configuration must allow root write access over NFS to the directories in which the Software Repository Cache will be installed.
- If you already have an SA Server Agent installed on a server you plan to use for a new Satellite, you must *uninstall* it before running the Satellite Installer.
- Make note that after the installation process completes, the new Satellite server is owned by the customer "Op_sware". You should take into account any effects this may have on access rights before beginning the installation.
- A minimum number of 2 CPUs and 2GB of RAM is required on the host where the satellite will be installed.

Disk Space Requirements for SA Satellites

Table 3 describes the free disk space (in addition to the operating files system) requirements for any SA Satellite and its op_sware components.

Table 3

Satellite Component Directory	Recommended Free Disk Space
/opt/op _s ware	15 GB
/var/log/op _s ware	10 GB
/var/opt/op _s ware	20 GB (dependent on caching plans and the core cache size)
/media/op _s ware	15 GB (dependent on SA Provisioning needs)

Required Linux Packages for SA Satellites

The SA Installer performs an automatic prerequisite check on the SA Satellite host to ensure that environment settings are met and all required OS packages are installed. For detailed information about the SA Prerequisite Checker, see "Familiarize Yourself with the SA Installer Prerequisite Checker" on page 37 of the *SA 10.2 Installation Guide*.

Required Open Ports

The ports listed in Table 4 must be open for use by the Satellite's Gateway. The port numbers listed in the table are default values. You can select other values during the installation.

Table 4 Open Ports for Satellites

Port	Description
------	-------------

1002	Agent
1003	Wordcache
1006	Wordcache
2001	The port used by a tunnel end-point listener. This port is used when you install other Gateways that tunnel to the Satellite.
3001	The proxy port on which Agents contact the Satellite.
4040	The Gateway <code>ident</code> service port, used by the Software Repository Cache.

DCAA Satellite - Installation Procedure

The installation procedure for a DCAA appliance satellite is similar to the one used for a "Satellite with a Single Core" topology described in the *SA Installation Guide*.

Phase 1: Prerequisites

Before starting the installation, make sure the machine where the satellite will be installed meets the prerequisites. In order to verify them, run the following command on the machine:

```
<distro_path>/dcaa-sat_osprov/disk001/opsware_installer/prereq/preinstall_requisites.sh satellite
```

Phase 2: Preparation

1. Copy and move the following three files from the appliance to the satellite machine:

- **crypto db:** from this location:

```
/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e (in the same folder on the satellite)
```

- **cdf file:** from this location:

```
/var/opt/opsware/install_opsware/cdf/cdf.xml
```

- **security.conf:** from this location:

```
/etc/opt/opsware/crypto/security.conf (in the same folder on the satellite)
```

2. Mount the folder containing the satellite installation media (`dcaa-sat_osprov`) or copy it on the host where the satellite will be installed.

Phase 3: Installation Procedure: Install the Satellite

- Invoke the installer from the satellite distro with the cdf file as an argument:

```
<distro_path>/dcaa-sat_osprov/disk001/opsware_installer/hpsa_add_satellite.sh -c  
<i.e. path_to_cdf_file >
```

- There are two types of satellites that can be installed: Base Satellite and Satellite with OS Provisioning support.

To install only the Base Satellite version; in the Host/Component Layout, assign a host only to the Satellite component.

When installing the Satellite with OS Provisioning support, the components can be split on multiple machines (i.e. each component can reside on a different host), in which case, the hosts must be added at the beginning of the interview. Use the <p> key to go to the previous screen.

- **Base Satellite** (Satellite Gateway + Software Repository Cache) - allows server management at a smaller remote site
- **Satellite with OS Provisioning** (Base + OSProv Media and Boot components) - allows additional server management and installation of an OS on servers
- Complete the interview. You can use the default values provided, except:
 - *word.store.host* – this needs to be the IP of the satellite Software Repository Cache (i.e. the satellite's IP address if you are installing everything on one machine)
 - *satellite.dcnm* – you need to input the *facility* name

NOTE: If you have changed the password of the *SA user admin* from the default password, you must use the **Advanced Interview** and provide the new *admin* password when asked for the parameter *cast.admin_pwd*.

- Install the components

On the first screen you will be asked to provide all the hosts on which the satellite components will be installed

```
Specify Satellite hosts:  
=====
```

```
Currently specified hosts:
```

```
192.168.1.10
```

```
Please select one of the following options:
```

1. Add/edit host(s)
2. Delete host(s)

Next you will be asked to assign the components to the hosts:

```
Host/Component Layout  
=====
```

1. Satellite
2. OS Provisioning Boot Server
3. OS Provisioning Media Server

```
Enter the number of the component or one of the following  
directives
```

```
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Select each component from the list and then select the host on which to install it. After each component has a host assigned you will have a screen similar to the one below:

Host/Component Layout

=====

1. *Satellite [192.168.1.10]*
2. *OS Provisioning Boot Server [192.168.1.10]*
3. *OS Provisioning Media Server [192.168.1.10]*

Enter the number of the component or one of the following directives

*(<c>ontinue, <p>revious, <h>elp, <q>uit): **c***

Select which type of interview you wish to run. The **Advanced Interview** allows for more customizations to be made, while the **Expert Interview** will present all the parameters. Most of the parameters also have default values which will be presented after the parameter's description; press **<Enter>** to accept the default value. For parameters that will not be presented in the interview, the installer will use the default values.

NOTE: It is mandatory to use the **Advanced Interview** if the password for the SA "admin" user was changed.

Interview Type

=====

1. *Simple Interview*
2. *Advanced Interview*
3. *Expert Interview*

Enter the option number or one of the following directives

*(<p>revious, <h>elp, <q>uit): **1***

Provide values for the requested parameters. See the '[Appendix A: Parameter Reference](#)' in this document.

Once the all the parameters have values, choose to continue. The installer will run the prerequisite checker and then the installation process will begin.

Phase 4: Post-installation Tasks

Once the satellite installation completes successfully:

- Add permissions on the satellite facility to the desired user groups. Permissions to **SuperUsers** group must be granted so that the servers managed through the satellite can be accessed from the **Operator Portal**.
- Check that the satellite gateway appears in Administration > Gateway
- Configure DHCP if using OSprov provisioning.

Uninstalling Satellites

Uninstallation

In order to uninstall a satellite, there are 2 steps that need to be performed:

1. [Decommission the satellite facility](#)
2. [Invoke the uninstaller](#)

1. Facility decommission

- First, deactivate agents registered in the facility, including the agent installed on the satellite host(s). This can be accomplished by deactivating them in the SA client or uninstalling the agent from the managed servers.
- In the SA client; select **Devices > All Managed Servers**. You can select all the servers that are registered to the satellite facility that are to be uninstalled, then **right click** and select **Deactivate SA agent**. **NOTE:** This does *not* uninstall the agent from those hosts.
- Detach customers currently attached to the facility. In **Administration > Facilities**, **double click** the **Satellite Facility** and in the **Properties** view, then **remove** the customers from the list.
- Finally, decommission the facility. In **Administration >** select **Facilities**, **right click** the satellite facility and select **Decommission**.

2. Invoke the uninstaller

- First, on the satellite (or the host where the boot server was installed), run this command:

```
— umount /opt/opsware/boot/tftpboot/hdt
```

- Then, invoke the uninstaller:

```
<media_path>/ dca-sat_osprov /disk001/opsware_installer/uninstall_opsware.sh -  
r /var/opt/opsware/install_opsware/resp/resp.<timestamp>
```

Select all the components to uninstall:

```
Welcome to the Opware Installer.  
Please select the components to uninstall.  
1 ( ) OS Provisioning Media Server  
2 ( ) OS Provisioning Boot Server  
3 ( ) Satellite  
Enter a component number to toggle ('a' for all, 'n' for none).  
When ready, press 'c' to continue, or 'q' to quit.
```

Note: if the satellite components were installed on separate hosts, you must uninstall them in the order shown above. Invoke the uninstall process on the OS Provisioning hosts first, and then invoke the uninstall process on the machine hosting the Satellite component.

- Next, you will be asked if you also want to remove all the software packages and the cryptographic material. You need to provide the following answers:

```
Parameter 1 of 2 (word.remove_files) is missing or invalid -  
Are you absolutely sure you want to remove all packages in the  
repository? (y/n): y  
Validating... OK.
```

```
Parameter 2 of 2 (save_crypto) is missing or invalid -  
Would you like to preserve the database of cryptographic  
material? (y/n): n  
Validating... OK.
```

- You will be asked to provide a filename where these answers will be saved for future reference.
- Finally, the uninstallation process will begin.

Chapter 4 Satellite Administration

This section describes basic SA Satellite topologies and concepts and the following administrative tasks:

- [Starting/Restarting a Satellite](#)
- [Stopping a Satellite](#)
- [Verifying Satellite Communication with the Primary Core](#)
- [Permissions Required for Managing Satellites](#)
- [Viewing Satellite Information](#)
- [Viewing Gateway Diagnostic and Debugging Information](#)
- [Identifying the Source IP Address and Realm for a Connection](#)
- [Changing the Bandwidth Usage or Link Cost Between Gateways](#)
- [Viewing the Gateway Log or Change the Log Level](#)
- [Restarting or Stopping a Gateway Process](#)

Starting/Restarting a Satellite

To *start* a Satellite, issue the following command:

```
/etc/init.d/opsware-sas start
```

To *restart* a Satellite, issue the following command:

```
/etc/init.d/opsware-sas restart
```

Note: If the Satellite Agent fails to restart (typically due to an NFS error blocking the availability of port 1002, which is required for Satellite Agent communication), restart the Satellite host or temporarily disable the service that is blocking 1002, restart the agent, then restart the blocking service.

Stopping a Satellite

To stop a Satellite, issue the following command:

```
/etc/init.d/opsware-sas stop
```

Verifying Satellite Communication with the Primary Core

To verify that the Core Management Gateway is communicating with the Satellite, perform the following steps:

1. **Log in** to the SA Client as a member of a user's group that has the **Manage Gateway** permission.
2. From the **Navigation** panel, click **Administration > Gateway**.
3. Verify that the upper left corner of the **Manage Gateway** page displays a link for the new **Satellite**.

If the **Manage Gateway** page does not display the link for the **Satellite**, you may need to edit the Satellite's properties. The full path name of the properties file is:

```
/etc/opt/opsware/opswgw/opswgw.properties
```

After modifying the properties file, you must restart the Satellite:

```
/etc/init.d/opsware-sas restart opswgw
```

4. **Log in** to the **SA Client** as a member of a user's group that has the Read (or Read & Write) permission on the Satellite's facility.
5. From the **Navigation** panel, click **Devices > All Managed Servers**.
6. Verify that the satellite host appears in the managed server list.

For further information, see also "*More Troubleshooting Server Communication Tests*" in the *SA User Guide: Server Automation*.

Permissions Required for Managing Satellites

To manage SA gateways, you must have the **Manage Gateway** permission. By default, this permission is included in the SA System Administrators group. To view facility information, you must have Read (or Read & Write) permission for the specific facility.

For more information about user groups and SA permissions, see the *Appendix A, Permissions Reference* section in the *SA 10.2 Administration Guide*, which you can access using the [Appendix C: SA Documentation Library](#) in this guide.

Viewing Satellite Information

This section discusses the following topics:

- [Viewing Satellite Facilities and Realms](#)
- [Viewing the Realm of a Satellite Managed Server](#)
- [Viewing and Managing Satellite Gateway Information](#)

Viewing Satellite Facilities and Realms

You can view the core and satellite facilities by selecting the **Administration** tab in the SA Client, then selecting **Facilities**. Select a facility, then select the **Realms** view to see the realms associated with the facility, including the bandwidth between realms in the facility.

For more information on facilities, see [Facility Administration](#).

Viewing the Realm of a Satellite Managed Server

When installed in a Satellite configuration, SA can manage servers with overlapping IP addresses. This situation

can occur when servers are behind NAT devices or firewalls. Servers with overlapping IP addresses *must* reside in different Realms.

When retrieving a list of servers resulting from a search, you might see multiple servers with the same IP address but in different Realms. You might also see multiple servers with the same IP address when you are planning to run a custom extension and you are prompted to select the servers on which to run the extension.

The Properties view of a server in the SA Client displays additional information that identifies the server corresponding to the IP address.

Viewing and Managing Satellite Gateway Information

To view satellite gateway information, in the SA Client navigation panel, select the **Administration** tab, then select **Gateway**. This displays the gateway status, as shown in Figure G. From the list of gateways on the left, select the gateway you want to view. Select the specific gateway information you want to see from the links across the top of the page.

Figure G. Gateway Status

The screenshot shows the 'Manage Gateway' interface. On the left, a list of gateways includes 'cgw0-C28', which is selected. The main content area displays the following information:

- Gateway Summary:** Gateway: cgw0-C28, Realm: C28, Host: true, Version: 1.8.22/1.5, Uptime: 366:11:00
- Navigation Links:** Status, Files, Routing, Param, L3DB, Config, History, Ident, Bandwidth, Link Cost, Logging, Process Control
- Gateway Statistics Table:**

Gateway	Cost	BWLimit Kbits/sec	Send BW Kbits/sec	Recv BW Kbits/sec	Total In Bytes	Total Out Bytes	Payload In Bytes	Payload Out Bytes	Age	Peer
cgw0-C28	1	0	3.21	1.03	382167107	45308297	314805635	395777686	3:5:36:5.45	192.168.196.244:54397
alice	10	0	1.58	1.23	39021616	56995009	30486969	43993609	3:6:6:8.40	192.168.9.50:41128
cgw0-C28	1	0	1.58	0.00	26469755	62224516	25923838	48682818	3:5:5:25.80	127.0.0.1:50991
- Endpoint Table:**

Endpoint	Resolved	Connected	Cost	BWLimit
002:128	0/0:1024	0/0:048	0/0:1024	0/0:1024
0:10:39:57.83	0:2:42:4.43	0:17:43:34.38	3:5:40:20.78	
- Route Table:**

Route	Balance	Resolve	Connect	Discard
002:128	0/0:1024	0/1:1024	0/1:1024	0/1:1024
0:10:38:21.82	3:6:6:11.64	0:1:22:24.84	0:1:22:24.84	3:5:40:9.23
- MsgProcessor Table:**

0/1:1024	0/1:1024	0/1:1024	1/1:1024	0/4:1024	0/1:1024	0/4:1024	0/4:1024
2:20:42:28.67	2:29:41:55.24	2:29:42:20.74	2:20:40:34.26	2:20:40:9.62	2:20:43:18.69	2:20:49:35.56	2:20:42:28.67
- DataMover Queue Table:**

Active Queues	Total Queued Packets	Total Queued RAM
0	0	0:00 Bytes
- Performance Metrics Table:**

TAC	TCC	FAC	PAC	POC	ACC	POC	UAC	UCC	UOC
2	3	2	1	1	0	6	8	5	0

Use the gateway status for the following tasks:

- Obtain status information about gateways and the tunnels between gateways.
- This can be useful for debugging gateways.
- Change the bandwidth limits or tunnel cost between gateway instances.

- Restart Gateway processes.
- Change the logging levels for gateway processes.

Viewing Gateway Diagnostic and Debugging Information

1. In the **SA Client**, select the **Administration** tab, then select **Gateway**.
2. From the list of gateways on the left, select the gateway for which you want to view information. This displays the following **Status** for the selected gateway:

A table of **Active Tunnels**, including:

- Tunnel Cost
- Bandwidth Constraints
- Bandwidth Estimates
- Age of the tunnels
- Information about the internal message queues. Each column in the table for a queue displays data in this format:
 - Number of messages in the queue
 - The message high-water mark for the queue
 - Maximum value configured for the queue
 - The last time the message high-water mark was attained for the queue. You can use the time stamp indicating when the message high-water mark was last reached to troubleshoot gateway issues. The time stamp is displayed in the format: DD: HH:mm:ss.

To view the details and statistics for a tunnel between gateways, select the link for the gateway that *terminates* the tunnel, as **Figure H** shows. This displays the tunnel details and statistics.

Figure H. Manage Gateway — Status Page

The screenshot shows the 'Manage Gateway' interface. On the left, a list of gateways includes gw2-nat1, Planet10, Purple11, Swing02, gw2-nat2 (selected), and ThereYouAre. The main area displays the status for gw2-nat2, including Gateway, Realm, Root, Version, and Uptime. Below this is a table with tabs for Status, Flows, Routing, PathDB, LSDB, Config, History, Ident, Bandwidth, and Link C. The table has columns for Gateway, Cost, BWLimit (Kbits/sec), Send BW (Kbits/sec), Recv BW (Kbits/sec), Total In Bytes, and T. The 'gw1-nat2' entry in the Gateway column is circled in red.

Gateway	Cost	BWLimit Kbits/sec	Send BW Kbits/sec	Recv BW Kbits/sec	Total In Bytes	T
gw1-nat2	1	0	0.00	0.83	686578431	24

1. To view the following pages containing diagnostic information, select one of the following links across the top of the page:
 - **Flows** displays information about all open connections for the selected gateway.

- **Routing** displays the inter-gateway routing table. This table shows which tunnel will be used to reach another gateway in the mesh. The routing table is computed from the data in the path database. The routing computation automatically updates when the link cost for a connection is changed.

Note: When a tunnel collapses, by default, routing information is retained in the routing table for two minutes to provide continuity for the mesh.

- **PathDB - Path Database** displays the route with the lowest cost to all reachable gateways in the mesh. SA determines the lowest cost route to all reachable gateways from the data in the Link State database.
- **LSDB - Link State Database** contains information about the state of all tunnels from the perspective of each gateway instance. The LSDB contains the data for all tunnels and the bandwidth constraint for each tunnel.
- **Config** displays the properties file for the selected gateway, including the path to the properties file on the server running the gateway component. Below the properties values, the page contains crypto file information and the mesh properties database. The **Properties Cache** field is above the properties values. When you change the bandwidth or link cost for a connection between gateways, the updated value appears in this field if the update was successful.
- **History** displays historical information about the inbound (ingress) and outbound (egress) connections between hosts using the gateway mesh. For example, when exactly host A in Realm A connected to host B in Realm B.

Identifying the Source IP Address and Realm for a Connection

The **Ident** link provides an interface to the real-time connection identification database. If necessary, contact HP Support for additional information about how to run this tool.

1. In the SA Client, select the **Administration** tab, then select **Gateway**.
2. Select the link **Ident**. This displays the real-time connection identification database.
3. In the edit box, enter the protocol and source port for an active connection, separated by a colon; for example, TCP: 25679.
4. Select the **Lookup** button. This displays the client **Realm** and client **IP address**, which is where the connection came from.

Changing the Bandwidth Usage or Link Cost Between Gateways

The **Edit** link lets you modify the link bandwidth constraint, the link cost, and the load balance rules.

Note: You must apply any bandwidth changes between gateways on core gateways only. Changes made on other gateways will not take effect.

1. In the SA Client, select the **Administration** tab, then select **Gateway**.
2. To specify a bandwidth limit for a connection:
 - a) Select the **Edit** link at the top of the page. This displays the **Modify Link Bandwidth Constraint** control.
 - b) Specify two gateway instance names that are connected by a tunnel.
 - c) Specify the bandwidth limit you want in kilobits per second (Kbps). Specify zero (0) to

- remove bandwidth constraints for the connection.
- d) Click **Apply**.
- 3. To set a link cost for a connection:
 - a) Select the **Edit** link at the top of the page. This displays the **Modify Link Cost** control.
 - b) Specify two gateway instance names that are connected by a tunnel.
 - c) Specify the cost you want in the **Cost** field.
 - d) Click **Apply**.
- 4. To set the load balance rules for a connection:
 - a) Select the **Edit** link at the top of the page. This displays the **Modify Load Balance Rules** control.
 - b) Specify a gateway instance name.
 - c) Specify a load balance rule.
 - d) Click **Apply**.

Viewing the Gateway Log or Change the Log Level

Note: Changing the logging level to `LOG_DEBUG` or `LOG_TRACE` greatly increases the log output of the gateway and can negatively impact the performance of the gateway.

1. In the **SA Client**, select the **Administration** tab, then select **Gateway**.
2. Select the **Logging** link at the top of the page. This displays the end of the gateway log file.
3. To change the logging level, select one of `LOG_INFO`, `LOG_DEBUG`, or `LOG_TRACE`.
4. Select **Submit**.

Restarting or Stopping a Gateway Process

1. In the **SA Client**, select the **Administration** tab, then select **Gateway**.
2. Select the **Process Control** link at the top of the page.
3. To restart the gateway process, click **Restart**.
4. To stop the gateway watchdog and the gateway, click **Shutdown**.

Caution: Stopping a gateway process can cause problems for an SA Core. For example, if you stop a core gateway process, you will stop all traffic to that SA Core and you will be unable to control the gateway from the SA Client.

Requirement: To restart the gateway after stopping it from the SA Client, you must log onto the server running the gateway component and manually restart the process.

Appendix A: Parameter Reference

This appendix lists parameters and requirements needed during installation.

Depending on the interview level you choose (simple, advanced), you will be prompted to supply the following parameter information during the installation process as shown in [Table 5](#).

Table 5 Required Parameter Information

Parameter	Requirement	Description
truth.oaPwd	opsware_admin user access	The opsware_admin password. Default: -the value is extracted from the provided cdf
decrypt_passwd	Accessing Core cryptographic material	The password required to access the Core's cryptographic material. Default: -the value is extracted from the provided cdf
cast.admin.pwd	SA Administrator's access	The SA_admin user's password Default: -the value is extracted from the provided cdf
word_root	Package Repository location	The root directory for the Package Repository. Default: /var/opt/opsware/word
word_tmp_dir	Software Repository	Directory where Package Repository will temporarily place content during uploads. Default: /var/opt/opsware/wordbot_tmp/
word.store.host	Software Repository	The host name of the NFS server where Software Repository Cache is stored. Usually this is the IP of the host where the Satellite component is installed.
agw_proxy_port	Gateway configuration	The port on which Agents can contact the Agent Gateway to request connections to core components Default: 3001
opswgw.ConfigPort	Bandwidth configuration	The gateway Bandwidth Configuration Management port. Default: 8086
opswgw.BwUsageChannelPort	Bandwidth configuration	The gateway bandwidth usage channel port. Default: 8084
opswgw.AdminPort	Gateway configuration	The port for the administrative interface of the Gateway Default: 8089
satellite.gateway.ConnectType	Gateway configuration	The Satellite Gateway Connect Type. Options are 1 or 3. Default: 1

<code>media_server.linux_media</code>	Linux media location (OS Provisioning)	The pathname to the Linux media. Default: <code>/media/opsware/linux</code>
<code>media_server.sunos_media</code>	Solaris media location (OS Provisioning)	The pathname to the Solaris media. Default: <code>/media/opsware/sunos</code>
<code>media_server.windows_media</code>	Windows media location (OS Provisioning)	The pathname to the Windows media. Default: <code>/media/opsware/windows</code>
<code>media_server.windows_share_name</code>	Windows Media location (OS Provisioning)	The share name to use for the Windows media sharing server (Note: share names that are longer than 8 characters may give errors while browsing or may not be accessible to some older clients.) Default: <code>OSMEDIA</code>
<code>media_server.windows_share_password</code>	Windows Media location (OS Provisioning)	The password to write-protect the Windows media share. <code>Import_media</code> tool will prompt for this password each time it is run.
<code>satellite.host_ip</code>	Gateway configuration	Satellite Gateway host's IP address
<code>satellite.dcNm</code>	The Satellite Facility identification	The name of the new Satellite's facility.
<code>satellite.realm_name</code>	The Satellite Realm name	The name for the Satellite's realm (name cannot contain spaces). WARNING: If this is the first Satellite you are adding to this Satellite Facility, please provide the satellite facility name (value of the <code>satellite.dcNm</code> parameter) as the realm name. <i>Not doing so will result in a misconfigured Satellite.</i>
<code>satellite.gateway_name</code>	The name for a new or existing Satellite Gateway (name cannot contain spaces)	The name of the Gateway the Satellite will use for communications with the Primary Core management Gateway or other Satellite Gateways (in a cascaded Satellite topology).
<code>satellite.proxy_port</code>	The port used by Agents to contact the new Satellite.	The port number on which agents can contact the Satellite Gateway. Default: 3001
<code>satellite.parentgw_ip</code>	A Core Management Gateway IP address	The IP address of a server running a Management Gateway. This must be the IP of the DCAA appliance

<p>satellite.parentgw. tunnel_listener_port</p>	<p>The Management Gateway's listener port</p>	<p>The port number through which tunnel connections to the Management Gateway will pass. The Management Gateway listens on this port for connection requests from the Satellite.</p> <p>In the Management Gateway Properties File, this port specified with the <i>opswgw.TunnelDst</i> parameter.</p> <p>The path to the Core's Gateway Properties file is: <i>/etc/opt/opsware/opswgw-mgw0-<facility>/opswgw.properties</i></p> <p>Default: 2001</p>
<p>satellite.parentgw. proxy_port</p>	<p>The port on which a Core's Management Gateway listens for connection requests.</p>	<p>The port number on which a Core's Management Gateway listens for connection requests from Satellite Gateways to SA Core Components (default 3003), or the port on which a Satellite Gateway listens for connection requests from other Satellite Gateways to SA Core Components (cascading Satellite links) (default 3001).</p> <p>Default: 3003</p>
<p>agent_gw_list_args</p>	<p>Agent- Gateway communications</p>	<p>The list of Gateways on which the Satellite's agent will be installed.</p> <p>Specified by the IP address and port number (ip:port) on which Agents can contact the Gateway in the Satellite facility.</p> <p>Default: <satellite_gateway>:3001.</p>

Appendix B: HP DCAA Doc Library

Table 6: DCAA 1.00 DOC LIBRARY

Tasks	Document Name	Link to Doc
Get started with DCAA, understand the IT Operator persona, components, and concepts for Express Edition users	DCAA 1.0 At a Glance Guide – Express Edition	go
Get started with DCAA, understand the IT Operator persona, components, and concepts for Premium Edition users	DCAA 1.0 At a Glance Guide – Premium Edition	go
How to install DCAA, Admin tasks	DCAA 1.0 Installation and Administration Guide	go
IT Operator Persona, Using DCAA UI	DCAA 1.0 Users Guide – Express Edition	go
IT Operator Persona, Using DCAA UI	DCAA 1.0 Users Guide – Premium Edition	go
Bugs and Fixes	DCAA 1.0 – Release Notes	go
Platform Support, Compatible products with DCAA	DCAA 1.0 – Support and Compatibility Matrix	go
See the full HP DCAA Documentation set	Documentation Library List	go

Appendix C: HP SA Doc Library

Table 7: HP SA Doc Library

Tasks	Document Name	Link to Doc
Contains information about downloading and applying patches to Linux, Windows, and Solaris systems.	Users Guide: Server Patching	GO
Contains information about SA Satellite Installations.	HP SA 10.2 Installation Guide	GO
Contains information about SA Satellites and advanced SA Architecture and topologies.	HP SA 10.2 Overview and Architecture Guide	GO
Contains information about installing and managing SA Server Agents.	User Guide: Server Automation	GO
Contains information about SA permissions and user groups.	SA 10.2 Administration Guide	GO
See the full HP SA Documentation Set	All Manuals Download - SA 10.20	GO