Server Automation

Software Version: 10.60

Install Guide

Document Release Date: May 24, 2017
Software Release Date: May 24, 2017

Hewlett Packard
Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise 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 Hewlett Packard Enterprise 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

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.

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: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

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

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE 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 website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE 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 HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Contents

Install

This section describes all necessary SA Core installation prerequisites and provides useful pre- and post-installation information, tasks and options.

It also provides the requirements and procedures for standard and advanced installations of:

- **Single-Host SA Cores and Multi-Host SA Cores**

  For small facilities, a single-host SA Core has all its core components installed on a single server. An SA Core can also be installed with its core components distributed between multiple host servers for scalability.

- **SA Primary Core with Secondary SA Cores (Multimaster Mesh)**

  For larger facilities, an SA Core, single- or multi-hosted, can act as the Primary Core of a Multimaster Mesh when you install Secondary SA Cores. The Primary and Secondary Cores manage the servers in their respective facilities as well as enable centralized administration of all facilities in the Mesh.

  - **SA Satellites**

    A Satellite installation is typically installed for remote sites that do not have a large enough number of potential SA Managed Servers to justify a full SA Core installation. A Satellite installation allows you to install only the minimum necessary Core Components on the Satellite host which then accesses the Primary Core’s database and other services through an SA Gateway connection.

- **Multi-Core configurations (Advanced - requires HPE Professional Services)**

  For very large facilities, SA Cores can be configured to communicate with each other across facilities adding scalability and failover capabilities. Such configurations are supported only for HPE Professional Services or certified consultant installation. Customer installation is not supported.

  "Customer installable SA Core configurations" describes the SA Core configurations supported by HPE for customer installation. For advanced and complex installation, contact HPE Professional Services or HPE-certified consultants.

> **Note:** If you are not familiar with the data center tasks that SA automates or want to be familiar about the architecture of an SA Core and its components, see the SA 10.60 Get started Guide.

Preinstallation tasks

This section describes all the tasks that must be performed before installing SA:

Topic	Description
"System requirements for installation " below	List of required hardware, software, and network that you must verify for SA Core host servers, agents, and satellites.
"Prepare the environment" on page 39	Information required to help you plan the SA configuration required for your facility.
"Important SA installation information" on page 54	Information you must know before start installing SA in your facility.

> **Note:** Upgrading a Mesh to version 10.60 after a CORD patch rollback fails if the *crypto.hash_algorithm*, *fips.mode* or *crypto.key_length* parameters do not have the default values.

System requirements for installation

This section describes hardware, software, and network requirements that you must verify for SA Core host servers, agents, and satellites.

Supported operating systems for SA Core hosts and Managed Servers are detailed in the SA 10.60 Support and Compatibility Matrix.

> - You must verify that your SA Core and satellite host servers meet the requirements listed in this section. If you do not, your installation may fail or core performance may be affected.
> - The disk hardware needs to be the same on all the core components.
> - The disks in `/var/opt/opsware/vault/omb` and the database disks are required to have the same speed.

There may be additional installation prerequisites. See the release notes for this SA version.

This section covers the following prerequisites:

Prerequisite checklist

Task	Status (Done/Not Done)
"Transfer installation files to a local disk"	
"Verify the operating system"	
"Verify Oracle requirements"	
"Verify Veritas File System (VxFS) requirements (optional)"	
"Verify the NFS services configuration"	
"Checking the free disk space requirements"	
"Check network requirements"	
"Checking Slice Component requirements" on page 24	
"SA Installer Prerequisite Checker"	
"Download and install Windows patch management files (optional)"	
"Check the SA Global File system (OGFS) requirements"	
"Check the Core host(s) time and locale requirements"	
"Installing the Windows Update Service "	
"Checking the user and group requirements "	
"Check SA Cores on VMs requirements (optional)"	

Transfer installation files to a local disk

HPE recommends that you copy the contents of the SA media to a local disk or to a network share and run the Installer from that location. See "Mounting the SA installation media".

Verify the operating system

For a complete list of all supported platforms for SA Cores hosts, Agents (managed servers), and Satellites, see the SA Support and Compatibility Matrix document.

> In an SA Core, all the servers that host a core’s components must be running the same operating system. Different update levels are supported on hosts within the same core. In a multiple core

> mesh, each distinct core can be run under a different operating system but all hosts in each distinct core must be running the same operating system.

Verify Oracle requirements

The Model Repository requires an installed Oracle database. You can either use the SA-supplied Oracle database or an Oracle database that you have installed. However, that database must be up and running before you begin the SA installation. For detailed information about the required database configuration, see"Oracle setup for the Model Repository" on page 100.

Verify Veritas File System (VxFS) requirements (optional)

SA supports the Veritas File System (VxFS) for Red Hat Enterprise Linux 5 and 6 x86_64. VxFS is not supported for any other operating systems. If you attempt to install SA components on a non-supported operating system running VxFS, the installation will fail and will need to be backed out. The SA Installer Prerequisite Checker validates VxFS for SA Cores and satellites and if prerequisites are not met, the installation will fail before SA is installed. VxFS is not validated for Oracle hosts, therefore, if Oracle is installed on the same host as SA Core Components, the Oracle installation may succeed and the SA Core installation subsequently fails. For the latest supported operating systems, see SA Support and Compatibility Matrix.

Verify the NFS services configuration

NFSv2 and NFSv3 must be enabled and NFSv4 must be disabled to support mounting file systems (**MOUNTD**). You must also configure the NFS/RPC server ports that are assigned.

> NFSv4 is enabled by default for Red Hat Enterprise Linux, SUSE Linux Enterprise Server.

- "NFS services configuration" on the next page
- "Configuring NFS/RPC server ports" on the next page
- "Restarting the NFS service" on page 12

NFS services configuration

Perform the following tasks based on your operating system.

- **Red Hat Enterprise Linux**

  If NFSv2 and NFSv3 are not enabled, you must modify the value of the following parameters as "**yes**" in the **/etc/sysconfig/nfs** folder:

  ```
  MOUNTD_NFS_V2=yes
  ```

  ```
  MOUNTD_NFS_V3=yes
  ```

  To disable NFSv4 support for nfsd, add the following parameter in the **/etc/sysconfig/nfs** folder.

  ```
  RPCNFSDARGS="--no-nfs-version 4"
  ```

  - **SUSE Linux Enterprise Server**

    In SUSE Linux Enterprise Server, NFSv2 and NFSv3 are enabled by default. Therefore, you do not need to manually modify the **MOUNTD** parameters in /etc/init.d/nfsserver.

    To disable NFSv4 support for nfsd, add the following parameter in the **/etc/sysconfig/nfs** folder:

    ```
    NFS4_SUPPORT="no"
    ```

Configuring NFS/RPC server ports

For a list of ports used by SA, see "Required open ports". Perform the following tasks based on your operating system:

- **Red Hat Enterprise Linux**

  Add or enable the following parameters in **/etc/sysconfig/nfs**:

  ```
  MOUNTD_PORT=<choose a non-SA port number>
  LOCKD_TCPPORT=<choose a non-SA port number>
  LOCKD_UDPPORT=<choose a non-SA port number>
  STATD_PORT=<choose a non-SA port number>
  STATD_OUTGOING_PORT=<choose a non-SA port number>
  ```

  If you have **rquotad** enabled, enable this parameter in **/etc/sysconfig/nfs**:

  ```
  RQUOTAD_PORT=<choose a non-SA port number>
  ```

- **SUSE Linux Enterprise Server**
  - For **MOUNTD** parameters, modify or add this parameter in **/etc/sysconfig/nfs**:

    ```
    MOUNTD_PORT=<choose a non-SA port number>
    ```

  - For **lockd** parameters, create or edit **/etc/modprobe.d/lockd** and add the following:

    ```
    options lockd nlm_udpport=<choose a non-SA port number>

    nlm_tcpport=<choose a non-SA port number>
    ```

  - For **statd** parameters, if the parameters are installed and running, edit **/etc/init.d/nfsserver**, search for "`startproc /usr/sbin/rpc.statd`" and append the **-p** parameter for specifying a non-SA port.

    For example:

    ```
    startproc /usr/sbin/rpc.statd --no-notify -p<choose a non-SA port number>
    ```

  - For **rquotad** parameter, if the parameter is already installed and running, edit **/etc/services** and add or edit TCP/UDP ports for **rquotad**.

    For example:

    ```
    rquotad <choose a non-SA port number>/tcp

    rquotad <choose a non-SA port number>/udp
    ```

Restarting the NFS service

After the required changes are made, restart the NFS server service:

- **Red Hat Enterprise Linux**

  ```
  /sbin/service nfs restart
  ```

- **SUSE Linux Enterprise Server**

  ```
  /sbin/service nfsserver restart
  ```

Checking the free disk space requirements

This section describes the free disk space (in addition to the operating files system) requirements for any SA Core Server, database, software repository, and media server:

- "Core server disk space requirements" below
- "Model Repository (Database) disk space requirements" on page 15
- "Software repository disk space requirements" on page 16
- "Media server disk space requirements" on page 16

Core server disk space requirements

If you are not using separate partitions for the directories listed below, make sure that the root directory has at least 72 GB free hard disk space on each Core server. This does not include the file system needs of the operating system. SA components are installed in the `/opt/opsware` directory.

The following table lists the recommended free disk space requirements for installing and running SA Core components. These sizes are recommended for primary production data. Calculate additional storage for backups separately.

Disk space requirements

SA Component Directory	Recommended Free Disk Space	Requirement Origin
/etc/opt/opsware	50 MB	Configuration information for all SA Core services. (Fixed disk usage)
/media *****	15 GB	**SA Provisioning**: The media directory holds the OS installation media that is shared over NFS or CIFS. The initial size for this directory depends on the total size of all OS installation media sets that you plan on provisioning, such as Windows Server 2012 R2 (8 GB) and RHEL 7 (4 GB). The network OS install shares do not need to reside on SA core systems and are typically dispersed across multiple servers as the Multimaster Mesh grows. (Bounded disk usage that grows quickly in large increments)
/opt/opsware	25 GB	The base directory for all SA Core services. (Fixed disk usage)
/u01/app/oracle /u02/app/oracle /unn/app/oracle ...	10 - 20 GB 19 - 20 GB 19 - 20 GB	For an SA installed Oracle RDBMS, /u01 contains the Oracle software files. /u02 - /u*nn* contains the Oracle tablespace

Disk space requirements, continued

SA Component Directory	Recommended Free Disk Space	Requirement Origin
		directory that contains all model and job history information. Known sizes range from 5 GB to 50 GB of space, depending on the frequency and type of work, the amount of software and servers managed, and the garbage collection frequency settings. (Bounded disk usage that grows slowly in small increments)
/var/log/opsware	80 GB	The total log space used by all SA Core Components. (Fixed disk usage)
/var/opt/opsware/	30+ GB	The total run space used by all SA Core Components, including instances, *.pid files, *.lock files, and so on. Variable disk usage - some package importers can increase the recommended 30 GB requirement. This is because the Package Repository temporary directory requires a significant amount of space for Windows and Solaris 10 patching uploads. By default, the Package Repository temporary directory is available at `/var/opt/opsware/wordbot_tmp` and configurable in `/etc/opt/opsware/mm_wordbot/mm_wordbot.args`. HPE recommends that you add another 25 GB for each Windows and Solaris 10 patching solution used.
/var/opt/opsware/word **+**	80 GB	(*Infrastructure host only*) The total run space used by all SA Core Components, including instances, *.pid files, *.lock files, and so on. (Fixed disk usage)
/var/opt/opsware/word * **+**	80 GB	(*Infrastructure host only*) The total disk space used by software that is imported into SA. Theoretically, this is infinite disk usage depending on how much software you import. Initial size calculation is based on the total size of all packages and patches that you want managed by SA. Known sizes range from 10 GB to 250 GB.

Disk space requirements, continued

SA Component Directory	Recommended Free Disk Space	Requirement Origin
		This directory does not require any additional space on the slice hosts. This is because the slice hosts access the directory through NFS.
/var/opt/opsware/ogfs/export/store **+**	20 GB	The home directory for the Global File System (OGFS) enabled SA user accounts.

> *The entries marked with an asterisk are directory path defaults that you can change during the installation process. The recommended disk space for these directories is based on average-sized directories, which could be smaller or larger, according to usage.

> +All installed Slices Component bundle hosts will remotely NFS mount these file systems.

> For performance reasons, you should install the SA Components on a local disk, not on a network file server. However, for the Software Repository, you can use a variety of storage solutions, including internal storage, Network Attached Storage (NAS), and Storage Area Networks (SANs).

Model Repository (Database) disk space requirements

Additional disk space is required for the Oracle software and the Model Repository data files. The storage requirements for the database grow as the number of managed servers grows.

As a benchmark figure, you should allow an additional 3.1 GB of database storage for every 1000 servers in the facility that SA manages. When sizing the tablespaces, follow the general guidelines described in the table below. If you need to determine a more precise tablespace sizing, contact your technical support representative.

Tablespace sizes

Tablespace	MB/1000 Servers	Minimum Size
`AAA_DATA`	256 MB	256 MB
`AAA_INDX`	256 MB	256 MB
`AUDIT_DATA`	256 MB	256 MB
`AUDIT_INDX`	256 MB	256 MB

Tablespace sizes, continued

Tablespace	MB/1000 Servers	Minimum Size
LCREP_DATA	3,000 MB	1,500 MB
LCREP_INDX	1,600 MB	800 MB
TRUTH_DATA	1,300 MB	700 MB
TRUTH_INDX	400 MB	400 MB
STRG_DATA	1,300 MB	700 MB
STRG_INDX	400 MB	400 MB

Software repository disk space requirements

The Software Repository contains software packages and other installable files and is part of the Slice Component bundle. A typical SA installation starts with approximately 300 GB allocated for the server hosting the Software Repository. However, more space might be required, depending on the number and size of the packages, as well as the frequency and duration of configuration backups.

Media server disk space requirements

Dependent on your SA Provisioning requirements, this component requires sufficient disk space for the OS media for all the operating system versions you intend to provision.

Check network requirements

This section discusses the network requirements within a facility, open ports required for Core Components, and name resolution requirements. These requirements must be met for Primary Core, Secondary Core, and Satellite installations.

- "Network requirements within a facility" on the next page
- "Required open ports" on page 18
- "Required reserved ports" on page 21
- "Host and service name resolution requirements" on page 22
- "SA Provisioning: DHCP proxying" on page 24

Network requirements within a facility

Before running the Installer, your network environment must meet the following requirements:

- It is recommended that all SA Core Servers be on the same Local Area Network (LAN or VLAN). If cores are placed in different subnets, be aware that there may be performance issues.
- There must be full network connectivity between all SA Core Servers and the servers that the SA Core will manage.
- Core Servers expect user accounts to be managed locally and cannot use the Network Information Service (NIS) directory to retrieve password and group information. During installation of the Core Components, the installer checks for the existence of certain target accounts before creating them. If you are using NIS, this check will fail.
- The Software Repository requires a Linux Network File System (NFS) server.
- When using network storage for Core Components, such as the Software Repository or SA Provisioning Media Server, you must ensure that the root user has write access over NFS to the directories where the components will be installed.
- The speed and duplex mode of the Core’s and Managed Servers’ NIC adapters must match the switch they are connected to. A mismatch will cause poor network performance between the Core and Managed Servers.
- On any given core server, having multiple interfaces which reside on the same subnet is an unsupported configuration. If the slice server has multiple interfaces, the active interfaces MUST reside on separate subnets.
- Firewall/network settings on the SA Core host servers can affect the accessibility of the network ports used for the SA Client, for example, restrictive Linux **iptables** rules. Ensure these operating system/network settings allow required SA Client access.
- If the **net.ipv6.conf.<interface>.disable_ipv6** kernel parameter on an interface is set to 1, then the IPv6 of the respective interface will be disabled. If the kernel parameter on all network interfaces excluding local interface is disabled, then httpsProxy will not start.
- The SA gateway only supports tunneling to port 443. You may need to change the gateway configuration to allow tunneling to other ports if you are:
    - Using iLO on other ports.
    - Integrating with a vCenter server that is on a port other than port 443.
    - Integrating with an OpenStack deployment. In this case, you need to allow tunneling to ports 5000, 8774, and 8776, or to the custom ports for your deployment.

For more information, see the Virtualization Service Tasks section in Virtualization management.

To identify the gateway host, open the **opswgw.args** file from the iLO or virtualization service server. The opswgw.args file is located on the managed server at:

- **UNIX/Linux**: `/etc/opt/opsware/agent`
- **Windows**: `%SystemDrive%\Program Files\Common Files\Opsware\etc\agent`

In this example, your agent gateway name is **opswgw-agws1-TEAL1**:

1. On the gateway host, open the opswgw.custom file.
   The opswgw.custom file is located on the gateway host at:
   - **UNIX/Linux**: `/etc/opt/opsware/opswgw-agws1-TEAL1`
   - **Windows**: `%SystemDrive%\Program Files\Common Files\Opsware\etc\opt\opsware\opswgw-agws1-TEAL1`
2. For each port on which you want to allow tunneling (for example, port 5000), add the following new line:
   ```
   opswgw.EgressFilter=tcp:*:5000::
   ```
3. Save and close the file.
4. Restart the agent gateway component on the gateway host by running the following command:
   ```
   /etc/init.d/opsware-sas restart opswgw-agws
   ```

Required open ports

You must configure any firewalls protecting your Core Servers to allow the ports (shown in the following table) to be open. Note that the ports numbers listed in the table are the default values that can be changed during the installation. Therefore, ensure you are leaving the correct ports open.

Open ports on a firewall protecting an SA Core

Source	Destination	Open Port(s)	Notes
Management Desktops	Slice Component bundle hosts	80, 443, 8080	Required
Direct access to Oracle database (reports, troubleshooting,	Model repository (`truth`) host	1521	Strongly recommended to allow Oracle management

Open ports on a firewall protecting an SA Core, continued

Source	Destination	Open Port(s)	Notes
management)			
Management Desktops	Slice Component bundle hosts	1004, 1018, 1032, 2222, 8061	[Optional] Useful for troubleshooting; ports represent spin, way, twist, tsunami and ogsh (ssh).
SA Core (Management Gateway)	SA Core (Management Gateway)	2001	Required
SA Core (Management Gateway)	SA Core in a different Multimaster Mesh (management gateway)	22, 2003	[Optional] For scp (default word replication, can be forwarded over 2001 connection), backup for 2001 if it is busy.
Slice Component bundles	SA Agents (in same network)	1002	Required (only for the Agent Gateway managing the Agent).
SA Core (Management Gateway)	Satellite/Gateway	3001	Required
SA Core hosts	Mail server	25	Required for email notifications
SA Core hosts	LDAP server	636	Required for secure LDAP access; port can change if you use unsecure LDAP.
SA Agents	SA Core servers and Satellites managing the agent	3001	Required
SA Satellite/Gateway	SA Core	2001	Required
SA Satellite/Gateway	Managed Agents	1002	Required

* Port 1521 is the default Oracle listener (**listener.ora**) port, but you can specify a different port in your Oracle configuration. In case your installation has been modified to use a port other than 1521, you should verify the port number from the Oracle listener status and ensure that your firewall is configured to allow the correct port to be open for the Oracle listener.

> If you have enabled IPTABLES, you must also add exception rules for the paramters, **mountd** (tcp/udp), **portmapper** (tcp/udp) and port 4040.

> SA’s data access layers (infrastructure) use connection pooling to the database. The connections between the database and the infrastructure layer must be maintained as long as SA is up and running. Ensure that your firewall is configured so that these connections do not time out and terminate the connections between the database and the infrastructure layers.

The following table shows the ports used by the SA Provisioning components that are accessed by servers during the provisioning process. (In SA, Provisioning refers to the installation of an operating system on and configuration of managed servers.)

Open Ports for the SA Provisioning components

Port	Component	Service
67 (UDP)	Boot Server	DHCP
69 (UDP)	Boot Server	TFTP
111 (UDP, TCP)	Boot Server, Media Server	RPC (`portmapper`), required for NFS
Dynamic/Static*	Boot Server, Media Server	`rpc.mountd`, required for NFS
2049 (UDP, TCP)	Boot Server, Media Server	NFS
137 (UDP)	Media Server	SMB NetBIOS Name Service
138 (UDP)	Media Server	SMB NetBIOS Datagram Service
139 (TCP)	Media Server	NetBIOS Session Service
445 (TCP)	Media Server	MS Directory Service

* By default, the **rpc.mountd** process uses a dynamic port, but it can be configured to use a static port. If you are using a dynamic port, the firewall must be an application layer firewall that can understand RPC requests that clients use to locate the port for **mountd**.

> Requirements: The SA Provisioning Boot Server and Media Server run various services (such as portmapper and rpc.mountd) that could be susceptible to network attacks. It is recommended that you segregate the SA Provisioning Boot Server and Media Server components onto their own DMZ network. When you segregate these components, the ports should be opened to the DMZ network from the installation client network. Additionally, the Boot Server and Media Server should have all vendor-recommended security patches applied.

The following table shows the Managed Server port that must be open for SA Core Server connections.

Open ports on managed servers

Port	Component
1002 (TCP)	SAAgent

Required reserved ports

The following ports must be reserved for use by SA as they are required by SA components (non-third party).

Reserved ports

SA Component	Port	Secured	Reason
Agent Gateway	8089	Yes	
3001	No	Proxy port	
8017	No	Forward port	
8086	No		
8084	No		
Core Gateway	8085	Yes	
2003	No		
2002	No	Localhost only	
8080	No	Proxy port	
3002	No	Proxy port	
4040	No		
443	Yes		
Management Gateway	2001	Yes	
3003	No	Proxy port	
4434	No	Forward port	
20002	No	Forward port	
Multimaster component (vault)	5678	Yes	
7501	No	Localhost only	
Data Access Engine (spin)	1004	Yes	
1007	No	Localhost only	
Web Services Data Access Engine (twist)	1032	Yes	
1026	No	Localhost only	

Reserved ports, continued

SA Component	Port	Secured	Reason
Command Engine (way)	1018	Yes	
Software Repository (word)	1003	Yes	
1006	No	Localhost only	
Software Repository Accelerator (tsunami)	8061	Yes	
1017	No		
Agent	1002	Yes	
AgentCache	8081	No	
SSHD	2222	Yes	
Command Center (occ)	9080	No	Localhost only
HTTP Proxy	80	No	Proxy port
4433	Yes		Localhost only
81	No	Localhost only	
82	No	Localhost only	
Global File System (spoke)	8020	No	
Deployment Automation (da)	7080	No	
8010	No		
7006	No	Localhost only	
1027	No	Localhost only	
1028	Yes		
1029	No	Localhost only	

Host and service name resolution requirements

SA must be able to resolve Core Server host names and service names to IP addresses through proper configuration of DNS or the /etc/hosts file.

Previous releases

If you plan to install the Core Components on a server that had a previous SA installation, you must verify that the host names and service names resolve correctly for the new installation.

Core servers and host/service name resolution

During the installation, the /etc/hosts file on machines where the *Slice Component bundle* is installed will be modified to contain entries pointing to the *Secondary Data Access Engine*, the *Command Center*, and the fully qualified domain name of the localhost.

All other servers hosting Core Components must be able to resolve their own valid host name and the valid host name of any other SA Core Server (if you will be using a multiple core installation or Multimaster Mesh). A fully qualified name includes the subdomain, for example, `myhost.acct.buzzcorp.com`. Enter the `hostname -f` command and verify that it displays the fully qualified name found in the local **/etc/hosts** file.

In a *typical* component layout, the Software Repository Store is installed as part of the Infrastructure Component bundle and the Slice Component bundle must able to map the IP of the Infrastructure host to its hostname. In a *custom* component layout, the Software Repository Store may be installed separately on any host, therefore the Slice Component bundle must be able to map the IP of that host to its hostname. It is a common practice, but not a requirement, to host the Software Repository Store and the OGFS home/audit directories on the same server.

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,
>
> ```
> 16.77.42.65 (oracle_sas, truth_mm_overlay)
> 16.77.41.24 (infrastructure, word_uploads)
> 16.77.43.252 (slice, osprov)
> 16.77.45.21 (satellite)
> ```
>
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
>
> ```
> 16.77.42.65 hostname1.example.com hostname1
> 16.77.41.24 hostname2.example.com hostname2
> 16.77.43.252 hostname3.example.com hostname3
> ```
>
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

SA Provisioning: DHCP proxying

If you plan to install your SA Provisioning components on a separate network from the Core Components, you must set up DHCP proxying to the DHCP server (for example, using Cisco IP Helper). If you use DHCP proxying, the server/router performing the DHCP proxying must also be the network router so that PXE can function correctly.

The SA Provisioning Boot Server component provides a DHCP server, but does not include a DHCP proxy. For DHCP server configuration information, see "DHCP configuration for SA Provisioning".

Checking Slice Component requirements

The recommended memory requirement for each Slice Component is 6 GB RAM and number of CPUs required for each Slice Component is 4.

SA Installer Prerequisite Checker

SA now performs validation of a minimum baseline requirement for an SA Core installation. This validation is performed automatically by the SA Installer during an SA Core installation. You can also run this check as a standalone utility prior to installation to verify the suitability of a server as an SA Core host before attempting an installation.

- "Prerequisites" below
- "Manual prerequisite check" on the next page
- "Interpreting prerequisite checker results" on page 26
- "Additional Linux requirements" on page 27
- "List of prerequisites validated by Prerequisite Checker " on page 27

Prerequisites

The SA prerequisite check requires the `/bin/sh` Unix shell. If `/bin/sh` is not available, the prerequisite check will not run.

Manual prerequisite check

You can run the SA prerequisite check manually using the instructions in this section.

When you manually run the prerequisite check before the Oracle RDBMS installation, CPU and disk space requirements are validated.

When you manually run the prerequisite check after the local installation of Oracle RDBMS but before SA Core Component installation, the required RDBMS version and patches are validated.

> If the Oracle database is installed remotely, prerequisite testing will extract database access information from the Core Definition File (CDF) of the current core install. If the database is accessible, it will be tested in a remote mode using Oracle's Translation Name Service (TNS). Accessibility depends on the availability of SQL*Plus which is installed as part of the database or as Oracle's InstantClient.

You invoke the prerequisite check from the command line on the server on which you plan to host the SA Core:

1. Locate the **<distro>/opsware_installer/OPSWprereqs-<version>.zip** file.

   where, **<distro>** is the full path to the Product Software (primary) media. Unzipping this file will create a sub-directory, **OPSWprereqs-<version>**, which contains the script **preinstall_requisites.sh**.

2. Run the following command:

   ```
   .../preinstall_requisites.sh <phase> [--upgrade] [--cdf_file=<path>] [--resp_file=<path>] [--verbose | --silent]
   ```

   Prerequisite check script arguments

Argument	Description
<phase>	Specifies an Oracle database validation or SA Core host validation. Valid Values: **Oracle**, **core_inst**, or **satellite**
--upgrade	Specifies an upgrade and suppresses the disk space checks. If not specified, fresh install is assumed and disk space checks are run assuming that no SA components are currently installed.
--cdf_file=<path>	Specifies the path to a valid CDF for the current installation. When specified, certain values that might be specified during the install process are taken from the CDF, such as Oracle installation values.

Prerequisite check script arguments, continued

Argument	Description
--verbose | --debug | --silent	`verbose` or `-- debug` display additional output, `silent` displays no output.

> You must have root privileges to run the script. There is a test to see if the logged in user can create users and groups. Therefore, the user running the SA Prerequisite Check must be capable of creating users and groups, but the current user must be the same user that will be running the installer.

Interpreting prerequisite checker results

When the prerequisite check completes, you see messages similar to the following.

```
Prerequisite Checks
===================
Results for <IP_address>:



        FAILURE Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

        WARNING File system ‘/’ has 29447 MBytes available and 154050 is
                recommended.

        [INFO] Processing on Linux/6Server-X86_64 using /var/tmp/hpsa_
media/               opsware_installer/prereq/Linux_oracle_rqmts.conf

        FAILURE These packages are required but not installed.

                If a version is specified, that version or higher is required.

                PACKAGE ARCH VERSION

                libaio-devel x86_64 0.3.107-10.el6



Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The SA Prerequisite Checker identifies warning and failures. Failures can cause a failed or incomplete installation and must be resolved before continuing the installation. Warnings allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, you can continue the installation.

Additional Linux requirements

For Linux systems, you must adhere to the following requirements:

- You must specify the server’s initial run level as level 3 in the /etc/inittab file.
- For RedHat Enterprise Linux 5 you need to upgrade iproute package to version greater than 2.6.32-10.
- If the server uses Integrated Drive Electronics (IDE) hard disks, you must enable Direct Memory Access (DMA) and some other advanced hard disk features that improve performance by running the following script as a user with root privileges on the server and then reboot the server:

  ```
  # cat > /etc/sysconfig/harddisks << EOF
  USE_DMA=1
  MULTIPLE_IO=16
  EIDE_32BIT=3
  LOOKAHEAD=1
  EOF
  ```

> Note: If the validation finds a requirement that is not met by your server, the installation stops and you must correct the problem before continuing the installation. If a recommended configuration is not met, you will see a warning, but can continue with the installation.

List of prerequisites validated by Prerequisite Checker

The prerequisites that are validated during the check include:

> The prerequisite check requires root privileges and validates both required and recommended items. Required items, such as required packages and Oracle settings, must be corrected if the validation fails, however, if you have business requirements that override recommendations, such as number of CPUs, you can still perform an SA Core installation.

Prerequisites	Validation
Host Physical Characteristics	- Physical memory - Number of CPUs (cores or physical) - IDE disk drive optimizations
Oracle Database -	- Disk space, parameter, tablespace requirements (*existing Oracle installations only*) - Supported Oracle version is installed - Required Oracle patches are installed - Supported operating system configuration - Swap space size - Temp space - User `oracle` defined - The port specified by the `db.port` parameter on remote database hosts is being monitored and accepts connections.
Required Packages	Packages that must be installed. During installation, the SA Installer performs a prerequisite check that includes checking for recommended package version levels. You may see warnings during the check if your installation has earlier versions of these packages. HPE recommends that you upgrade any packages flagged with a warning in order to ensure SA's full functionality. You can continue the SA installation with the earlier packages but may sacrifice the functionality provided by the newer version.
Recommended Packages	Packages that should be installed
Unsupported Packages	Packages that must not be installed
Reserved Ports -	Ports that must be open and available
Disk Space Requirements	Checks that minimum disk space required for installation available (fresh install only)
Operating System Configuration:	- Hostname is resolvable - File system (links maintained, case sensitive) - Ability to create new users and groups - Allocated swap space - Timezone setting (UTC - sets hwclock to match the system clock on Linux systems) and locale (`en_US.UTF-8` or equivalent)

	• NFS versions • No VxFS (SLES only) • Sufficient `temp` space is available • Translations for localhost are available • Verification that no critical file paths contain symbolic links
Validation of non-SA-supplied Oracle installations	If you intend to use an existing Oracle installation rather than the SA-supplied Oracle database, that database must meet the requirements described in "Oracle setup for the Model Repository". When you begin an SA Core installation and an existing database installation, the prerequisite checker will validate the Oracle requirements as well as the core server requirements.

SA Core server validation	After you have initiated an SA Core installation, the installer performs the prerequisite check before installation of the Oracle database and before installation of the SA Core Components. The validation progress is displayed on screen showing the items being validated and the results of the validation. The display during validation will be similar to this:
	`Processing on Linux/4AS-X86_64 using`
	`/tmp/OPSWprereqs-40.0.0.0.54/Linux_oracle_rqmts.conf`
	`Checking 'required' packages for Linux/4AS-X86_64`
	`Checking 'required' patches for LINUX/4AS-X86_64`
	`Checking 'recommended' packages for LINUX/4AS-X86_64`
	`Checking 'absent' packages for LINUX/4AS-X86_64`
	`Testing memory size`
	`Testing for number of CPUs`
	`Testing hostname for FQDN`
	`Testing swap space allocated`
	`Verify timezone is UTC`
	`[...]`
	If the validation indicates that your system does not meet the recommended configuration, you can either stop the installation, take measures to meet the recommendations, and restart the installation or you can choose to continue the installation without changes.

Download and install Windows patch management files (optional)

The SA Windows Patch Management feature requires several files from the Microsoft software download repository. These files are installed during Core installation.

> **Note:** If you do not plan to use SA to manage Windows servers, you can optionally choose not to install these files and successfully complete installation. However, if these files are not installed, no operations against Windows servers should be performed. These files are required for many Windows-based operations other than Windows patching.

- "Installing the required Windows patch management files on an existing Core" below
- "Requirements" below
- "Manually obtaining Windows patching utilities" on the next page

Installing the required Windows patch management files on an existing Core

To perform Windows patching in the future, you will need to install the required Windows Patch Management files either by using the SA Client’s Import feature or the **populate-opsware-update-library** command line script as described in the SA User Guide.

See "Manually obtaining Windows patching utilities" for more information about manually downloading the Windows Patching Utilities.

Requirements

Managed Servers must meet the following Windows patching requirements:

- Windows Installer 3.1 must be installed
- MSXML 3+ must be installed (MSXML is a general requirement for all Windows managed servers regardless of whether the managed server will or will not use the Windows patching feature).
- The Windows Update Agent must be installed
- The Windows (Automatic) Update service must *not* be disabled but must be set to *never* check for updates.

> Note: As of Windows Server 2008, the Automatic Update service was renamed the Windows Update service.

Manually obtaining Windows patching utilities

If you did not install the Windows patch management files during core installation and your SA Core and SA Client do not have internet access, you can perform the following tasks from a machine with internet access to obtain the files and transfer them to the core:

1. Obtain the following files from Microsoft:

   > Note: The links to these files are provided as a convenience, however, Microsoft Corp. may change the links after the release of this document. Therefore, we cannot guarantee that these links will be valid when you use them and you may need to search the Microsoft Support website to find the correct files.

   - wsusscn2.cab

     The wsusscn2.cab file contains the Microsoft patch database. Download wsusscn2.cab from: http://go.microsoft.com/fwlink/?LinkID=74689

   - WindowsUpdateAgent30-x86.exe
     The WindowsUpdateAgent30-x86.exe file is required when SA scans x86-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing WindowsUpdateAgent30-x86.exe from:
     http://go.microsoft.com/fwlink/?LinkID=100334

     > Note: After downloading, you must rename the file to "WindowsUpdateAgent-x86.exe".

     - WindowsUpdateAgent30-x64.exe

       The WindowsUpdateAgent30-x64.exe file is required when SA scans x64-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing WindowsUpdateAgent30-x64.exe from:
       http://go.microsoft.com/fwlink/?LinkID=100335

       > Note: After downloading, you must rename the file to "WindowsUpdateAgent-x64.exe".

     - WindowsUpdateAgent30-ia64.exe

       The WindowsUpdateAgent30-ia64.exe file is required when SA scans Itanium x64-based managed servers to determine which Windows patches/hotfixes are installed. Download the package containing WindowsUpdateAgent30-ia64.exefrom:
       http://go.microsoft.com/fwlink/?LinkID=100336

> Note: After downloading, you must rename the file to "WindowsUpdateAgent-ia64.exe".

2. Copy the files you obtained in the preceding steps to a directory that will be accessible by the SA Installer during the Software Repository installation. For example, you might copy the files to the **/opsw/win_util** directory.
3. Write down the name of the directory containing the Windows Update Agent files. You will need this location when you run the SA Installer and are prompted to provide the fully qualified directory path to the WUA files. You can also find the WUA file location by checking the SA parameter, **windows_util_loc**.

These patch management files will be copied to all Windows servers during SA Agent deployment. If you upload newer versions of the WUA files to the Software Repository later, they will be downloaded to all managed Windows servers during software registration. After the core is installed and running, you can upload new versions of these files with the Patch Settings window of the SA Client.

For more information on Windows Patch Management, see the SA 10.60 User Guide.

Check the SA Global File system (OGFS) requirements

This section discusses requirements for SA's Global File System (OGFS). The OGFS represents objects in the platform data model (such as facilities, customers, and device groups) and information available on platform managed devices (such as the configuration setting on a managed network device or the file system of a managed server) as a hierarchical structure of file directories and text files.

OGFS store and audit hosts

When you run the SA Installer interviewer in advanced mode, you can specify values for the *ogfs.store.host.ip* and *ogfs.audit.host.ip* parameters. If you set either of these parameters to point to a host that does not run the Slice Component bundle (which contains OGFS and the Software repository), then perform the following steps on the host you do specify:

1. With **mkdir**, create the directories that you specified for the *ogfs.store.path* and *ogfs.audit.path* parameters.
2. Modify the export tables.

   > Note: In these examples, the Slice Component bundle is installed on two separate hosts within the same core.

   On a Linux host, modify the **/etc/exports** file, such as:

   ```
   # Begin Opsware ogfs export
   /export/ogfs/store 1.2.3.4(rw,no_root_squash,sync) \
   1.2.3.5(rw,no_root_squash,sync)
   /export/ogfs/audit 1.2.3.4(rw,no_root_squash,sync) \
   1.2.3.5(rw,no_root_squash,sync)
   # End Opsware ogfs exports
   ```

   where 1.2.3.4 and 1.2.3.5 are example IP addresses of the two Slice Component bundle hosts and where /export/ogfs/store and /export/ogfs/audit are corresponding paths that exist on the host from where you are exporting the OGFS data.
3. After you add new entries to the export tables, export the directories or restart the Network File System using standard system procedures.

> Note: Remember to verify that the NFS Daemon starts when the system reboots. If your security policies require that NFS services be disabled, in order to install the Slice Component bundle on Linux systems you will need to configure the services `nfs`, `nfslock` to start the services and `netfs` to ensure that network (remote) filesystems are mounted after the network is available. Slice Component bundle installation will fail otherwise. The services can be disabled again after installation.

Name Service Caching Daemon (nscd) and OGFS

If the Name Service Caching Daemon (**nscd**) runs on the same server as the Slice Component bundle, then users cannot open a global shell session with a direct **ssh** connection. If **ncsd** is running on the Slice Component bundle server, the Installer turns it off and runs the **chkconfig nscd off** command to prevent it from starting after a reboot. No action is required.

Check the Core host(s) time and locale requirements

This section discusses the time and locale requirements for SA Core Servers.

Core time requirements

Core Servers (either Single Core or Multimaster) and Satellite Core Servers must meet the following requirements. These time requirements do not apply to Managed Servers.

- All SA Core Servers must have their time zone set to Coordinated Universal Time (UTC).
- All SA Core Servers must maintain synchronized system clocks. Typically, you will synchronize the system clocks through an external server that uses NTP (Network Time Protocol) services.

To configure the time zone on a Linux server, copy or link **/usr/share/zoneinfo/UTC** to **/etc/localtime** and ensure that the /etc/sysconfig/clock file contains the following lines:

```
ZONE="UTC"

UTC=true
```

Locale requirements

- The servers hosting the Model Repository and the Software Repository (part of the Slice Component bundle) must have the `en_US.UTF-8` locale installed.
- To display data from Managed Servers using various locales, the server hosting the Global File System (OGFS) must also have all the locales installed.

  For information about enabling non-English locales for Windows patching, see Server patching.
- To verify whether the `en_US.UTF-8` locale is installed on a server, enter the following command:

  ```
  echo $LANG
  ```
- To define or modify the locale, enter the following values in the **/etc/sysconfig/i18n** file:

  ```
  LANG="en_US.UTF-8"

  SUPPORTED="en_US.UTF-8:en_US:en"
  ```

- To verify whether the en_US.UTF-8 locale is installed on a server, enter the following command:

  ```
  LANG="en_US.UTF-8"
  ```

  ```
  SUPPORTED="en_US.UTF-8:en_US:en"
  ```

Installing the Windows Update Service

Installation of an SA Agent on a managed server requires the Windows Update service to be installed.

- The Windows Update Service Startup Type configuration should be set to automatic.
- If the Windows Update Service Startup Type configuration is set to manual, the agent must start the service each time it registers software, performs compliance scans, or remediates packages or patches.
- If the Windows Update Service Startup Type configuration is disabled, the agent will not start the service and it will be unable to detect installed and needed patches on the managed server, resulting in a Scan Failed during Windows patch compliance scans.
  The Windows Event Log may contain an {E60687F7-01A1-40AA-86AC-DB1CBF673334} error as described at http://support.microsoft.com/kb/896224.

Checking the user and group requirements

During installation, the SA Installer creates new users and groups. These users and groups are:

Users and groups created during an SA/Linux Install

userid	group	home directory	shell	remote login enabled
twist	users	/var/opt/opsware/twist	/bin/sh	No*
occ	occ	/var/opt/opsware/occ	/bin/sh	No*
opswgw	opswgw	/var/opt/opsware/ opswgw-<gw name>	/sbin/nologin	No
**oracle	oinstall	/u01/app/oracle	/bin/bash	No*
*Password disabled **SA-supplied Oracle installation only				

File ownership

userid	Files and folders owned

`twist`	`/etc/opt/opsware/twist`
	`/var/opt/opsware/twist`
	`/var/opt/opsware/crypto/twist`
	`/var/log/opsware/twist`
	`/opt/opsware/twist`

`occ`	`/etc/opt/opsware/occ`
	`/var/opt/opsware/occ`
	`/var/opt/opsware/crypto/occ`
	`/var/log/opsware/occ`
	`/opt/opsware/occclient`
	`/opt/opsware/occ`

`opswgw`	`/etc/opt/opsware/ opswgw-<gw name>`
	`/var/opt/opsware/ opswgw-<gw name>`
	`/opt/opsware/ opswgw-<gw name>`

Check SA Cores on VMs requirements (optional)

SA Cores are certified for VMware VMs running Red Hat Enterprise Linux as the guest operating system.

SA Cores are certified for running inside VMware VMs for all the supported core platforms as guest operating system. The supported versions of the ESXi hypervisors are generally the latest available releases from the vendor. For more information, see SA Support and Compatibility Matrix.

The following topics describe the requirements and instructions for installing an SA Core on a VMware VM.

- "Supported Hypervisor and Guest Operating Systems" on the next page
- "VM CPU and memory requirements" on the next page
- "SA satellite memory requirements" on page 38
- "Hardware performance issues" on page 38

- "VMware virtual center requirements" on page 39
- "SA Core component VMs on SAN or NAS devices" on page 39
- "Installing SA Cores under VMware VMs" on page 39

Supported Hypervisor and Guest Operating Systems

For the list supported Hypervisor and Guest Operating Systems, see SA Support and Compatibility Matrix.

VM CPU and memory requirements

The following table shows the minimum number of CPUs and required memory to run SA Cores on VMs for setting up a laboratory or development environment:

VM CPU and memory requirements

Number of VMs	Number of CPUs and RAM for each VM		Number of Managed Servers
	4 CPUs 16GB RAM	4 CPUs 16GB RAM	
1	Infrastructure Component bundle SA Provisioning bundle Slice Component bundle		960
2	Infrastructure Component bundle SA Provisioning bundle Slice 0 Component bundle	Slice 1 Component bundle	2250

> Note: SA supports core components installed on VMs only when your VM configurations follow VMware best practices for managing resource allocation and overall workload. You must ensure that other VMs sharing the same ESXi hypervisor do not significantly impact the resources available to the VM hosting the SA Core. If there are performance issues, for troubleshooting

> purposes, HPE Support may require you to replicate these issues in an environment in which the VM supporting the SA Core is the sole VM active within the ESXi hypervisor.

> Note: It is essential that you avoid over-commitment of physical resources (CPU and physical memory) to ensure proper functioning of the VMs. Over-commitment of these resources can lead to performance issues as well as time synchronization issues.

SA satellite memory requirements

The following table provides the minimum number of CPUs and required memory to run SA Satellites on VMs:

Satellite CPU and Memory Requirements

Number of VMs	Number of CPUs and RAM for each VM	Number of Managed Servers
	2 CPUs 2 GB RAM	
1	Satellite Components	1500

Hardware performance issues

The hardware requirements for Hypervisors running SA Core VMs can vary based on the following factors:

- The availability of the physical CPUs and memory in the Hypervisor to support the recommended SA Core VM configuration.
- The number of VMs running concurrently on the physical server.
- The number of servers that the SA Core manages.
- The number and complexity of your concurrent operations.
- The number of concurrent users who can access the SA Command Center.
- The number of facilities in which the SA Core operates.

VMware virtual center requirements

Use of the following Virtual Center features with an SA Core installed on a VM has *not* been validated and could make it difficult for HPE Support to diagnose possible problems with your installation if required:

- Snapshots
- Distributed Resource Scheduling (DRS)
- VMotion
- Storage VMotion
- Fault Tolerance
- High Availability (HA)

HPE is continuing to validate these advanced Virtual Center features and will announce support when available.

SA Core component VMs on SAN or NAS devices

Running SA Core Components on VMs is supported if the VM images are run from a local disk or SAN. Running SA Core Components on VMs is not supported if the VM images are stored on NAS devices.

Installing SA Cores under VMware VMs

SA Core pre-installation requirements, disk space requirements, installation, and post-installation requirements under VMware VMs are the same as those for installation on a physical server. You can use the instructions described in this guide to install an SA Core on an existing VMware VM.

Prepare the environment

This section provides you with the information required to help you plan the SA configuration required for your facility. It also provides you with information to scale the performance of SA.

- "SA Core configuration for your facility" below
- "Customer installable SA Core configurations" on page 42
- "Configuration of additional components" on page 45
- "Performance scalability" on page 49
- "Oracle setup for the Model Repository" on page 100

SA Core configuration for your facility

See "Customer installable SA Core configurations" for detailed descriptions of supported SA Core configurations. For performance scalability information, see "Performance scalability"

The SA Core configuration that is most appropriate for your facility will depend primarily on the number of servers that are to be managed by SA in the facility.

A typical SA Core installation has three main components. The Model Repository, the Infrastructure Component bundle and one Slice Component bundle. SA Provisioning also requires a Media Server and Boot Server. Since the Media Server and Boot Server do not generate much load and often have environmental dependencies they are not listed in the tables below. If you need more detailed information about SA Core Components, see the "SA Overview and Architecture" in the SA 10.60 Key Concepts Guide.

There is no infallible way to select hardware for an SA Core installation. However, the following two tables show a few recommended SA Core Component layouts that should perform well.

As you can see, scaling a core requires adding slices. Each slice adds highly available UI, API, OGFS, and Gateway resources. If you have only a few core servers, you can begin with two larger servers, then increase the capacity of the core by adding additional slices.

The following abbreviations are used in the tables below:

MR:	Model Repository
INFRA:	Infrastructure Component bundle
Slice <x>:	Slice Component bundle
OS Prov:	Operating System Provisioning Component bundle

Small-to-Medium SA deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server		
	Server 1	**Server 2**	
500	MR, Infra, Slice 0, OS Prov	N/A	
1000	MR	Infra, Slice 0, OS Prov	
Server Configuration: 4 CPU cores, 16 GB RAM, 1 GB/s network			

Medium-to-large SA deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server				
	Server 1**	**Server 2***	**Server 3***	**Server 4***	**Server 5***
2000	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
4000	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A
6000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
8000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3
* Server Configuration: 8 CPU Cores, 16 GB RAM, 1 GB/s network ** Server Configuration: 12 CPU Cores, 32 GB RAM, 1 GB/s network					

For more information about performance scalability, see "Performance scalability".

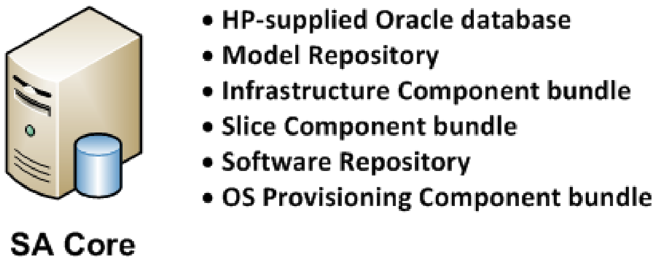
Customer installable SA Core configurations

The following are SA Core configurations supported by HPE for customer installation.

1. SA Core with a local SA-supplied Oracle database

Suitable for small facilities. See "Install SA Core with a local SA-supplied database"

Configuration 1

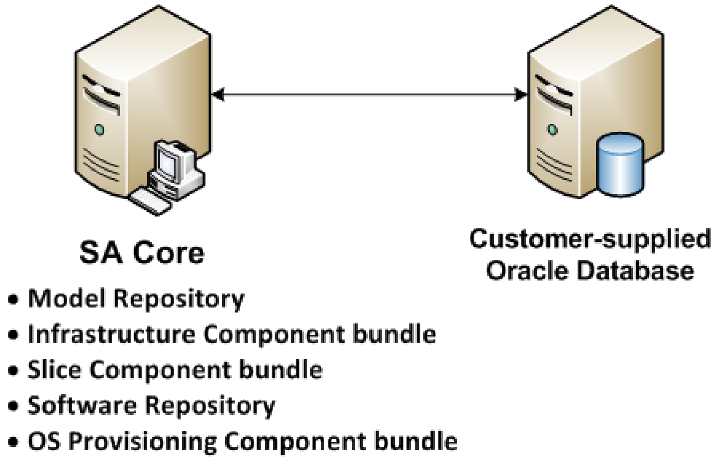


- HP-supplied Oracle database
- Model Repository
- Infrastructure Component bundle
- Slice Component bundle
- Software Repository
- OS Provisioning Component bundle

2. SA Core with a remote customer-supplied Oracle database

Suitable for small to medium facilities. See "Install SA Core with a remote customer-supplied Oracle database".

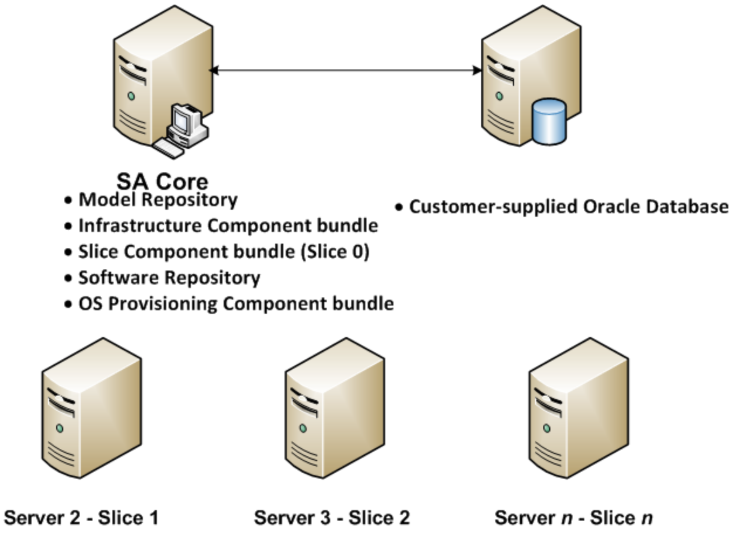
Configuration 2



3. SA Core with a remote customer-supplied Oracle database and additional slice component bundles

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. See "Installing SA Core with a remote customer-supplied database and additional slice component bundles" on page 195..

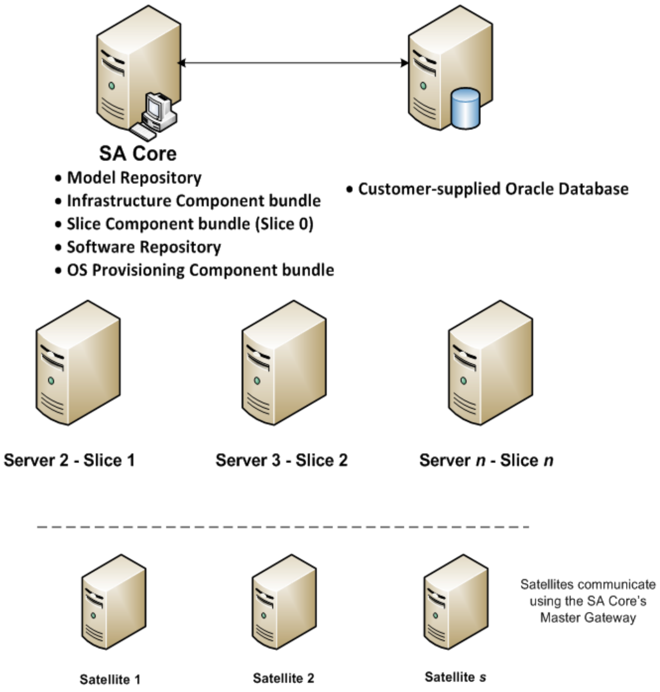
Configuration 5


SA Core
• Model Repository
• Infrastructure Component bundle
• Slice Component bundle (Slice 0)
• Software Repository
• OS Provisioning Component bundle
• Customer-supplied Oracle Database
Server 2 - Slice 1
Server 3 - Slice 2
Server *n* - Slice *n*

4. SA Core with a remote customer-supplied Oracle database, additional slice component bundles and satellites

Suitable for small, medium and some larger facilities depending on the number of Slice Component bundles installed. Satellite installations can handle in facilities in which the number of managed servers is not large enough for a full SA Core.

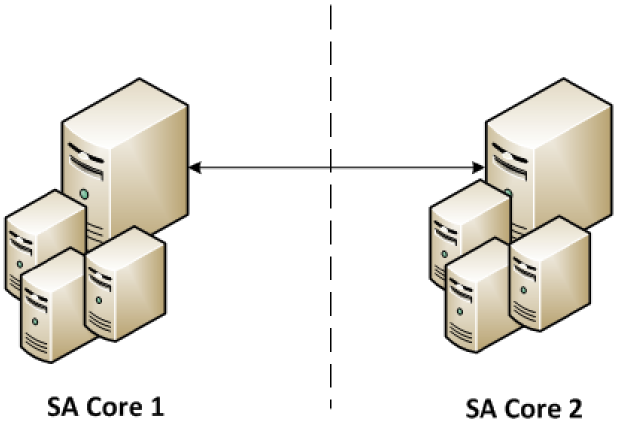
Configuration 7


SA Core
• Model Repository
• Infrastructure Component bundle
• Slice Component bundle (Slice 0)
• Software Repository
• OS Provisioning Component bundle
• Customer-supplied Oracle Database
Server 2 - Slice 1
Server 3 - Slice 2
Server *n* - Slice *n*
Satellites communicate using the SA Core's Master Gateway
Satellite 1
Satellite 2
Satellite *s*

5. First (Primary) Core with a Secondary Core (Multimaster Mesh)

Suitable for medium and larger facilities with a number of servers to be managed large enough to require a second core. See "Install SA first (primary) core with a secondary Core (multimaster mesh)".

Configuration 8



Configuration of additional components

This section provides information about configuring the following additional components:

- "FIPS compliance options" below
- "Enabling IPv6 networking " on the next page
- "Cryptographic material modes" on the next page
- "Mounting the SA ISO media" on page 47

FIPS compliance options

HPE Server Automation (SA) complies with the Federal Information Processing Standards publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules. During installation you can choose to enable FIPS by setting the `fips.mode` parameter to **enabled**.

You will be prompted during the installation to specify whether FIPS should be enabled or not.

Under normal security conditions, HPE recommends using SHA256 with a key length of 2048. Higher security requirements could require FIPS with a key length of 4096 or other hash functions from SHA-2 family. Note that use of FIPS or other hash functions from SHA-2 family can impact core performance. Contact your Security Administrator for more information.

See FIPS 140-2 compliance.

> **Note:** In FIPS mode, sufficient entropy stemming from the character device /dev/random must be

> available on the core servers, to ensure proper startup and functionality of SA components.

Enabling IPv6 networking

To enable IPv6 networking, run the **`enable_ipv6.sh`** script as a post-installation or upgrade step. This enables IPv6 on the SA core and satellite gateways and OS provisioning components on SA 10.2 or later releases. The script is available on all infrastructure, slices, boot servers, and satellite systems. For more information, see "Enable IPv6 networking post installation".

For further information about IPv6 and the `enable_ipv6.sh` script, see “SA Remote Communications Administration” in the SA 10.60 Administration Guide.

For information about running the `enable_ipv6.sh` script post-installation, see "Enable IPv6 networking post installation".

Cryptographic material modes

SA 10.60 and later supports two certificate modes for installing an SA core:

- **self-signed** certificate mode installation
- **third-party** certificate mode installation

In **self-signed** certificate mode, SA uses its own Certificate Authorities (CAs) to automatically sign all the SA Core components certificates.

In **third-party** certificate mode, SA generates Certificate Signing Requests (CSRs) for the SA certificates. You are responsible for managing these CSRs and for providing SA with the certificates issued by your trusted CA. The SA Core installation completes only after SA can pick up the valid certificates from your specified location.

To switch from self-signed to third-party certificate mode, upgrade your SA Core and Agents, then run a Core Recertification job. This will replace all certificates signed by self-signed CAs with certificates signed by third-party CAs.

> - Your selected certificate mode applies to all the SA Cores and Satellites in the SA mesh. This means that you cannot target only specific cores for third-party certification and keep others under SA certification.

- SA certificates are unique for each Core, Satellite and managed server. SA Core and Satellite components have unique certificates based on the server they are installed on. For example, on a Core with two slices installed on two servers, the slice certificates of the first server are different from the slice certificates of the second server.

In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.

Example: to install an SA mesh with the following topology,

```
16.77.42.65 (oracle_sas, truth_mm_overlay)
16.77.41.24 (infrastructure, word_uploads)
16.77.43.252 (slice, osprov)
16.77.45.21 (satellite)
```

add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:

```
16.77.42.65 hostname1.example.com hostname1
16.77.41.24 hostname2.example.com hostname2
16.77.43.252 hostname3.example.com hostname3
```

The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

Starting with SA 10.60, if you want to use cryptographic material from a previous SA installation (SA 10.0 or earlier), you can no longer simply copy the existing crypto file due to enhancements to the way SA handles encryption.
You can, however, copy the crypto file from an existing SA 10.1 or later SA Core. You can do so by copying the crypto file `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e` and the `/etc/opt/opsware/crypto/security.conf` file to the same locations on the server that will host the SA Core or First Core (Multimaster Mesh) before beginning the installation. During installation, do not have the installer generate cryptographic material and when you are prompted, provide the password for this cryptographic material.

Mounting the SA ISO media

The SA installation/upgrade media is organized into separate categories in the downloaded file structure, for example:

- `oracle_sas` (HPE Server Automation Database)
  The media used to install the Oracle database
- `primary` (HPE Server Automation Product Software)
  The media used to install the SA Core Components
- `upload` (HPE Server Automation Agents and Utilities)
  The media used to upload and install SA Core content and tools
- `sat_base` (HPE Server Automation Satellite Base)
  The media used to install the SA Satellite components, it does not include the OS Provisioning components and is therefore smaller and can be helpful when you are transferring the media over the network.
- `sat_osprov` (HPE Server Automation Satellite Base including OS Provisioning)
  The media used to install the SA Satellite and the Satellite’s OS Provisioning components.

Initial invocation of the **`hpsa*`** scripts for core install/upgrade for SA Cores must be from the **`primary`** media, Satellites from the **`sat_base`** or **`sat_osprov`** media.

The SA Installer requires that the media directory structure be maintained, for example:

```
<mountpoint>/<user_defined_prefix>-<media_name>/disk001/opsware_installer/hpsa*.sh
```

where <**`user_defined_prefix>-<media_name>`** is, for example, **`hpsa-primary`**, **`hpsa-sat_base`**, etc. HPE recommends the prefix **`hpsa`** and the media category identifiers shown above (**`sat_base,primary`**, etc.). *The hyphen after* **`hpsa`** *is required even if you do not append a prefix*.

SA is delivered as media that can be copied to a local disk or mounted as an NFS mount point. You must mount all media on a host where install script will be invoked. If media is mounted as follows the SA installer will auto mount it on local or remote core host(s) as needed. For example:

- **oracle_sas**

  ```
  mount oracle_sas.iso /<mountpoint>/hpsa-oracle_sas/
  ```

- **primary**

  ```
  mount primary.iso /<mountpoint>/hpsa-primary/
  ```

- **upload**

  ```
  mount upload.iso /<mountpoint>/hpsa-upload/
  ```

- **sat_base**

  ```
  mount upload.iso /<mountpoint>/hpsa-sat_base/
  ```

- **sat_osprov**

  ```
  mount upload.iso /<mountpoint>/hpsa-sat_osprov/
  ```

Where `<mountpoint>` is a media mount location of your choosing, for example `/mnt`.

If you use a different directory structure, the SA Installer will prompt you for the path each time it needs to access the media.

Performance scalability

This section provides information about improving the performance of your SA Core and its components.

You can vertically scale the SA Core Components, by adding additional CPUs and memory, or horizontally, by distributing the Core Components to multiple servers.

The " Small-to-Medium SA deployment (SA 7.80 and later)" and "Medium-to-Large SA deployment (SA 7.80 and later) " tables list the recommended distribution of SA components across multiple servers. In both tables, the bundled SA Core Components are distributed in the following way:

- MR: Model Repository
- INFRA: Infrastructure Component
  - Model Repository Multimaster Component
  - Management Gateway
  - Primary Data Access Engine
- Slice(*x*):
  - Agent Gateway
  - Core Gateway
  - Command Engine
  - Software Repository
  - Command Center
  - Web Services Data Access Engine
  - Secondary Data Access engine)
  - Global File System

- Software Repository Accelerator (`tsunami`)
- Memcache

Core Component distribution

The introduction of bundled components requires that you consider how to distribute the SA Core Components based on the available hardware and memory. A typical SA installation now has three main components:

- Model Repository,
- Infrastructure Component bundle
- One Slice Component bundle in addition to the Media Server and Boot Server.

Since the Media Server and Boot Server do not generate much load and often have environmental dependencies they are not listed in the tables below.

There is no infallible way to select hardware for an SA installation. However, below are some recommended SA Core Component layouts that perform well. As you can see, scaling a core requires adding slices. Each slice adds highly available UI, API, OGFS, Gateway resources. Considering this, when you have a small number of core servers, it may be best to begin with two larger servers, then grow the capacity of the core by adding additional slices. The following abbreviations are in the tables listed below:

- MR — Model Repository
- INFRA — Infrastructure Component bundle
- Slice <*X*> — Slice Component bundle
- OS Prov — Operating System Provisioning Component bundle. :

Small-to-Medium SA deployment (SA 7.80 and later)

Managed Servers	**SA Component Distribution by Server**		
	Server 1	**Server 2**	
500	MR, Infra, Slice 0, OS Prov	N/A	
1000	MR	Infra, Slice 0,	

Small-to-Medium SA deployment (SA 7.80 and later), continued

Managed Servers	SA Component Distribution by Server		
		OS Prov	
Server Configuration: 4 CPU cores, 16 GB RAM, 1 GB/s network			

Medium-to-Large SA deployment (SA 7.80 and later)

Managed Servers	SA Component Distribution by Server				
	Server 1**	**Server 2***	**Server 3***	**Server 4***	**Server 5***
2000	MR	Infra, Slice 0, OS Prov	N/A	N/A	N/A
4000	MR	Infra, Slice 0, OS Prov	Slice 1	N/A	N/A
6000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	N/A
8000	MR	Infra, Slice 0, OS Prov	Slice 1	Slice 2	Slice 3
* Server Configuration: 8 CPU Cores, 16 GB RAM, 1 GB/s network ** Server Configuration: 12 CPU Cores, 32 GB RAM, 1 GB/s network					

Factors affecting core performance

- The hardware requirements for SA vary based on these factors:
- The number of servers that SA manages
- The number and complexity of concurrent operations
- The number of concurrent users accessing the Command Center
- The number of facilities in which SA operates

Multimaster Mesh scalability

To support global scalability, you can install an SA Core in each major facility, linking the cores in a Multimaster Mesh. The size of the SA Core in each facility can be scaled according to local requirements.

Multimaster Mesh availability

In addition to Model Repository replication, a Multimaster Mesh supports the replication and caching of the packages stored in the Software Repository. Typically, the core in each facility owns the software that is uploaded to the core’s Software Repository. To support availability, multiple copies of the packages can be maintained in remote Software Repositories. See the SA 10.60 Administration Guide for more information.

The bundling of the Software Repository with the Slice Component bundle and the Software Repository Store with the Infrastructure Component bundle does not affect availability. The Software Repository reads the replicator configuration file to determine how to serve files from backed up directories.

Satellite Core CPU/Memory requirements

Servers hosting SA Satellite Core installations must meet the following minimum requirement:

- 2 CPUs and 2 GB RAM per 1,500 managed servers per Satellite Core up to 4 CPUs and 4 GB RAM for 3000 managed servers per Satellite Core

The capacity of a server hosting an SA Satellite can be increased to support additional managed servers as indicated above. Workload characteristics across SA environments can vary dramatically and the carrying capacity of a given SA satellite under those workloads can vary as well. For deployments that require more than 3,000 devices behind an SA Satellite, HPE recommends that you consider deploying additional SA satellites in the same realm. This solution provides increased redundancy and additionally avoids reaching the point of diminishing return from a single SA Satellite host server which requires you to continuously increase its capacity in order to support increasing load demands.

Load balancing additional instances of core components

If SA must support a larger operational environment, you can improve performance by installing additional instances of the *Slice Component bundle* which provides you with these additional components per installation:

- Agent Gateway
- Core Gateway
- Command Center
- Software Repository
- Web Services Data Access Engine
- Secondary Data Access engine
- Software Repository Accelerator (`tsunami`)
- Memcache

If you have installed multiple instances of the Slice Component bundle, load balancing between the instances occurs automatically as requests for load services are received by the Core Gateway. The Core Gateway handles incoming client connections and load balances them across the Slice Component bundles in the core.

You can also deploy a hardware load balancer for the servers that run additional instances of the Slice Component bundle. You can configure the load balancer for SSL session persistence (stickiness) with the least connections algorithm.

You can also put a load balancer in front of the Core Gateways, however, this will only load balance the Gateways, but with the added benefit that clients would have only one address to connect to and would failover gracefully in the event of a Slice Component bundle host failure.

Load balancing does not affect validation of `httpProxy` certificates since the identity of the core is based on the address the clients use to connect, not the identity of the server that ultimately serves the request. All Slice Component bundles should be issued the same certificate and the hostname referenced in the certificate should match the DNS hostname that external clients use to connect. If a load balancer is used, this should be the hostname of the load balancer.

Important SA installation information

Read the information in this section before you start installing SA in your facility.

- "Invoke the SA Installer" below
- "SA Installer installation modes" on page 56
- "SA Interview and the Core Definition File (CDF)" on page 56
- "Master passwords" on page 58
- "SA Core installation by root or non-root users" on page 59
- "Help" on page 61
- "Restart an interrupted installation" on page 61
- "Installer logs" on page 64
- "SA parameter password security" on page 65
- "SA Core installation process flow" on page 67
- "SA Core parameter reference" on page 68

> **Important:** Since SA 10.60 is enabled with HPE AutoPass licensing, ensure that you have enough licenses available for the number of SA Agent managed servers in your business environment. For more information, see **AutoPass licesing** section in the Adminstration Guide.

Invoke the SA Installer

You invoke the SA Installer using one of the following scripts from the *SA Product Software* media or mounted copy:

- **`hpsa_install.sh`** installs the Oracle database and Model Repository, installs the Core Components for a Primary Core, installs the components for Secondary Cores, exports the contents of the Model Repository.

- **uninstall_opsware.sh** uninstalls a single Core Component or uninstalls all Core components. For more information about uninstalling an SA Core, see "SA Core uninstallation" on page 309.

> **Caution:** Do not invoke the SA Installer from any other distribution.

hpsa_install.sh accepts the command line arguments shown in the following table.

SA Installer command line arguments

Argument	Description
-h	Display the Installer help for the command line options. *To display help during the interview, press ctrl-I*.
-c <cdf_ filename>	Invoke the Installer using the SA installation configuration parameter values in a specified saved Core Definition File (CDF. If you do not specify a CDF, you must provide the values for certain configuration parameters or accept the SA default values. The SA configuration parameter values you provide during the installation interview are used for the current installation and are automatically saved into an initial CDF that is used later during SA Core upgrades and installation of Secondary SA Cores.
--pwsave	Specifies that the root passwords for all servers specified during installation are to be encrypted and accessed by a master password that you specify. See "Master passwords".
--verbose | --debug	Run the installer in verbose or debug mode which causes more information to be displayed on the console. See "Installer logs".

Best Practice: Using the screen utility for SA installation

The screen utility for Linux enables you to safely run the SA Installer and recover from interruptions such as a network disconnection. If, for some reason, you are disconnected from an installation session, you can log back into the machine and use screen to reattach to your installation session.

SA recommends that you invoke the SA Installer using the screen utility in order to minimize the impact of an installation problem due to a network failure.

Red Hat Enterprise Linux, SUSE Linux Enterprise Server and Oracle Enterprise Linux distributions include the screen package but you must explicitly install it (it is not available by default).

SA Installer installation modes

Depending on how you invoke the SA Installer, you are prompted to provide values for a number of parameters, for example, passwords, file locations, and so on. The number of parameters you are prompted for varies depending on the installation method you choose.

Simple installation mode

If you choose a Simple Installation, the default values for certain parameters that are rarely modified will be used (you will not be prompted to specify values for these parameters). These parameters include the various Oracle passwords used internally by the Core Components.

> **Note:**
> Advanced and Expert Interview modes should be used only by HPE technical services.

Advanced installation mode

If you choose the Advanced Installation, the installer prompts you to supply values for *those* parameters not modifiable in the Simple Installation.

Expert installation mode

Used by HPE Technical Staff.

SA Interview and the Core Definition File (CDF)

During installation, you are required to provide values for certain SA parameters that are used to configure your SA installation. This process is known as the SA Interview. The values you provide are saved to a Core Definition File (CDF).

SA creates the first CDF when you install the SA Primary Core. You will use this CDF later to add a Secondary Core for a Multimaster Mesh (multiple core SA installation) or perform an upgrade. See

"Reusing a Core Definition File (CDF)". The CDF is saved in/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml.

In some cases, when you provide a parameter value, the SA Installer validates the response (for example, a directory or path that does not exist or an invalid value or range); you are asked to re-enter a value if the installer is not able to validate your response. Some parameters are also re-validated during the actual installation of the Core Components. If a response to a prompt cannot be validated at time of installation, the installer runs a mini-interview during which you can provide a valid response.

How and when CDFs are saved

During installation, the SA Installer saves a temporary CDF whenever you press `c` to continue on an action confirmation screen. For example, the `Install Components` screen:

```
Upgrade Components

=====================

Components to be Upgraded

-------------------------

Model Repository, First Core

Core Infrastructure Components

Slice

OS Provisioning Components

Software Repository - Content (install once per mesh)

Up-to-date Components (will not upgrade)

----------------------------------------

Oracle RDBMS for SAS

Enter one of the following directives

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

The temporary CDF is saved in /var/tmp/cdf_<timestamp>_temp.xml. This file can be used to resume an interrupted installation. See "Restart an interrupted installation". This temporary file is updated as each component is processed thus maintaining the setup state as of the most recent action.

If you are concerned about security of CDFs, this file should be saved in a secure location or deleted. Before deleting, however, consider you may need to reuse the CDF in future for adding facilities, additional Slice Component bundles, upgrades and patching the SA Core or mesh.

Concluding the interview

After you have provided values for all the SA configuration parameters, the SA Installer automatically saves the CDF at the end of the installation. The location of the CDF is determined by following factors:

- If the infrastructure component bundle host is known at the point of exit, then the CDF is saved on that host under /var/opt/opsware/install_opsware/cdf as cdf.xml. CDF backups are saved as .cdf_<timestamp>.xml
- If the Infrastructure host is unknown at the point of exit, the CDF is saved as cdf_tmp.xml in /var/tmp on the server on which the installer was invoked.

Reusing a Core Definition File (CDF)

You can specify a CDF to use during the installation by invoking the installer using the `-c <cdf_filename>` argument. The installer reads the contents of CDF and uses the parameter values stored in that file as the defaults. Use the latest CDF as determined by the time stamp. The CDF is saved as described in "How and when CDFs are saved".

Master passwords

You can specify a master password to be used to access the encrypted user passwords of all core hosts specified during the installation of a new SA Core.

To encrypt server passwords specified during installation, invoke the installation with the `--pwsave` argument. When you begin an installation with the `--pswave` argument specified, the installer encrypts host passwords and saves them in the final CDF on completion of the installation whether a successful or failed install. See "Invoke the SA Installer".

The Master Password (MP) is saved as a hash of hash SHA(SHA(MP)). SA uses this key to encrypt the host passwords of all servers that are specified as part of a new core installation and secure hash SHA(MP) is used to generate a 1024 character key and an encrypted password string which is saved on each host as `root_user_password` for root passwords and `non_root_user_password` for non-root passwords.

You specify the master password when you see this prompt at the end of the installation, specify “none” if you do not want to create a master password:

```
Creating temporary CDF [/var/tmp/cdf_tmp.xml]

master.password []:

Specify a master password. This password will enable encryption of the server(s)
password. If "none" is specified then server(s) password will not be saved.

master.password []: *******
```

Invoking the Installer on an SA Core that uses a master password

When you begin an installation on a core that uses a master password, you are prompted to provide the password before continuing:

```
Specify a master password. This password will enable decryption of the server(s)
password. Enter "none" to provide the server(s) password again.

master.password []:
```

The installer will use the encrypted passwords for the core hosts that were stored when you created the master password. If you specify “none” as the master password, the installer prompts you to provide passwords for each core server.

SA Core installation by root or non-root users

Multiple types of users can perform installations and upgrades on SA Cores. Previously, only root ssh users with root ssh login enabled could perform installations on SA Cores. This is no longer required.

Types of Install users

The following users are supported when using the SA installer to install, or upgrade SA on a **local** machine:

- Root user
- User who has permissions to invoke commands with su
- User who has permissions to invoke commands as root with sudo capabilities

When a core has multiple core servers, the installer will need to run commands on hosts other than the one where the installer runs. Hence, during the installation process, it will require user and password credentials for such hosts. The following users are supported when installing SA on remote machines:

- Root user (including root ssh access)
- User with sudo capabilities (including user ssh access)

Password-less sudo is not supported for regular users with sudo capabilities.

When performing the installation or upgrade of a core as a user other than root, make sure you invoke all the commands using `sudo`.
For example: **`sudo /`*`media_path`*`/opsware_installer/hpsa_install.sh`**

Settings required for regular users with sudo capabilities

Make the following changes to the /etc/sudoers file on every machine where the user (in this case, Bob) installs SA:

```
Defaults        lecture=never

Bob             ALL=(ALL)       ALL

Defaults        secure_path = /sbin:/bin:/usr/sbin:/usr/bin
```

> **Note:**
> For remote users, the home directory must exist on the remote host, otherwise the installer will not be able to validate the credentials.

General settings for user names

This topic describes the general rules for user names in SA.

User names should have the following characteristics:

- Be portable across systems conforming to the POSIX.1-2008 standard for portable OS interfaces. The value is composed of characters from the portable filename character set.
- Not contain a hyphen (-) character as the first character of a portable user name.
- Use the following set of characters if it is a portable filename:

  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a b c d e f g h i j k

  l m n o p q r s t u v w x y z 0 1 2 3 4 5 6 7 8 9 . _

Help

At any time during the interview, you can press `ctrl-I` to display help for the current interview prompt. A brief description of the prompt and the expected responses will be displayed.

Restart an interrupted installation

If the SA Installer encounters an error, the installation stops. Correct all the errors before you retry the installation.

> **Note:** When resuming an interrupted installation, you must not change the hosts or component host assignments you specified during the original installation.

To restart an interrupted installation, perform the following tasks:

1. Invoke the SA Installer using the temporary CDF that was created by the interrupted installation. For example:
   `/<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf_ts_temp.xml`

   where, **`<distro>`** is the full path to the *Product Software* (primary) media. Use the latest CDF as determined by the time stamp. See "How and when CDFs are saved".

   You see a screen similar to the following:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:

   <IP_address> (oracle_sas)

   ```

```
<IP_address> (word_store)
<IP_address> (gateway_master, osprov_boot_slice, slice, osprov_media)

Please select one of the following options:

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

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

where, **`<IP_address>`** is the IP address for the host(s) you specified during the interrupted installation (taken from the CDF).

2. Press **c** to continue.

   You see a screen similar to the following:

   ```
   Host Passwords
   ==============


   Parameter 1 of 6
   <IP_address> user [root]:
   Parameter 2 of 6
   <IP_address> password []:
   ```

3. Enter the OS credentials for each host specified as part of the installation.

   When all credentials have been entered, press **Y** to continue.

   ```
   All values are entered. Do you wish to continue? (Y/N) [Y]:
   End of interview.
   ```

   At this point, the SA Installer will check the state of any components already installed before the installation was interrupted.

4. Select the Install Type when prompted (must be the same as the Install Type selected for the interrupted installation).

   You see a screen similar to the following:

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


   Installed Components

   ```

```
Oracle RDBMS for SAS : <IP_address>
Model Repository, First Core : <IP_address>
Multimaster Infrastructure Components : <IP_address>
Software Repository Storage : <IP_address>
Slice : <IP_address>
OS Provisioning Media Server : <IP_address>
OS Provisioning Boot Server, Slice version : <IP_address>
Software Repository - Content (install once per mesh): <IP_address>

------------------------------------------

Select a component to assign

1. Slice

Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

5. Press **c** to continue.

   You see a screen similar to the following:

```
Interview Parameters
====================

Navigation keys:
Use <ctrl>P to go to the previous parameter.
Use <ctrl>N to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>C to abort the interview.


All prompts have values. What would you like to do:

1. Re-enter values
2. Continue

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

The SA Installer uses the parameter values specified in the CDF from the interrupted installation. You should not need to change these values.

6. Press **c** to continue.

   After the Installer completes initial preparation, you see a screen similar to the following:

```
Install components
==================

Components to be Installed
-------------------------
OS Provisioning Boot Server, Slice version: <IP_address>

Up-to-date Components (will not install)
----------------------------------------
Oracle RDBMS for SAS : <IP_address>
Model Repository, First Core : <IP_address>
Multimaster Infrastructure Components : <IP_address>
Software Repository Storage : <IP_address>
Slice : <IP_address>
OS Provisioning Media Server : <IP_address>
Software Repository - Content (install once per mesh): <IP_address>

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

   The uninstalled components are listed under **Components to be Installed**.

   The components that were installed before the interruption are listed under **Up-to-date Components** (and these will not be installed).

7. Press **c** to continue the installation from the point it was interrupted.

Installer logs

The SA Installer logs component installation output to a standard log file, /var/log/opsware/install_opsware/hpsa_installer_<timestamp>.log.

If the **--verbose** argument is specified, the installer generates verbose logs for various component installations at /var/log/opsware/install_opsware/. For example:

- <ip_address>-install-infrastructure-<timestamp>.verbose.log
- <ip_address>-install-osprov-<timestamp>.verbose.log
- <ip_address>-install-slice-<timestamp>.verbose.log
- <ip_address>-install-word_uploads-<timestamp>.verbose.log

Console output is logged to /var/log/opsware/install_opsware/hpsa_installer-<timestamp>.log

If you specify the **--verbose** and **--debug** options, the output to the console will be more verbose while the contents of the standard and verbose log files will remain the same.

Some SA Core Components have supplementary logs that contain additional details about the installation of those components.

For more information about SA Core Component logs, see the SA 10.60 Administration Guide.

The following log files are created during the installation of the Model Repository:

- /var/log/opsware/install_opsware/truth/truth_install_<number>.log
- /var/log/opsware/install_opsware/truth/truth_install_<number>_sql.log

SA parameter password security

During the SA installation or upgrade process, some cleartext passwords specified for core parameters are automatically obfuscated and some are not. Some passwords are obfuscated when SA Core Components start up. Passwords in some files must be manually obfuscated, such as passwords in the installation logs and Installer response files.

There are several ways to manually secure cleartext passwords. Which you choose will depend on your security requirements:

- Encrypt the response files and installation logs.
- Purge sensitive information from the Installer response files.
- Store the Installer response files and logs on a secure server.

"Cleartext passwords" The following table lists cleartext passwords that are automatically obfuscated and passwords that must be manually secured:

Cleartext passwords

Cleartext Password	Filename	Automatically Obfuscated	Manually Secured
`admin`	`/var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift`	✓	
`buildmgr`	`/var/opt/opsware/crypto/occ/twist.passwd` `/var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift`	✓ ✓	
`cleartext admin`	`/etc/opt/opsware/twist/startup.properties`	✓	
`detuser`	`/var/opt/opsware/crypto/twist/detuserpwd` `/var/opt/opsware/crypto/OPSWhub/twist.pwd`	✓ ✓	
`integration`	`/var/opt/opsware/twist/?DefaultAuthenticatorInit.ldift`	✓	
	Installer response files:		
	`/var/opt/opsware/install_opsware/cdf/* (infrastructure component host)`		✓
	`/var/log/cdf_tmp.xml (on host where installer invoked)`		✓
	`/var/opt/opsware/install_opsware/resp (pre-10.0 response files)`		✓
	`/var/tmp/*`		✓
	`/var/log/opsware/install_opsware/truth/truth_install_*`		✓
	`/var/log/opsware/install_opsware/hpsa_console_logs`	✓	
`spin`	`/etc/opt/opsware/spin/spin.args`	✓	
`vault`	`/var/opt/opsware/crypto/vault/vault.pwd`	✓	

Securing Installer log and CDFs

Depending on the level of your security requirements, it is recommended that the installation or upgrade team should encrypt or move installation log files to a secure server. Remember that certain CDFs are needed for SA Core upgrades and Secondary Core installations and the log files are useful for troubleshooting so completely removing them is not recommended.

SA Core installation process flow

The six main phases of the SA core installation process are summarized below. For more detailed information, see the cross references associated with each step.

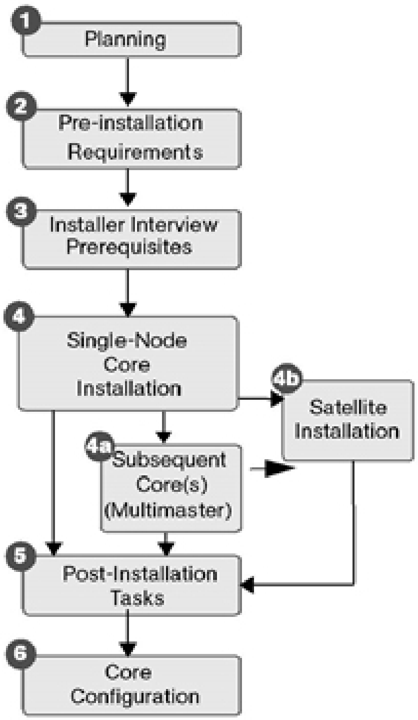
1. **Planning**: In the planning phase, you must decide which facilities and servers you will manage with SA. You must also choose the type of SA installation that is appropriate for your site(s) and ensure that you have the required hardware and software, including operating systems, and sufficient network connectivity.
   See the "SA Overview and Architecture" in the SA 10.60 Key Concepts Guide and "System requirements for installation " for more information.
2. **Pre-installation Requirements**: Before beginning a core installation, whether it is a Single Core or a core in a Multimaster Mesh, you must perform such administrative tasks as ensuring that host names can be resolved, required ports are open and available, and installing any necessary operating system utilities, packages, and/or patches.
   See "System requirements for installation "for more information.
3. **Prerequisite Information for the SA Installer Interview**: Installer Interview requires that you have certain information about your operational environment available. The information you provide will be saved into a Core Definition File (*CDF)*. You must gather this information and have it at hand as you run the pre-installation interview. Some examples of the information required are the name of the Facility to be managed by the core, the authorization domain, host names and IP addresses, and passwords used for SA users and the Oracle database, and so on.
   For a detailed description of the information required during the Installer Interview, see "SA Core parameter reference".
4. **SA Core Installation**: During this phase, you will run the Installer, complete the installation interview and install one of the following types of Cores:

- **First or Single Core Installation**: See "Install SA Core with a local SA-supplied database".
- **Secondary Core Installations for a Multimaster Mesh:** See "Install SA first (primary) core with a secondary Core (multimaster mesh)".

5. **Post-installation Tasks**: See "SA Core post-installation tasks".
6. **Core Configuration**: You will configure SA, performing tasks such as creating SA users and groups. At the end of this phase, SA is ready for operational use by system administrators. See the SA 10.60 Administration Guide for more information.

The following figure shows the overall process of an SA core installation.

SA Core Installation Process Flow


1
Planning
2
Pre-installation Requirements
3
Installer Interview Prerequisites
4
Single-Node Core Installation
4a
Subsequent Core(s) (Multimaster)
4b
Satellite Installation
5
Post-Installation Tasks
6
Core Configuration

SA Core parameter reference

This section describes configuration parameters that you will be required to specify values for during an SA Core installation.

Depending on the type of installation you are performing, Single-host, Simple or Advanced, you will be prompted to provide certain required parameter values.

These parameters provide values for:

- Passwords (SA Administrator, Database Administrator, etc.)
- Service Names (TNS name)
- Configuration parameter values
- Certification-related parameters
- Path names for programs, configuration file, logs
- IP Addresses for Core hosts and devices hosting Core components
- Gateway port numbers, and so on

The values you provide are used for the current installation and are saved to a Core Definition File (CDF) that you will use again later when upgrading the SA Core and when adding Secondary Cores for a Multimaster Mesh. This file is automatically saved during installation to /var/tmp and given a timestamp to aid you in identifying the file.

During installation, the SA Installer displays a series of parameters, some with default values that you can accept or modify, and other parameters that you must supply values for.

The number of parameters varies depending on whether you choose a single-host, standard, or advanced installation.

SA installation configuration parameters

You can use the following reference to gather the information that you will need for the SA installation.

The tables below, list the various parameters that you may be asked to provide values for. The parameters are labeled with the type of installation in which they appear (Single-host, Simple, and Advanced).

When you run the SA Installation script, the Installer prompts you to choose either the **Simple** or **Advanced** interview. If you choose Simple mode, the default values are used for certain values, for example, passwords for the Oracle database, the Model Repository (truth) and Data Access Engine (spin) user, ports used by the Gateways, among others. In Advanced Mode, you can select values other than the default, giving you finer control.

Configuration parameters by installation type

The configuration parameters you are asked to provide values for during the SA Installer Interview depend on the installation method you select:

- "Simple installation configuration parameters" below
- "Advanced installation configuration parameters" on page 74
- "Defining new facility parameters" on page 84
- "SA Core uninstallation configuration parameters" on page 86

Simple installation configuration parameters

The following table lists the simple installation configuration parameters and the expected values.

Simple installation configuration parameters

Parameter	Description
Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. If you are installing Oracle with SA the `opsware_admin` user will be created with this password. Make sure the password complexity matches the security guidelines in your organization. **Parameter:** `truth.oaPwd`	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks. If you are installing the SA-supplied Oracle database created by the Installer, the password you provide here will be associated with opsware_admin during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source**: Oracle DBA
Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source**: Variable **Example**: HEADQUARTERS
Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities.	Specify the directory to which you have already copied the Microsoft utilities required for Window’s Patch Management or enter “none” if you do not plan to perform Windows patching and do not want

Simple installation configuration parameters, continued

Parameter	Description
Parameter: `windows_util_loc`	to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client’s Import feature or the `populate-opsware-update-library` command line script as described in the Server Patching. **Source**: Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example**: `/tmp`
Please enter the IP address of the Management Gateway. **Parameter**: `mgw_address`	Specify the IP address of the Management Gateway. The Management Gateway manages Core-to-Core communications. Core Gateways installed on Secondary Cores and/or Satellite Gateways also communicate with the Management Gateway. **Source**: Variable **Example**: `192.168.165.242`
Do you want SA to be in FIPS mode? (y/n) [n] **Parameter**: `fips.mode`	Specify is FIPS mode will be enabled or disabled for the SA installation. **Source**: Variable **Example**: `y`
Enter the hashing algorithm for the SA cryptographic module. [SHA256]: **Parameter**: `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source**: Variable **Valid Values**: SHA1, SHA224, SHA256, SHA384, or SHA512.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter**: `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source**: Variable **Valid Values**: 2048 or 4096
Enter the hostname/IPaddress of the Oracle database server	Specify the hostname/IPaddress of the Oracle database server.

Simple installation configuration parameters, continued

Parameter	Description
Parameter: db.host	**Source**: Variable **Example**: 192.168.165.242
Enter the service name of the Model Repository instance in the facility where Opsware Installer is being run **Parameter**: truth.servicename	Specify the service name, also known as the *alias*, for the Model Repository. For a Single Core, this is the server on which you are running the Installer. If you are installing the default Oracle database created by the Installer, the service name you provide here will be associated with the database during installation. If you intend to use an existing Oracle database, you can find the service name by looking in the tnsnames.ora file on the Model Repository instance. The service name is the value before the first equals sign (=) in the file. The location of this file can vary, so check with your DBA if you are not sure where to find it. **Source**: Check with the DBA who created the Oracle database. **Example**: truth.example.com
Enter the SID of the Oracle instance containing the Model Repository **Parameter**: db.sid	Specify the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository is installed. If you are installing the SA-supplied Oracle database created by the Installer, the SID is truth. If you will be using an existing SA-supplied Oracle database, you will not be asked to supply this parameter. For an existing non-SA-supplied Oracle database, you can find the SID by looking in the tnsnames.ora file. The location of this file can vary, so check with your DBA if you are not sure where to find it. **Source**: Check with the DBA who created the Oracle database. **Default**: truth **Example**: DTC05
Enter the port on which the database is	Specify the port on which the Model Repository

Simple installation configuration parameters, continued

Parameter	Description
listening **Parameter**: `db.port`	database listens. **Source**: Variable **Example**: `1521`
Enter the path of the Oracle home directory. **Parameter**: `db.orahome`	Specify the base directory of the Oracle database installation. If you are installing the SA-supplied Oracle database created by the Installer, the default location of ORACLE_HOME is `/u01/app/oracle/product/12.1.0.2/db_2`. If you have an existing SA-supplied Oracle database, you will not be prompted for this parameter. For an existing non-SA-supplied Oracle database, you can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. (For a remote database installation, this parameter refers to the Oracle Client on the Model Repository server.) **Source**: The DBA who created the Oracle database. **Example**: `/u01/app/oracle/product/12.1.0.2/db_2`
Please enter the host (NFS server) where Software Repository Content resides. **Parameter** `word.store.host`	Specify the host name of the server where Software Repository content is stored. **Source**: Variable **Example**: `192.168.165.243`
Please enter the path to the server where Software Respiratory content resides. **Parameter** `word.store.path`	Specify the path to the server where Software repository content is stored. This will be to the server specified in word.store.host. **Source**: Variable
Please enter the OS Provisioning Boot Server IP address or hostname. **Parameter**: `bootagent.host`	Specify the IP address for server on which you installed the SA Provisioning Boot Server. **Important:** You must provide a valid IP address or host name that can be resolved from the server on which you installed the SA

Simple installation configuration parameters, continued

Parameter	Description
	Provisioning Boot Server component. Additionally, the host name must be resolvable by SA managed servers for SA Provisioning. **Source**: Variable **Example**: `foo.example.com`
Select a certificate mode to use in SA. **Parameter**: `crypto.certificateMode`	Specify the type of certificate mode you want to use: • **Self-signed**: SA uses its own Certificate Authorities (CAs) to automatically sign all the SA Core components certificates. • **Third-party**: SA generates CSRs for the certificates it needs. Submit these CSRs to your chosen CA for signing, and provide SA with the resulting certificates to complete the SA Core installation. **Source**: Variable **Example**: Self-signed
Enter the number of days for which a legacy certificate will be valid. **Parameter**: `crypto.legacyCertificateValidity`	Specify the number of days for which a temporary self-signed SA Agent certificate is valid. **Source**: Variable **Example**: 30

Advanced installation configuration parameters

The following table lists the advanced installation configuration parameters and the expected values.

Advanced installation configuration parameters

Parameter	Description
Please enter the database password for the `opsware_admin` user. This password is used to connect to the Oracle database. If you are installing Oracle with SA the `opsware_admin` user will be created with this password. Make sure the password complexity matches the	Specify the `opsware_admin` password created by your database administrator. `opsware_admin` is an Oracle user that the Installer uses during installation to perform required tasks.

Advanced installation configuration parameters, continued

Parameter	Description
security guidelines in your organization. **Parameter:** `truth.oaPwd`	If you are installing the SA-supplied Oracle database created by the Installer, the password you provide here will be associated with opsware_ admin during installation of the database. If you have an existing Oracle database installation, this must be the password that your DBA set for the `opsware_admin` user when setting up the Oracle instance on the server. **Source**: Oracle DBA
Enter the short name of the facility where the SA Installer is being run (no spaces). **Parameter:** `truth.dcNm`	Specify the short name of the facility where the Installer is being run. This would also be the location of the First Core. Some SA processes use this name internally. It must be in uppercase, less than 25 characters, and cannot contain spaces or special characters (underscores are allowed, dashes are *not* allowed). **Source**: Variable **Example**: HEADQUARTERS
Enter the hashing algorithm for the SA cryptographic module [SHA256]: **Parameter**: `crypto.hash_algorithm`	Specify the hashing algorithm that SA should use for the cryptographic module. **Source**: Variable **Valid Values**: SHA1, SHA224, SHA256, SHA384, or SHA512.
Enter the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module. [2048]: **Parameter**: `crypto.key_length`	Specify the key length to use for the cryptographic module hashing algorithm. **Source**: Variable **Valid Values**: 2048 or 4096
Enter the directory that contains the Microsoft patching utilities. (Press Ctrl-I for a list of required files) or enter "none" if you do not wish to upload these utilities. **Parameter**: `windows_util_loc`	Specify the directory to which you have already copied the Microsoft utilities required for Window's Patch Management or enter "none" if you do not plan to perform Windows patching and do not want to upload these files. Should you decide later that you need to perform Windows patching, you will need to install the required Windows Patch Management files either by using the SA Client's Import feature or the

Advanced installation configuration parameters, continued

Parameter	Description
	`populate-opsware-update-library` command line script as described in the Server Patching. **Source**: Variable, however, this directory *must* exist on the same server as the Software Repository (part of the Slice Component bundle). **Example**: `/tmp`
Please enter the IP address of the Management Gateway. **Parameter**: `mgw_address`	Specify the IP address of the Management Gateway. The Management Gateway manages Core-to-Core communications. Core Gateways installed on Secondary Cores and/or Satellite Gateways also communicate with the Management Gateway. **Source**: Variable **Example**: `192.168.165.242`
Please enter the password for the cryptographic material. **Parameter:** `decrypt_passwd`	Specify the password to use for decrypting cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for decrypting cryptographic material. **Password Restrictions**: The password cannot contain spaces and it must be between 4 and 20 characters long. **Source**: Variable **Example**: `x145_pwd03`
Enter the path of the Oracle home directory. **Parameter**: `db.orahome`	Specify the base directory of the Oracle database installation. If you are installing the SA-supplied Oracle database created by the Installer, the default location of ORACLE_HOME is `/u01/app/oracle/product/12.1.0.2/db_2`. If you have an existing SA-supplied Oracle database, you will not be prompted for this parameter.

Advanced installation configuration parameters, continued

Parameter	Description
	For an existing non-SA-supplied Oracle database, you can determine the Oracle home directory by logging in as the `oracle user` on the Model Repository server, and checking the value of the `$ORACLE_HOME` environment variable. (For a remote database installation, this parameter refers to the Oracle Client on the Model Repository server.) **Source**: The DBA who created the Oracle database. **Example**: `/u01/app/oracle/product/12.1.0.2/db_2`
Please enter the host (NFS server) where Software Repository Content resides. **Parameter** `word.store.host`	Specify the host name of the server where Software Repository content is stored. **Source**: Variable **Example**: `192.168.165.243`
Please enter the path to the server where Software Respiratory content resides. **Parameter**: `word.store.path`	Specify the path to the server where Software repository content is stored. This will be to the server specified in word.store.host. **Source**: Variable
Please enter the OS Provisioning Boot Server IP address or hostname. **Parameter**: `bootagent.host`	Specify the IP address for server on which you installed the SA Provisioning Boot Server. **Important:** You must provide a valid IP address or host name that can be resolved from the server on which you installed the SA Provisioning Boot Server component. Additionally, the host name must be resolvable by SA *managed servers for SA Provisioning.* **Source**: Variable **Example**: `foo.example.com`
Please enter the password for the SA admin user. this is the password that will be used to authenticate the user admin to SA. **Parameter**: `cast.admin_pwd`	Specify the password for the SA `admin` user. **Password Restrictions**: This password cannot contain spaces. The Installer automatically creates the `admin` user. The first time you log in to the SA Client to access a new Facility, you must log in as the `admin` user.

Advanced installation configuration parameters, continued

Parameter	Description
	Source: Variable **Example**: `x145_pwd03`
Enter the fully qualified path to the directory where the export file will be saved. **Parameter**: `truth.dest`	You must create this directory on the Model Repository server before you run the Installer. Specify the directory in which the `truth.<new_facility>.tar.gz` file will be saved. This directory must reside on the Model Repository server in the source facility. You will see this prompt only when defining a new facility (hpsa_add_dc_to_mesh.sh). **Note**: When adding a facility to a Multimaster Mesh, you must export the Model Repository from the source facility, then copy it to the destination facility. **Source**: Variable **Default**: `/var/opt/opsware/truth/`
Enter the fully qualified path to the directory that contains the export file. **Parameter**: `truth.sourcePath`	This parameter is used when a new facility is added to a Multimaster Mesh and the source export file is copied to the new facility. This directory must exist on the server and contain the database export file before you run the Installer on the server. Specify the directory on the destination facility’s Model Repository server to which you copied the export data file from the source facility. **Source**: Variable **Default**: `/var/opt/opsware/truth/`
Please enter the Facility ID (number only, less than or equal to 950, with no leading zeros). **Parameter**: `truth.dcId`	Specify an ID that uniquely identifies the facility. When you install the First Core, you will be prompted to provide this ID. When you install Secondary Cores in the same Multimaster Mesh, SA automatically generates the Facility ID when you add a new facility using the SA Client. You can determine the Secondary Core’s Facility ID by logging in to the SA Client at the First Core facility, then select **Facilities** under **Administration** in the Navigation pane and click

Advanced installation configuration parameters, continued

Parameter	Description
	the facility’s name. **ID Restrictions**: The Facility ID value is capped at 950. Therefore, you must specify a number for the first facility that is far enough below 950 that you will have sufficient IDs available to continue adding facilities to your Multimaster Mesh. **Source:** Variable for the first facility; set by the SA for subsequent facilities. **Default**: 1
Would you like this facility to mirror all Software Repository content in the mesh? **Parameter**: `word.enable_content_mirroring`	Enables mirroring (replication) of the Software Repository (word). **Source**: Variable **Default**: Y
Enter the SID of the Oracle instance that contains the Data Model Repository. **Parameter**: `db.sid`	Specify the database system ID (SID) that was set when Oracle was installed on the server where the Model Repository is installed. If you are installing the SA-supplied Oracle database created by the Installer, the SID is `truth`. If you have an existing SA-supplied Oracle database, you will not be asked to supply this parameter. For an existing non SA-supplied Oracle database, you can find the SID by looking in the `tnsnames.ora` file. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Default**: truth **Example**: `DTC05`
Enter the fully-qualified path to the TNS admin directory (where the `tnsnames.ora` file resides). **Parameter**: `truth.tnsdir`	Specify the directory that contains the `tnsnames.ora` file. **Note**: This directory and path must be the same on all servers in a core. For example, since the Data Access Engine must access the `tnsnames.ora` file to connect to the

Advanced installation configuration parameters, continued

Parameter	Description
	Model Repository, the location of tnsnames.ora directory on the Data Access Engine server must be the same as the directory location on the Model Repository server. If you are installing the SA-supplied Oracle database created by the Installer, the `tnsnames.ora` file will be installed under `/var/opt/oracle.` If you have an existing SA-supplied Oracle database installed, you will not be prompted for this parameter. If you have an existing non-SA-supplied Oracle database, the location of the `tnsnames.ora` file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Example**: `/var/opt/oracle`
Please enter the port on which the Model Repository database is listening. **Parameter**: `db.port`	Specify the port on which the Model Repository database listens. If you have an existing SA-supplied Oracle database, you will not be asked to supply this parameter. **Source**: Variable **Default**: 1521
Please enter the absolute path on the NFS server for the Opsware Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Parameter**: `ogfs.store.path`	Specify the absolute path on the NFS server for the Global File System (`/user`, `/home`, and `/tmp` directories). This value should be different from `ogfs.audit.path` and `word.store.path`. **Source**: Variable **Default**: `/var/opt/opsware/ogfs/export/store`
Please enter the absolute path on the NFS server for the Opsware Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Parameter**:	Specify the absolute path on the NFS server for the Global File System where the audit streams will be stored. This value should be different from `ogfs.store.path` and `word.store.path`. **Source**: Variable

Advanced installation configuration parameters, continued

Parameter	Description
`ogfs.audit.path`	**Default**: `/var/opt/opsware/ogfs/export/audit`
Please enter the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. Typically it's set to 2001.) **Parameter**: `masterCore.mgw_tunnel_listener_port`	Specify the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of `mgw_tunnel_listener_port` parameter in First Core's CDF. **Source**: Variable **Default**: None
Enter the port on which the Management Gateway will listen for connections from other gateways. **Parameter**: `mgw_tunnel_listener_port`	Specify the port on which the First and Secondary Cores' Management Gateways will listen for connections from other Core and Satellite gateways. **Source**: Variable **Example**: 2001
Please enter the port on which Agents can contact the Agent Gateway to request connections to Core Components. **Parameter**: `agw_proxy_port`	Specify the port that agents should use to connect to the SA Core. **Source**: Variable **Default**: 3001
Please enter the pathname to the Linux media. **Parameter**: `media_server.linux_media`	Specify the path to the Linux OS media on the server on which the Media Server will be installed. Providing the path to the Linux OS media does not actually copy the media to the Media Server. See the "OS Provisioning" section in the the *SA* 10.60 Administration Guide for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/linux`
Please enter the pathname to the Solaris OS media. **Parameter**: `media_server.sunos_media`	Specify the path to the Sun Solaris OS media on the server on which the Media Server will be installed. Providing the path to the Solaris OS media does not

Advanced installation configuration parameters, continued

Parameter	Description
	actually copy the media to the Media Server See the "OS Provisioning" section in the the *SA* 10.60 Administration Guide for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/solaris/`
Please enter the pathname to the Windows OS media. **Parameter**: `media_server.windows_media`	Specify the path to the Microsoft Windows OS media on the server on which the Media Server will be installed. The SA Provisioning feature exports Windows OS media to SMB clients through a Samba share. Providing the path to the Windows OS media does not actually copy the media to the Media Server. See the "OS Provisioning" section in the the *SA* 10.60 Administration Guide for the steps required to set up the media on the Media Server for SA Provisioning. **Source**: Variable, however, this directory must exist on the server where the Media Server is installed. **Default**: `/media/opsware/windows/`
Please enter the host name or IP address of the Network Automation (NA) server. (Enter “none” if NA is not installed.) **Parameter**: `twist.nasdata.host`	Specify the host name or IP address of the server running HPE Network Automation (NA), if installed. If NA is not installed, accept the default value `none`. Enter a value without spaces. **Source**: The network administrator/SA administrator who installed HPE Network Automation. **Example**: `192.168.165.242`
Please enter the username used to connect to HPE Live Network. (Leave as "none" if HPELN is not being configured.) **Parameter**:	Specify the username used to connect to the HPE Live Network (HPELN). The value should adhere to HPELN's standard. A minimum of 5 characters and it cannot contain the

Advanced installation configuration parameters, continued

Parameter	Description
hpln_user_name	special characters &, |, or *. Also, any of the invalid characters defined for the SA install also apply, such as leading #, quotes, and so on **Source**: Variable **Default**: None
Please enter the password associated with the username used to connect to HPE Live Network. (Leave as "none" if HPELN is not being configured.) **Parameter**: hpln_password	Specify the HPELN user password used to connect to the HPE Live Network (HPELN). The value must follow the same rules as hpln_user_name, except the minimum characters accepted is 6. **Source**: Variable **Default**: None
Please enter the address of the proxy used to connect to the HPE Live Network. (Leave as "none" if HPELN is not being configured or no proxy is needed to connect to HPE Live Network.) **Parameter**: hpln_proxy	Specify the IP address or hostname of the proxy used to connect to the HPE Live Network (HPELN) The value must follow the following format: <protocol>://<host> or <protocol>://<host>:<port>. If no <port> value is provided, the default 3128 is used. **Source**: Variable **Default**: None
Please enter the username of the proxy user required to connect to the HPE Live Network. (Leave as "none" if HPELN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: hpln_proxy_user	Specify the username for the HPELN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. Source: Variable Default: None
Please enter the password of the proxy user required to connect to the HPE Live Network. (Leave as "none" if HPELN is not being configured, no proxy is configured or if no username is needed.) **Parameter**: hpln_proxy_pwd	Specify the password for the HPELN proxy user. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on. **Source**: Variable **Default**: None

Advanced installation configuration parameters, continued

Parameter	Description
Please enter the gateway Bandwidth Configuration Management for remote connections port. **Parameter**: `opswgw.ConfigPort`	Specify the port to be used for pushing bandwidth configurations to Satellite Gateways. **Source**: Variable **Default**: None
Please enter the gateway bandwidth usage channel port. **Parameter**: `opswgw.BwUsageChannelPort`	Specify the port to be used for retrieving Satellite Gateway bandwidth usage information. **Source**: Variable **Default**: None
Select a certificate mode to use in SA. **Parameter**: `crypto.certificateMode`	Specify the type of certificate mode you want to use: • **Self-signed**: SA uses its own Certificate Authorities (CAs) to automatically sign all the SA Core components certificates. • **Third-party**: SA generates CSRs for the certificates it needs. Submit these CSRs to your chosen CA for signing, and provide SA with the resulting certificates to complete the SA Core installation. **Source**: Variable **Example**: Self-signed
Enter the number of days for which a legacy certificate will be valid. **Parameter**: `crypto.legacyCertificateValidity`	Specify the number of days for which a temporary self-signed SA Agent certificate is valid. **Source**: Variable **Example**: 30

Defining new facility parameters

A *Facility* is a system object that represents a specific geographical location (such as Sunnyvale, Plano, Sacramento, or a data center). Servers and users are often associated with a facility as a means to enforce access rights and privileges. If you are performing a Single Core installation, your deployment is a single facility. Multimaster installations, however, consist of two or more facilities.

In this section, the first core installed in a Multimaster Mesh is called the *First Core*, and is the core that has the first Model Repository installed. *Secondary Cores* are the second, third, and fourth (and so on) cores installed in the mesh. For historical reasons, First Cores are sometimes referred to in parameter names as *Master* and Secondary Cores as *Slave*.

The following table lists the parameters you see when defining a new Facility and the expected values.

Define new facility parameters

Parameter	Description
Enter the short name of the new facility you would like to define **Parameter**: `newCore.dcNm`	Specify the default facility name for the Secondary Core. Some SA processes use this name internally. It must be less than 25 characters, and cannot contain spaces or special characters (both dashes and underscores are allowed). **Source**: Variable **Example**: NORTHSIDE
Enter the IP address of the host where you want to install the Model Repository in the new facility. **Parameter**: `newCore.dbHost`	Specify the IP address of the host on which you will install the Model Repository for the new target core. **Source**: Variable **Example**: `192.168.165.242`
Please enter the SID of the Oracle instance containing the Model Repository for the new facility. **Parameter**: `newCore.dbSid`	Specify the database system ID (SID) of the Oracle instance that will contain the Model Repository for the new facility. You will need to supply this parameter only if you will be using a remote non-SA supplied Oracle database. **Source**: Variable **Example**: `truth`
Please enter the port on which the database is listening for the new facility. **Parameter**: `newCore.dbPort`	Specify the port on which the new facility’s Model Repository database will listen. You will need to supply this parameter only if you will be using a remote non-SA supplied Oracle database. **Source**: Variable **Example**: `1521`
Please enter the IP address of the device where you are planning to install the Infrastructure component in the new facility (or where the management gateway will be installed).	Specify the IP address of the host on which you will install the Infrastructure Component bundle or the host on which the Management Gateway will be installed. **Source**: Variable

Define new facility parameters, continued

Parameter	Description
Parameter: `newCore.mgwIP`	**Example**: 192.168.165.202
Enter the subdomain for the facility you are about to create (lowercase, no spaces). **Parameter:** newCore.dcSubDom	Specify the fully-qualified DNS subdomain where the Destination Multimaster Core is to be deployed. This value must be *unique* for each core in the Multimaster Mesh, both Source and Destination Cores. The value is based on the VLAN for the facility in which you are installing the Multimaster core. The subdomain name must be in lowercase with no spaces, less than 50 characters, and in subdomain format. **Source**: Your network administrator. **Example**: dc2.example.com
Enter the service name (aka TNS name) of the Model Repository instance. **Parameter:** `newCore.servicename`	Specify the service name, also known as the *alias*, for the core's Model Repository. You will see this prompt only when installing a new First Core. If this is a new installation, the service name you specify will be associated with the Model Repository during installation. If you plan to use an existing Model Repository, you can find the service name by looking in the `tnsnames.ora` file on the Model Repository instance. The location of this file can vary, so check with your DBA if you are not sure where to look. **Source**: The DBA who created the Oracle database. **Example**: `truth02.example.com`

SA Core uninstallation configuration parameters

The following table lists the SA Core uninstallation configuration parameters and the expected values.

SA Core uninstallation parameters

Parameter	Description
Are you absolutely sure you want to remove all packages in the repository? [Y/N]	If you answer Yes, the packages, logs, and cryptographic material for the Software Repository are removed.

SA Core uninstallation parameters, continued

Parameter	Description
Parameter: `word.remove_files`	**Default**: None
Are you absolutely sure you want to remove users' OGFS home and audit directories? (home and audit directories will only be removed if they are stored on the Software Repository server) (Y/N)? Parameter: `ogfs.remove_home_dirs`	Respond Yes if you want the uninstall to remove all users' OGFS home and audit directories. Backup any information you want to retain. Source: Variable Default: None
Do you need to preserve any of the data in this database? [Y/N] **Parameter**: `truth.uninstall.needdata`	Uninstalling the Model Repository permanently deletes all data in the database, therefore, the uninstallation process stops if you reply Yes to this prompt. If you want to do an uninstallation, backup your data, run the uninstallation again and answer No to this prompt. Remember, the Installer *does not* preserve any data. **Default**: Y
Are you sure you want to remove all data and schema from this database? [Y/N **Parameter:**`truth.uninstall.aresure`	Uninstalling the Model Repository by responding Yes permanently deletes all data in the database. You can stop the uninstallation by responding No to this prompt. Default: None
Would you like to preserve the database of cryptographic material? [Y/N] **Parameter**: `save_crypto`	If you answer Yes, the database of cryptographic material is saved. If you answer No, the material is deleted as part of the uninstallation. Default: None
Would you like to preserve the HPELN content? (Y/N) Parameter: `hpln.uninstall.keepcontent`	Responding No uninstalls all HPE Live Network content. Source: Variable Default: None
Parameter	Description
Are you absolutely sure you want to remove all packages in the repository? [Y/N]	If you answer Yes, the packages, logs, and cryptographic material for the Software Repository are removed.

SA Core uninstallation parameters, continued

Parameter	Description
Parameter: `word.remove_files`	**Default**: None
Are you absolutely sure you want to remove users' OGFS home and audit directories? (home and audit directories will only be removed if they are stored on the Software Repository server) (Y/N)? Parameter: `ogfs.remove_home_dirs`	Respond Yes if you want the uninstall to remove all users' OGFS home and audit directories. Backup any information you want to retain. Source: Variable Default: None
Do you need to preserve any of the data in this database? [Y/N] **Parameter**: `truth.uninstall.needdata`	Uninstalling the Model Repository permanently deletes all data in the database, therefore, the uninstallation process stops if you reply Yes to this prompt. If you want to do an uninstallation, backup your data, run the uninstallation again and answer No to this prompt. Remember, the Installer *does not* preserve any data. **Default**: Y
Are you sure you want to remove all data and schema from this database? [Y/N **Parameter:** `truth.uninstall.aresure`	Uninstalling the Model Repository by responding Yes permanently deletes all data in the database. You can stop the uninstallation by responding No to this prompt. Default: None
Would you like to preserve the database of cryptographic material? [Y/N] **Parameter**: `save_crypto`	If you answer Yes, the database of cryptographic material is saved. If you answer No, the material is deleted as part of the uninstallation. Default: None
Would you like to preserve the HPELN content? (Y/N) Parameter: `hpln.uninstall.keepcontent`	Responding No uninstalls all HPE Live Network content. Source: Variable Default: None

Full SA Core configuration parameter listing

The SA Installer provides an Expert level interview which displays and allows modifications of all SA Core configuration parameters, some of which are not displayed during the Simple or Advanced interviews. Modifying these parameters requires extensive knowledge of SA Core capabilities and configuration and applying incorrect values will cause unexpected results.

The following table lists all SA Core configuration parameters as seen when you perform an installation using the Expert level interview.

For a detailed description of these parameters their values and ranges, see "SA Core parameter reference".

Full SA Core configuration parameter list

Parameter	Default Value	Description
agw_proxy_port	3001	This port must be open between the Agents in this facility and the Agent Gateway. Agents will contact the Agent Gateway on this port to request connections to core components
bootagent.host	Provisioning Boot Server host	Specify the SA Provisioning Boot Server IP address or hostname.
cast.admin_pwd	Value of truth.oaPwd	Specify the password for the SA admin user. The Installer automatically creates the admin user. The first time you log in to the SA Client to access a new Facility, you must log in as the admin user. Password Restrictions: This password cannot contain spaces.
cgw_admin_port	8085	Specify the port for the administrative interface of the core Gateway. The Gateway has a browser-based administrative interface that allows you to view configuration and monitor traffic.

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
cgw_proxy_port	3002	Specify the port on which core components can contact this core Gateway to request tunneled connections.
cgw_slice_tunnel_listener_port	2003	Specify the port on which the core Gateway on the Slice Component bundle will listen for connections from other Gateways (only used if the Infrastructure component bundle is installed on the same box as the Slice Component bundle).
crypto.hash_algorithm	SHA256	Please enter the hashing algorithm for SA cryptographic module.
crypto.key_length	2048	Specify the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
db.host	none	Specify the hostname/IP address of the Oracle database server.
db.orahome	/u01/app/oracle/product/12.1.0.2/db_2	Specify the path of the `ORACLE_HOME` directory of your Model Repository (truth) server.
db.port	1521	Specify the port on which the database listens for incoming connections. This value is recorded in the `tnsnames.ora` file.
db.sid	truth	Specify the SID of the Oracle instance containing the Model Repository.
decrypt_passwd	Value of truth.oaPwd	Specify the password for the cryptographic material. This password must be the same across all cores in a Multimaster Mesh. If you have an existing SA installation, this must be the password previously set for

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		decrypting cryptographic material. Password Restrictions: The password cannot contain spaces and it must be between 4 and 20 characters long.
hpln_password	none	Specify the user password used to connect to the HPE Live Network (HPELN). Specify "none" if HPELN is not being configured. The value must follow the same rules as `hpln_user_name`, except the minimum characters accepted is 6.
hpln_proxy	3128	Specify the IP address or hostname of the proxy used to connect to the HPE Live Network (HPELN). Specify "none" if HPELN is not being configured or no proxy is needed to connect to HPE Live Network. The value must follow the following format: <protocol>://<host> or <protocol>: //<host>:<port>. If no `<port>` value is provided, the default 3128 is used.
hpln_proxy_pwd	none	Specify the password for the HPELN proxy user. Specify "none" if HPELN is not being configured, no proxy is configured, or no password is required. The invalid characters for this parameter follow the SA convention for usernames, such as no leading `#`, no quotes, no

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		whitespace, and so on.
hpln_proxy_user	none	Specify the username for the HPELN proxy user. Specify "none" if HPELN is not being configured, no proxy is configured, or no username is required. The invalid characters for this parameter follow the SA convention for usernames, such as no leading #, no quotes, no whitespace, and so on.
hpln_user_name	none	Specify the username used to connect to the HPE Live Network (HPELN). Specify "none" if HPELN is not being configured. The value should adhere to HPELN's standard. A minimum of 5 characters and it cannot contain the special characters &, |, or *. Also, any of the invalid characters defined for the SA install also apply, such as leading #, quotes, and so on.
masterCore.mgw_ tunnel_listener_port	2001	Specify the port on which Management Gateway in the First Core listens for connections from other Gateways (this value should match the value of the mgw_tunnel_listener_port parameter for the First Core (typically 2001).
media_server.linux_ media	/media/opsware/linux	Specify the path to the location on the Media Server where the Linux media shouldbe placed when SA Provisioning components are installed. **Note:** Providing the path to the Linux OS media does not actually copy the media to

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		the Media Server. See the "OS Provisioning" section in the SA 10.60 Administration Guide for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.
media_server.sunos_ media	/media/opsware/solaris/	Specify the path to the location on the Media Server where the Oracle Sun Solaris OS media should be placed when SA Provisioning components are installed. Note: Providing the path to the Solaris OS media does not actually copy the media to the Media Server See the "OS Provisioning" section in the SA 10.60 Administration Guide for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.
media_server.windows_ media	/media/opsware/windows	Specify the path to the location on the Media Server where the Windows OS media should be placed when SA Provisioning components are installed. The SA Provisioning feature exports Windows OS media to SMB clients through a Samba share. **Note:** Providing the path to the Windows OS media does not actually copy the media to the Media Server

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		See the "OS Provisioning" section in the SA 10.60 Administration Guide for the steps required to set up media on the Media Server. This directory must exist on the Media Server host.
media_server.windows_share_name	OSMEDIA	Specify 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.
media_server.windows_share_password	Value of truth.oaPwd	Specify a password to write-protect the Windows media share. The `import_media` tool will prompt for this password each time it is run.
mgw_address	none	Specify the IP address of the Management Gateway.
mgw_proxy_port	3003	Specify the port number through which Core Components can request tunneled connections to other components through the Management Gateway.
mgw_tunnel_listener_port	2001	Specify the port on which the First and Subsequent Cores' Management Gateways will listen for connections from other Core and Satellite gateways.
ogfs.audit.host.ip	Value of word.store.host	Specify the IP address of the NFS server for the Global File System where audit streams will be stored.
ogfs.audit.path	/var/opt/opsware/ogfs/export/audit	the absolute path on the nfs server for the Opsware Global File System where the audit

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		streams will be stored. This value should be different from *ogfs.store.path* and *word.store.path*
ogfs.store.host.ip	Value of word.store.host	Specify the IP address of the NFS server for the Opsware Global File System (user, home, and tmp directories).
ogfs.store.path	/var/opt/opsware/ogfs/export/store	Specify the absolute path on the NFS server for the Global File System (user, home, and tmp directories). This value should be different from *ogfs.audit.path* and *word.store.path*
spoke.cachedir	/var/opt/opsware/compliance cache	Specify the directory in which the Global File System service will cache snapshots and audits for quick access. This directory can require a large amount of disk space (4Gb by default)
truth.aaaPwd	Value of truth.oaPwd	Enter database password for the AAA user.
truth.authDom	MY.CUSTOMER.COM	Enter the authorization domain used by the Access and Authentication Directory.
truth.dcNm	none	Specify the short name of the facility in which the SA Installer is being run (no spaces).
truth.dcSubDom	Value of truth.dcNm	Specify the subdomain for the facility in which the SA Installer is being run (lowercase, no spaces). The value must be a valid domain name (for example, SUB.DOMAIN.COM) and is limited to 50 characters.
truth.detuserpwd	Value of truth.oaPwd	Specify the password to use for the DCML exchange tool (DET) user.
truth.gcPwd	Value of truth.oaPwd	Specify database password for

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		the `gcadmin` user.
truth.lcrepPwd	Value of truth.oaPwd	Specify the database password for the `lcrep` user.
truth.oaPwd	None	Specify the password for the `opsware_admin` user. This is the password used to connect to the Oracle database. If you are installing Oracle with SA the opsware_admin user will be created with this password. Make sure the password complexity matches the security guidelines in your organization.
truth.pubViewsPwd	Value of truth.oaPwd	Specify the database password for the `public views` user.
truth.servicename	truth.<value of truth.dcNm>	Specify the service name of the Model Repository instance in the facility where SA Installer is being run. For Oracle, you can identify the service name by looking in the `tnsnames.ora` file on the Model Respository instance. Locate the appropriate TNS entry in this file for the Model Repository and note the value before the first "`=`" sign. For example, if the database name is "`truth`", the entry may look like "`truth=(DESCRIPTION=(...))`". The location and contents of this file can vary, check with your DBA if you are not sure where to look.
truth.sourcePath	/var/opt/opsware/truth	Specify the full path to the directory containing the source_db_charset.txt file. When adding a facility to a multimaster mesh, the Model Respository (truth) data must be exported from the source facility,

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		then copied to the destination facility. The destination directory path must be the same as the directory on the Model Repository (truth) server as the source directory path.
truth.spinPwd	Value of truth.oaPwd	Specify the database password for the `spin` user.
truth.tnsdir	/var/opt/oracle	Specify the path to the TNS admin directory (where the `tnsnames.ora` file resides)
truth.truthPwd	Value of truth.oaPwd	Specify the database password for the `truth` user.
truth.twistPwd	Value of truth.oaPwd	Specify the database password for the `twist` user.
truth.vaultPwd	Value of truth.oaPwd	Specify the database password for the `vault` user.
twist.default_gid	70001	Specify the default UNIX Group ID to assign to SA users (number only, no less than 1024 and no greater than 90000000, with no leading zeros
twist.integration.passwd	Value of truth.oaPwd	Specify the password for the `Integration` user.
twist.min_uid	80001	Specify the minimum ID to use when assigning UNIX User IDs to Opsware users (number only, no less than 1024 and no greater than 90000000, with no leading zeros). UNIX UIDs are generated automatically for each SA user. UIDs are allocated counting up from the minimum specified in this parameter.
twist.nasdata.host	none	Specify the hostname or IP address of the NA (Network Automation) server (Enter "none" if NA is not installed).

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
windows_util_loc	none	Specify the path to the directory in which SA should install the Microsoft patching utilities or, if you have already manually downloaded the utilities, the path to the directory that contains the files. For a list of required files, press Ctrl-I at the prompt. Enter "none" if you do not wish to install the utilities.
word.enable_content_ mirroring	Y(es)	Enable/disable mirroring of all Software Repository content in a Multimaster Mesh.
word.store.host	Software Repository Storage host	Specify the IP address of the NFS server for the Software Repository. For satellite installs, enter the IP address of the Software Repository Cache. Storage for the Software Repository will be mounted from the server specified in this parameter..
word.store.path	/var/opt/opsware/word	Specify the absolute path on the NFS server for the Software Repository. Storage for the Software Repository will be mounted from this directory on the server specified by the *word.store.host* parameter. Ensure that this directory has sufficient free disk space. This value should be different from *ogfs.store.path* and *ogfs.audit.path*
word_root	/var/opt/opsware/word	Specify the mount point for the Software Repository root directory. For satellite installs, enter the root directory of the Software Repository Cache. Package Repository contents will be mounted from the server and

Full SA Core configuration parameter list, continued

Parameter	Default Value	Description
		directory specified by *word.store.host* and *word.store.path* parameters, respectively.
word_tmp_dir	/var/opt/opsware/wordbot_ tmp/	Specify the directory where the Package Repository will temporarily place content during uploads.
crypto.certificateMode	self-signed	Specify the type of certificate mode you want to use: • **Self-signed**: SA uses its own Certificate Authorities (CAs) to automatically sign all the SA Core components certificates. • **Third-party**: SA generate CSRs for the certificates it needs. Submit these CSRs to your chosen CA for signing, and provide SA with the resulting certificates to complete the SA Core installation.
crypto.certificateValidity	1	Specify the number of days for which a temporary self-signed SA Agent certificate is valid. Change the current default value of one day to a more relevant period of time.

Oracle setup for the Model Repository

This section explains how to install, configure, and maintain an Oracle database to support the SA Model Repository.

You can easily install the SA-supplied database by running the SA Installer and selecting the option to install the database, either as a local database or on a remote database server by providing the IP address of the remote host.

The primary benefit of using the SA-supplied Oracle database is ease of installation for small or medium sized installations. The SA-supplied database is installed with a configuration that is optimized and tested for use with SA. The SA-supplied database has also been updated with all available patches/PSUs released by Oracle and has been tested to insure compatibility of the database with SA.

Some customers may already have an installed Oracle database or may have larger SA requirements that would benefit from a dedicated Oracle database server. If you have an existing Oracle database you prefer to use or want to install the Oracle database for use by SA yourself, then you can run the SA Installer and choose the option to use an existing Oracle database. Again, this database must be installed and up-and-running and you must have access to the database before you run the SA Installer.

> **Note:** If you plan to use an Oracle database you have installed yourself, you must ensure that the database meets the minimum requirements and configuration documented in this section.

Supported Oracle versions and operating systems

Support for the Model Repository is limited to certain versions of Oracle running on certain versions of operating systems. HPE strongly recommends that you also apply the latest Oracle CPU or PSU patches.

See the SA Support and Compatibility Matrix for a list of supported Oracle versions and operating systems.

System requirements for Oracle database

The following sections list the system requirements for Oracle 11g and 12c. The SA Installer performs an automated check to ensure that these requirements are met on the Oracle host.

The system requirements and configurations listed in this section apply both to the SA-supplied Oracle RDBMS software as well as to non-SA-supplied Oracle RDBMS and software installations.

> Note: If you create the database using the Oracle Universal Installer rather than the SA Installer, you must check for these packages and patches manually.

> Note: The Oracle database must be installed either on its own host or on a server that has the SA Infrastructure Component bundle installed.

Database server time requirements

Database servers must meet the following requirements. These time requirements do not apply to Managed Servers.

- All SA database servers must have their time zone set to Coordinated Universal Time (UTC).
- All SA database servers must maintain synchronized system clocks. Typically, you will synchronize the system clocks through an external server that uses NTP (Network Time Protocol) services.

Linux time configuration

To configure the time zone on a Linux server, copy or link **/usr/share/zoneinfo/UTC** to **/etc/localtime** and ensure that the /etc/sysconfig/clock file contains the following lines:

```
ZONE="UTC"

UTC=true
```

Hostname setup

1. You must be able to ping the database server host name. To verify this, enter the following command:
   ```
   # ping <hostname>
   ```
2. Check that the database server name is FQDN by using the following command:
   ```
   # hostname -f
   ```

If the host name is not configured correctly, Oracle will not start and you will encounter the following error:

```
ORA-00600: internal error code, arguments: [keltnfy-ldmInit], [46], [1], [], [],
[], [], []
```

Hardware requirements

The server that will host the Oracle database for the Model Repository must meet the hardware requirements listed in this section.

- **Linux requirements**
  The following are hardware requirements for running Oracle 11g and 12c under Linux.

  For detailed Linux requirements, see the Oracle® Database Quick Installation Guide11g Release 2 (11.2) for Linux x86-64 (Part Number E24326-02) and *Oracle® Database Quick Installation Guide12c Release 1 (12.1) for Linux x86-64* (Part Number E17718-09) available at: *http://docs.oracle.com*

  - Determine the processor type to verify that the processor’s architecture matches the Oracle software release you will install. Use the following command to check system architecture:

    ```
    # uname -m
    ```

  - The recommended physical memory is 32 GB or more of RAM and 12 CPUs. If the machine running the Oracle database is a virtual machine, then the amount of RAM should be fully allocated to that machine. An SA-supplied Oracle installation will use a minimum of 2 GB memory. The Oracle SGA memory can be increased after database installation. You can use the following command to check memory status:

```
grep MemTotal /proc/meminfo
```

- Required available swap space is shown below:

  Required available RAM Swap Space

RAM	Available Swap Space
4 GB and 16 GB	Equal to the size of RAM
More than 16 GB	16 GB

  You can use the following command to check swap space:

  ```
  grep SwapTotal /proc/meminfo
  ```

- As of Oracle 11g, Automatic Memory Management (AMM) requires more shared memory (`/dev/shm`) and file descriptors. Shared memory should be sized to be at least the greater of `MEMORY_MAX_TARGET` and `MEMORY_TARGET` for each Oracle instance on a database server. You can use the following command to check available shared memory:

  ```
  df -h /dev/shm/
  ```

- Free `tmp` space should be 1GB or more of /tmp directory space. You can use the following command to check `tmp` space:

  ```
  df -h /tmp
  ```

- **Solaris requirements**

  See "Oracle Sun Solaris equirements" and "HP-UX and IBM AIX version and package requirements".

- **HP-UX and IBM**

  Refer to the Checking the Hardware Requirements section in the following Oracle documents:

  - Database Quick Installation Guide for HP-UX Itanium
  - Database Quick Installation Guide for IBM AIX on POWER Systems (64-Bit)

- **Oracle Sun Solaris**

  The following are hardware requirements for running Oracle 11g under Oracle Sun Solaris:

For detailed Solaris requirements, see the *Oracle® Database Quick Installation Guide 11g Release 2 (11.2) for Oracle Solaris on SPARC (64-Bit)*, Part Number E24349-03 and *Oracle® Database Quick Installation Guide 12c Release 1 (12.1) for Oracle Solaris on SPARC (64-Bit)*, Part Number E17756-08 available from http://docs.oracle.com.

- Determine the processor type to verify that the processor architecture matches the Oracle software release you will install. Use the following command to check system architecture:

  ```
  # /bin/isainfo -kv
  ```

- The recommended physical memory is 32 GB or more of RAM. An SA-supplied Oracle installation will use around 2 GB of memory. The Oracle SGA memory can be increased after database installation.
  You can use the following command to check the physical memory:

  ```
  /usr/sbin/prtconf | grep "Memory"
  ```

- **Solaris operating system-specific patches**
  - The following patches for Oracle Sun Solaris 10 must be installed:
    - 120753-06: SunOS 5.10: Microtasking libraries (`libmtsk`) patch
    - 139574-03: SunOS 5.10
    - 141444-09
    - 141414-02
  - To determine that an operating system patch is installed, enter the following command:

    ```
    # /usr/sbin/patchadd -p | grep patch_number(without version number)
    ```

  - Required available swap space is shown below:

    Required available swap space

RAM	Available Swap Space
4 GB and 16 GB	Equal to the size of the RAM
More than 16 GB	16 GB

    You can use the following command to check the swap space:

    ```
    /usr/sbin/swap -l
    ```

  - Free `tmp` space should be 1GB /tmp directory space.

    You can use the following command to check `tmp` space:

    ```
    df -k /tmp | grep / | awk '{ print $3 }'
    ```

- Required operating system version is: 5.10

  You can use the following command to check the operating system version:

  ```
  uname -r
  ```

- To determine the update level of Oracle Solaris installed:

  ```
  $ cat /etc/release
  ```

- **Model repository (Database) disk space requirements**

  Additional disk space is required for the Oracle software and the Model Repository data files. Keep in mind that storage requirements for the database grow as the number of managed servers and database activity grows.

  As a benchmark figure, you should allow an additional 3.5 GB of database storage for every 1,000 servers in the facility that SA manages. When sizing the tablespaces, follow the general guidelines described in the table below. If you need to determine a more precise tablespace sizing, contact your technical support representative.

  Tablespace sizes

Tablespace	MB/1000	Recommended minimum tablespace size
AAA_DATA	256 MB	2000 MB
AAA_INDX	256 MB	2000 MB
AUDIT_DATA	256 MB	2000 MB
AUDIT_INDX	256 MB	2000 MB
LCREP_DATA	3000 MB	8000 MB
LCREP_INDX	2000 MB	8000 MB
TRUTH_DATA	1500 MB	4000 MB
TRUTH_INDX	500 MB	4000 MB
STRG_DATA	1300 MB	2000 MB
STRG_INDX	400 MB	2000 MB

Software requirements

This section lists the requirements for running Oracle 11g and 12c under Red Hat Enterprise Linux, Oracle Enterprise Linux and SUSE Linux Enterprise Server.

- **Linux requirements**

  The following are software requirements for running Oracle 11g and 12c under Red Hat Enterprise Linux, Oracle Enterprise Linux and SUSE Linux Enterprise Server:

  - Required operating system version for 11g:
    - Oracle Linux 5 Update 2 (with Red Hat Compatible Kernel)
    - Red Hat Enterprise Linux 5 Update 2
    - Red Hat Enterprise Linux 6
    - SUSE Linux Enterprise Server 10 SP2 (for customer supplied oracle database only)
    - SUSE Linux Enterprise Server 11 (for customer supplied oracle database only)
  - Required operating system version for 12c:
    - Oracle Linux 5 Update 6 (with Red Hat Compatible Kernel)
    - Oracle Linux 6 (with Red Hat Compatible Kernel)
    - Red Hat Enterprise Linux 5 Update 6
    - Red Hat Enterprise Linux 6
    - Red Hat Enterprise Linux 7 (supported only starting with Oracle 12.1.0.2)
    - SUSE Linux Enterprise Server 11 SP2

    You can use the following command to determine the distribution and version of Linux installed:

    ```
    # cat /proc/version
    ```

  - Required Kernel version for Oracle Database 11g Release 2 (11.2):
    - Oracle Linux 5 Update 2

      2.6.18 or later (with Red Hat Compatible Kernel)
    - Oracle Linux 6

      2.6.32-71.el6.x86_64 or later (with Red Hat Compatible Kernel)
    - Red Hat Enterprise Linux 6

      2.6.32-71.el6.x86_64 or later
    - Red Hat Enterprise Linux 5 Update 2

      2.6.18 or later
    - SUSE Linux Enterprise Server 10 (for customer supplied oracle database only)

      2.6.16.21 or later

    - SUSE Linux Enterprise Server 11 (for customer supplied oracle database only)

      2.6.27.19 or later

  - Required Kernel version for Oracle Database 12c Release 1 (12.1):

    - Oracle Linux 5 Update 6

      2.6.18-238.0.0.0.1.el5 or later

    - Oracle Linux 6 (with Red Hat Compatible Kernel)

      2.6.32-71.el6.x86_64 or later

    - Red Hat Enterprise Linux 5 Update 6

      2.6.18-238.0.0.0.1.el5 or later

    - Red Hat Enterprise Linux 6

      2.6.32-71.el6.x86_64 or later

    - Red Hat Enterprise Linux 7

      3.10.0-54.0.1.el7.x86_64 or later

    - SUSE Linux Enterprise Server 11 SP2 (for customer supplied oracle database only)

      3.0.13-0.27 or later

    You can use the following command to check the kernel versions:

    ```
    uname -r
    ```

    You can use the following command to check the platform:

    ```
    uname -mi
    ```

    You can use the following command to check the processor type:

    ```
    grep "model name" /proc/cpuinfo
    ```

- **Linux package requirements**
  - **Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g**

    The following or later package versions for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 (with Red Hat compatible kernel) must be installed (shaded rows indicate 32-bit packages):

    > Note: Starting with Oracle Database 11g Release 2 (11.2.0.2), all the 32-bit packages, excepting `gcc-32bit-4.3`, listed in the following table are no longer required for installing a database on Linux x86-64. Only the 64-bit packages are required. However, for any Oracle

Database 11g release before 11.2.0.2, both the 32-bit and 64-bit packages listed in the following table are required.

Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g

Required Packages	Version
bc	NA
binutils	2.17.50.0.6
compat-libstdc++	33-3.2.3
compat-libstdc++	33-3.2.3 (32-bit)
elfutils-libelf	0.125
elfutils-libelf-devel	0.125
gcc	4.1.2
gcc-c++	4.1.2
glibc	2.5-24
glibc	2.5-24 (32-bit)
glibc-common	2.5
glibc-devel	2.5
glibc-devel	2.5 (32-bit)
glibc-headers	2.5
ksh	NA
libaio	0.3.106
libaio	0.3.106 (32-bit)
libaio-devel	0.3.106
libaio-devel	0.3.106 (32-bit)
libgcc	4.1.2
libgcc	4.1.2 (32-bit)
libstdc++	4.1.2
libstdc++	4.1.2 (32-bit)

Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 11g, continued

Required Packages	Version
libstdc++-devel	4.1.2
make	3.81
sysstat	7.0.2

- **Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 12c**

  The following or later package versions for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 (with Red Hat compatible kernel) must be installed (shaded rows indicate 32-bit packages):

Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 12c

Required Packages	Version
bc	NA
binutils	2.17.50.0.6
compat-libstdc++	33-3.2.3
compat-libstdc++	33-3.2.3 (32-bit)
gcc	4.1.2
gcc-c++	4.1.2
glibc	2.5-58
glibc	2.5-58 (32-bit)
glibc-common	2.5
glibc-devel	2.5-58
glibc-devel	2.5-58 (32-bit)
ksh	NA
libaio	0.3.106
libaio	0.3.106 (32-bit)
libaio-devel	0.3.106
libaio-devel	0.3.106 (32-bit)

Required Packages for Red Hat Enterprise Linux 5 and Oracle Enterprise Linux 5 for Oracle 12c, continued

Required Packages	Version
libgcc	4.1.2
libgcc	4.1.2 (32-bit)
libstdc++	4.1.2
libstdc++	4.1.2 (32-bit)
libstdc++-devel	4.1.2
libXext	1.0.1
libXext	1.0.1 (32-bit)
libXtst	1.0.1
libXtst	1.0.1 (32-bit)
libX11	1.0.3
libX11	1.0.3 (32-bit)
libXau	1.0.1
libXau	1.0.1 (32-bit)
libXi	1.0.1
libXi	1.0.1 (32-bit)
make	3.81
sysstat	7.0.2

- **Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 11g**

  The following or later package versions for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 (with Red Hat compatible kernel) must be installed:

Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 11g

Required Packages	Version
bc	NA
binutils	2.20.51.0.2-5.11.el6 (x86_64)

Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 11g, continued

Required Packages	Version
compat-libcap1	1-1.10-1 (x86_64)
compat-libstdc++	33-3.2.3-69.el6 (x86_64)
compat-libstdc++	33-3.2.3-69.el6.i686
gcc	4.4.4-13.el6 (x86_64)
gcc-c++	4.4.4-13.el6 (x86_64)
glibc	2.12-1.7.el6 (x86_64)
glibc	2.12-1.7.el6 (i686)
glibc-devel	2.12-1.7.el6 (x86_64)
glibc-devel	2.12-1.7.el6.i686
ksh	NA
libaio	0.3.107-10.el6 (x86_64)
libaio	0.3.107-10.el6.i686
libaio-devel	0.3.107-10.el6 (x86_64)
libaio-devel	0.3.107-10.el6.i686
libgcc	4.4.4-13.el6 (x86_64)
libgcc	4.4.4-13.el6 (i686)
libstdc++	4.4.4-13.el6 (x86_64)
libstdc++	4.4.4-13.el6.i686
libstdc++-devel	4.4.4-13.el6 (x86_64)
libstdc++-devel	4.4.4-13.el6.i686
make	3.81-19.el6
sysstat	9.0.4-11.el6 (x86_64)

- **Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 12c**

  The following or later package versions for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 (with Red Hat compatible kernel) must be installed:

Required Packages for Red Hat Enterprise Linux 6 and Oracle Enterprise Linux 6 for Oracle 12c

Required Packages	Version
bc	NA
binutils	2.20.51.0.2-5.11.el6 (x86_64)
compat-libcap1	1.10-1 (x86_64)
compat-libstdc++	33-3.2.3-69.el6 (x86_64)
compat-libstdc++	33-3.2.3-69.el6 (i686)
gcc	4.4.4-13.el6 (x86_64)
gcc-c++	4.4.4-13.el6 (x86_64)
glibc	2.12-1.7.el6 (x86_64)
glibc	2.12-1.7.el6 (i686)
glibc-devel	2.12-1.7.el6 (x86_64)
glibc-devel	2.12-1.7.el6 (i686)
ksh	NA
libaio	0.3.107-10.el6 (x86_64)
libaio	0.3.107-10.el6 (i686)
libaio-devel	0.3.107-10.el6 (x86_64)
libaio-devel	0.3.107-10.el6 (i686)
libgcc	4.4.4-13.el6 (x86_64)
libgcc	4.4.4-13.el6 (i686)
libstdc++	4.4.4-13.el6 (x86_64)
libstdc++	4.4.4-13.el6 (i686)
libstdc++-devel	4.4.4-13.el6 (x86_64)
libstdc++-devel	4.4.4-13.el6 (i686)
make	3.81-19.el6
sysstat	9.0.4-11.el6 (x86_64)

- **Red Hat Enterprise Linux 7 for Oracle 12c**

  The following package versions or later for Red Hat Enterprise Linux 7 must be installed:

Required Packages for Red Hat Enterprise Linux 7 for Oracle 12c

Required Packages	Version
binutils	2.23.52.0.1-12.el7.x86_64
compat-libcap1	1.10-3.el7.x86_64
compat-libstdc++	33-3.2.3-71.el7.x86_64 (*this requirement can be ignored - Oracle bug 21151912)
gcc	4.8.2-3.el7.x86_64
gcc-c++	4.8.2-3.el7.x86_64
glibc	2.17-36.el7.x86_64
glibc	2.17-36.el7.i686
glibc-devel	2.17-36.el7.x86_64
glibc-devel	2.17-36.el7.i686
ksh	NA
libaio	0.3.109-9.el7.x86_64
libaio	0.3.109-9.el7.i686
libaio-devel	0.3.109-9.el7.x86_64
libaio-devel	0.3.109-9.el7.i686
libgcc	4.8.2-3.el7.x86_64
libgcc	4.8.2-3.el7.i686
libstdc++	4.8.2-3.el7.x86_64
libstdc++	4.8.2-3.el7.i686
libstdc++-devel	4.8.2-3.el7.x86_64
libstdc++-devel	4.8.2-3.el7.i686
libXi	1.7.2-1.el7.x86_64
libXi	1.7.2-1.el7.i686
libXtst	1.2.2-1.el7.x86_64
libXtst	1.2.2-1.el7.i686
make	3.82-19.el7.x86_64
sysstat	10.1.5-1.el7.x86_64

- ○ **SUSE Linux Enterprise Server 10 for Oracle 11g**

  The following or later package versions for SUSE Linux Enterprise Server 10 must be installed:

  Required Packages for SUSE Linux Enterprise Server 10 for Oracle 11g

Required Packages	Version
bc	NA
binutils	2.16.91.0.5
compat-libstdc++	5.0.7
gcc	4.1.0
gcc-c++	4.1.2
glibc	4.1.2
glibc-devel	2.4-31.63
glibc-devel	2.4-31.63 (32-bit)
ksh	93r-12.9
libaio	0.3.104
libaio	0.3.104 (32-bit)
libaio-devel	0.3.104
libaio-devel	0.3.104 (32-bit)
libelf	0.8.5
libgcc	4.1.2
libstdc++	4.1.2
libstdc++-devel	4.1.2
make	3.80
numactl	0.9.6.x86_64
sysstat	8.0.4

- **SUSE Linux Enterprise Server 11 for Oracle 11g** (for customer supplied oracle database only)

  The following or later package versions for SUSE Linux Enterprise Server 11 must be installed:

  Required Packages for SUSE Linux Enterprise Server 11for Oracle 11g

Required Packages	Version
bc	NA
binutils	2.19
gcc	4.3
gcc	4.3 (32-bit)
gcc-c++	4.3
glibc	2.9
glibc	2.9 (32-bit)
glibc-devel	2.9
glibc-devel	2.9 (32-bit)
ksh	93t
libaio	0.3.104
libaio	0.3.104 (32-bit)
libaio-devel	0.3.104
libaio-devel	0.3.104 (32-bit)
libgcc43	4.3.3_20081022
libstdc++-devel	4.3
libstdc++33	3.3.3
libstdc++33	3.3.3 (32-bit)
libstdc++43	4.3.3_20081022
libstdc++43	4.3.3_20081022 (32-bit)
libstdc++43-devel	4.3.3_20081022

Required Packages for SUSE Linux Enterprise Server 11for Oracle 11g, continued

Required Packages	Version
libstdc++43-devel	4.3.3_20081022 (32-bit)
make	3.81
sysstat	8.1.5

- **SUSE Linux Enterprise Server 11 for Oracle 12c (for customer supplied oracle database only)**

  The following or later package versions for SUSE Linux Enterprise Server 11 must be installed:

Required Packages for SUSE Linux Enterprise Server 11 for Oracle 12c

Required Packages	Version
bc	NA
binutils	2.21.1-0.7.25
gcc	4.3-62.198
gcc-c++	4.3-62.198
glibc	2.11.3-17.31.1
glibc-devel	2.11.3-17.31.1
ksh	93u-0.6.1
libaio	0.3.109-0.1.46
libaio-devel	0.3.109-0.1.46
libcap1	1.10-6.10
libgcc46	4.6.1_20110701-0.13.9
libstdc++33	3.3.3-11.9
libstdc++33	3.3.3-11.9 (32-bit)
libstdc++43-devel	4.3.4_20091019-0.22.17
libstdc++46	4.6.1_20110701-0.13.9
make	3.81

Required Packages for SUSE Linux Enterprise Server 11 for Oracle 12c, continued

Required Packages	Version
sysstat	8.1.5-7.32.1
xorg-x11-libs	7.4 (x86_64)
xorg-x11-libs	7.4 (32-bit)
xorg-x11-libX11	7.4 (x86_64)
xorg-x11-libX11	7.4 (32-bit)
xorg-x11-libXau	7.4 (x86_64)
xorg-x11-libXau	7.4 (32-bit)
xorg-x11-libxcb	7.4 (x86_64)
xorg-x11-libxcb	7.4 (32-bit)
xorg-x11-libXext	7.4 (x86_64)
xorg-x11-libXext	7.4 (32-bit)

Verifying if packages are installed

To verify if RPMs are installed under Linux, enter the following command:

```
rpm -q --qf '%{NAME}-%{VERSION}-%{RELEASE} (%{ARCH})\n' <rpm_name>
```

- **Oracle Sun Solaris equirements**

  This topic lists the requirements for running Oracle 11g under Oracle Sun Solaris.

  - Required operating system version:
    - Oracle Solaris 10 U6 (5.10-2008.10)
    - Oracle Solaris 11 11/11 SPARC (for Oracle 11.2.0.3 only)

- You can use the following command to determine the distribution and version of Solaris installed:

  ```
  # uname -r
  ```

  - You can use the following to determine the update level of Oracle Solaris installed:

    ```
    $ cat /etc/release
    ```

- **Solaris package requirements**

  The following packages (or later versions) are required for Oracle Database 11g Release 2 (11.2) on Oracle Solaris 10:

  - SUNWarc
  - SUNWbtool
  - SUNWhea
  - SUNWlibC
  - SUNWlibm
  - SUNWlibms
  - SUNWsprot
  - SUNWtoo
  - SUNWi1of
  - SUNWi1cs (ISO8859-1)
  - SUNWi15cs (ISO8859-15)
  - SUNWxwfnt
  - SUNWcsl

  To verify whether these packages are installed on the OS, enter the following command:

  ```
  # pkginfo -i SUNWarc SUNWbtool SUNWhea SUNWlibC SUNWlibms SUNWsprot \
    SUNWtoo SUNWi1of SUNWi1cs SUNWi15cs SUNWxwfnt
  ```

- **HP-UX and IBM AIX version and package requirements**

  For HP-UX and IBM AIX operating system, compiler, patch and any additional software requirements, see the Checking the Software Requirements section in the Oracle® Database Quick Installation Guide for your operating system.

Non-SA-supplied Oracle software and database setup

> Note: If you plan to install the SA-supplied Oracle RDBMS software and database, you do not need to perform the tasks in this section. The SA Installer performs all the tasks discussed below. For information about installing the SA-supplied Oracle software and database, see "SA-supplied Oracle RDBMS software and database setup".

If you plan to use a non-SA-supplied Oracle database with the SA Model Repository, the following steps are required for compatibility with SA. You should also review "System requirements for Oracle database" before preceding with this section.

- "Modifiable kernel parameters" below
- "Installing the Oracle database " on page 121
- "SA Database installation sample scripts" on page 128

Modifiable kernel parameters

If you manually install the Oracle database, or use an existing database, you must insure that all kernel parameter values are specified correctly for your environment but also within the limitations required by SA.

You can find additional information about kernel parameter configuration in the Configuring Kernel Parameters section of the Oracle® Database Quick Installation Guide.

Modifiable kernel parameter values for Linux

This topic provides you information about the kernel parameters you can change for supported Linux operating systems.

- You can change values for the following parameters in /etc/sysctl.conf. If the current value of any parameter is higher than the value listed in this table, then do not change the value of that parameter:

  ```
  #SA Oracle parameters begin
  fs.aio-max-nr=1048576
  fs.file-max=6815744
  kernel.shmmax=2147483648
  ```

```
kernel.shmall=2097152
kernel.shmmni=4096
kernel.sem=250 32000 100 128
net.core.rmem_default=262144
net.core.rmem_max=4194304
net.core.wmem_default=262144
net.core.wmem_max=1048586
net.ipv4.ip_local_port_range=9081 65500
net.ipv4.tcp_wmem=262144 262144 262144
net.ipv4.tcp_rmem=4194304 4194304 4194304
#SA Oracle parameters end
```

- You can change values for the following parameters in /etc/security/limits.conf:

```
#SA Oracle parameters begin
oracle soft nofile 1024
oracle hard nofile 65536
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft stack 10240
oracle hard stack 32768
#SA Oracle parameters end
```

- You can change values for the following parameters in /etc/pam.d/login:

```
session required /lib/security/pam_limits.so
```

- You can change values for the following parameters in `/etc/fstab`:

```
shmfs /dev/shm tmpfs size=4g 0 0
```

> **Note:** For RHEL 7 systems, the mount should be `tmpfs /dev/shm tmpfs size=4g 0 0`.

- You can change values for the following parameters in /etc/selinux/config:

```
#SA Oracle parameters begin
SELINUX=disabled
#SA Oracle parameters end
```

Modifiable kernel parameter values for SUSE Linux x86_64

This topic identifies additional required settings for SUSE Linux x86_64 when running Oracle 11g or 12c:

- Enter the following command to cause the system to read the /etc/sysctl.conf file when it restarts:

  ```
  # /sbin/chkconfig boot.sysctl on
  ```

- You must enter the GID of the `oinstall` group as the value for the `/proc/sys/vm/hugetlb_shm_group` parameter. Doing this grants members of `oinstall` a group permission to create shared memory segments. For example, where the `oinstall` group GID is 501:

  ```
  # echo 501 > /proc/sys/vm/hugetlb_shm_group
  ```

  After running this command, use vi to add the following text to /etc/sysctl.conf, and enable the boot.sysctl script to run on system restart:

  ```
  vm.hugetlb_shm_group=501
  ```

> Note: Only one group can be defined as the `vm.hugetlb_shm_group`.

Modifiable kernel parameter values for Oracle SPARC Solaris (64 bit), HP-UX, and IBM AIX

Refer the Configuring Kernel Parameters section in the following Oracle documents:

- *Database Quick Installation Guide for Oracle Solaris on SPARC (64 Bit)*
- *Database Quick Installation Guide for HP-UX Itanium*
- *Database Quick Installation Guide for IBM AIX on POWER Systems (64-Bit)*

Installing the Oracle database

To install an Oracle database for use with the SA Model Repository:

1. Create the database with the UTF8 database character set .
2. Set the database with `TIME_ZONE` to `'+00:00'`.
3. Create the database with the required initialization (`init.ora`) parameters.
4. Create the database with required tablespaces.
5. Create the database user `opsware_admin`.
6. `tnsnames.ora` file requirements
7. File linking requirements
8. Enable Oracle Daylight Savings Time (DST)
9. sqlnet.ora requirements

1. Create UTF8 Database character set

Create the database with the UTF8 database character set:

```
CHARACTER SET UTF8
```

2. Set the Database TIME_ZONE

Create the database with `TIME_ZONE` set to `'+00:00'`:

```
SET TIME_ZONE = '+00:00'
```

3. Specify the required initialization (init.ora) parameters

Create the database instance with the following initialization (`init.ora`) parameters. For parameters not listed, SA assumes that the default Oracle parameters are used.

Oracle 11.2.0.x

```
compatible := required to be >= 11.2.0
cursor_sharing := required to be = FORCE
db_file_multiblock_read_count := suggested to be >= 16
db_block_size := required to be >= 8192
deferred_segment_creation := required to be = FALSE
event := required to be = 12099 trace name context forever, level 1
job_queue_processes := required to be >= 1000
log_buffer := required to be >= 5242880
memory_target := required to be >= 1879048192 (1.75GB)
nls_length_semantics := required to be = CHAR
nls_sort := required to be = GENERIC_M
open_cursors := required to be >= 1500
optimizer_index_cost_adj := required to be = 100
optimizer_index_caching := required to be = 0
optimizer_mode := 'required to be = ALL_ROWS
processes := required to be >= 1024
recyclebin := required to be = OFF
remote_login_passwordfile := required to be = EXCLUSIVE
session_cached_cursors := required to be >= 50
undo_tablespace := should be = UNDO or other UNDO tablespace
undo_management := should be = AUTO
_complex_view_merging := required to be = FALSE
```

Oracle 12.1.0.x

```
compatible := required to be >= 12.1.0
cursor_sharing := required to be = FORCE
db_block_size := required to be >= 8192
```

```
db_file_multiblock_read_count := suggested to be >= 16
deferred_segment_creation := required to be = FALSE
job_queue_processes := required to be >= 1000
max_string_size := required to be = STANDARD
memory_target := required to be >= 2684354560 (2.5GB)
nls_length_semantics := required to be = CHAR
nls_sort := required to be = GENERIC_M
open_cursors := required to be >= 1500
optimizer_index_cost_adj := required to be = 100
optimizer_index_caching := required to be = 0
optimizer_mode := 'required to be = ALL_ROWS
processes := required to be >= 1024
recyclebin := required to be = OFF
remote_login_passwordfile := required to be = EXCLUSIVE
session_cached_cursors := required to be >= 50
undo_tablespace := should be = UNDO or other UNDO tablespace
```

> **Note**: The parameters `_complex_view_merging` and `event` are no longer required for Oracle 12c.

4. Create the required tablespaces

The following tablespaces must be created to support SA. For tablespace disk space requirements, see "Model repository (Database) disk space requirements".

- LCREP_DATA
- LCREP_INDX
- TRUTH_DATA
- TRUTH_INDX
- AAA_DATA
- AAA_INDX
- AUDIT_DATA
- AUDIT_INDX
- STRG_DATA
- STRG_INDX

5. Create the Database user opsware_admin

Create the database user 'opsware_admin' with the following privileges.

```
SQL> create user opsware_admin identified by opsware_admin
default tablespace truth_data temporary tablespace temp
```

```
quota unlimited on truth_data;
SQL> grant alter session to opsware_admin with admin option;
SQL> grant create procedure to opsware_admin with admin option;
SQL> grant create public synonym to opsware_admin with admin option;
SQL> grant create sequence to opsware_admin with admin option;
SQL> grant create session to opsware_admin with admin option;
SQL> grant create table to opsware_admin with admin option;
SQL> grant create trigger to opsware_admin with admin option;
SQL> grant create type to opsware_admin with admin option;
SQL> grant create view to opsware_admin with admin option;
SQL> grant delete any table to opsware_admin with admin option;
SQL> grant drop public synonym to opsware_admin with admin option;
SQL> grant select any table to opsware_admin with admin option;
SQL> grant select_catalog_role to opsware_admin with admin option;
SQL> grant query rewrite to opsware_admin with admin option;
SQL> grant restricted session to opsware_admin with admin option;
SQL> grant execute on dbms_utility to opsware_admin with grant option;
SQL> grant analyze any to opsware_admin;
SQL> grant insert, update, delete, select on sys.aux_stats$ to opsware_admin;
SQL> grant gather_system_statistics to opsware_admin;
SQL> grant create job to opsware_admin with admin option;
SQL> grant create any directory to opsware_admin;
SQL> grant drop any directory to opsware_admin;
SQL> grant alter system to opsware_admin;
SQL> grant create role to opsware_admin;
SQL> grant create user to opsware_admin;
SQL> grant alter user to opsware_admin;
SQL> grant drop user to opsware_admin;
SQL> grant create profile to opsware_admin;
SQL> grant alter profile to opsware_admin;
SQL> grant drop profile to opsware_admin;
```

If Oracle version is 12.2.0.x or 18.6.0.0.0, create the database user 'truth' with the following privileges:

```
SQL> create user truth identified by opsware_admin default tablespace
truth_data temporary tablespace temp;
SQL> grant select on ALL_TAB_COLUMNS to truth with grant option;
SQL> grant select on ALL_INDEXES to truth with grant option;
SQL> grant select on ALL_IND_COLUMNS to truth with grant option;
SQL> grant select on ALL_CONSTRAINTS to truth with grant option;
SQL> grant select on ALL_CONS_COLUMNS to truth with grant option;
SQL> grant select on ALL_TRIGGERS to truth with grant option;
```

In the above example, the password, "opsware_admin' for the user, 'truth' should have the same value as the truth.password from the SA installation interview.

If you have any security concerns after the SA install, revoke the following privileges granted to the database user 'truth':

```
SQL> revoke select on ALL_TAB_COLUMNS from truth;
SQL> revoke select on ALL_INDEXES from truth;
SQL> revoke select on ALL_IND_COLUMNS from truth;
SQL> revoke select on ALL_CONSTRAINTS from truth;
SQL> revoke select on ALL_CONS_COLUMNS from truth;
SQL> revoke select on ALL_TRIGGERS from truth;
```

6. tnsnames.ora file requirements

The tnsnames.ora file enables resolution of database names used internally by the core components. SA has the following requirements for the tnsnames.ora file:

- The file must reside in the /var/opt/oracle/tnsnames.ora and $ORACLE_HOME/network/admin locations
- If the core is installed across multiple servers, a copy of the file must reside on the servers hosting the following components:
  - Model Repository
  - Infrastructure Component bundle (required by the Data Access Engine, Model Repository Multimaster Component, Software Repository Store)
  - Slice Component bundle (required by the Command Center, Web Services Data Access Engine, Global File System)
- For a core installed on multiple servers, the directory path of the tnsnames.ora file must be the same on each server.
- In a Single Core installation, the tnsnames.ora file must contain an entry for the Model Repository, as in the following example:

  ```
  truth = DESCRIPTION= (ADDRESS=(HOST=magenta.example.com)(PORT=1521)

  (PROTOCOL=tcp)) (CONNECT_DATA=(SERVICE_NAME=truth)))
  ```

tnsnames.ora: Multimaster Mesh requirements

In a Multimaster Mesh, the tnsnames.ora file must be set up for a Source Core and a Destination Core using the following guidelines.

- **Source core**

  The tnsnames.ora file must contain an entry for its own Model Repository. The port number must be set to the port that you have designated that the Oracle listener process use, such as `1521 (default)`, `1526`, and so on.

  The tnsnames.ora file must also contain an entry that specifies the Source Core Management Gateway. This port is used by the Data Access Engine for Multimaster traffic. The port number is derived from the following formula: (20000) + (facility ID of the Destination Core).

  Example: In the following example, the TNS service name of the Source Core is `orange_truth`, which runs on the host `orange.example.com`. The TNS name of the Destination Core is `cyan_truth`, which has a facility ID of `556`. Note that the entry for `cyan_truth` specifies `orange.example.com`, which is the host running the Source Core's Management Gateway.

  ```
  orange_truth=(DESCRIPTION=(ADDRESS=(HOST=orange.example.com)(PORT=1521)
  (PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
  ```

  ```
  cyan_truth=(DESCRIPTION=(ADDRESS=(HOST=orange.example.com)(PORT=20556)
  (PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
  ```

- **Destination core**

  The tnsnames.ora file must contain an entry for its own Model Repository. The port number must be set to the port that you have designated that the Oracle listener process use, such as `1521 (default)`, `1526`, and so on. The tnsnames.ora file does not require any entries for other cores in the mesh.

  Example: In the following example, the TNS service name of the Destination Core is `cyan_truth`, and the core runs on the host, `cyan.example.com`.

  ```
  cyan_truth=(DESCRIPTION=(ADDRESS=(HOST=cyan.example.com)(PORT=1521)
  (PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
  ```

7. File linking requirements

After creating the database, but before installing the Model Repository with the SA Installer, perform the following tasks:

1. Create the tnsnames.ora file in the /var/opt/oracle directory.
2. Verify that the file conforms to the rules listed in "6. tnsnames.ora file requirements".
   If it does not exist, create mkdir -p /var/opt/oracle directory:
3. Create the following symbolic link:
   `ln -s /var/opt/oracle/tnsnames.ora $ORACLE_HOME/network/admin/tnsnames.ora`

4. Ensure that the oracle Unix user has read-write permission on the tnsnames.ora file.
5. If Oracle version is 12.2.0.x or 18.6.0.0.0, as oracle user, create the following symbolic link:
6. **su - oracle**

   ```
   cd $ORACLE_HOME/jdbc/lib/
   ln -s ojdbc8.jar ojdbc7.jar
   ```

For Red Hat Enterprise Linux:

1. Create another symbolic link:

   ```
   ln -s /etc/oratab /var/opt/oracle/oratab
   ```

2. Copy the sample `opsware-oracle` script to **/etc/init.d/**.
3. Link **/etc/init.d/opsware-oracle** to corresponding scripts in the **/etc/rc*** directories. For example:

   ```
   ln -s /etc/init.d/opsware-oracle \
         /etc/rc0.d/K02opsware-oracle
   ln -s /etc/init.d/opsware-oracle \
         /etc/rc1.d/K02opsware-oracle
   ln -s /etc/init.d/opsware-oracle \
         /etc/rc2.d/S60opsware-oracle
   ln -s /etc/init.d/opsware-oracle \
         /etc/rcS.d/K02opsware-oracle
   ```

8. Enable Oracle Daylight Savings Time (DST)

To enable Daylight Saving Time for the Oracle database, you must apply database tier patches. To apply these patches, perform the following steps:

1. Verify that your database is running on Oracle 11g, 12c or higher.
2. Use MetaLink Note 412160.1 to apply Oracle Database time zone fixes specific to your database version.
   Use MetaLink Note 412160.1 to apply time zone fixes to the Oracle Java Virtual Machine (JVM) in the Oracle Database specific to your E-Business Suite database version.

9. sqlnet.ora requirements

Some applications in Server Automation use the oracle classes12.jar file to connect to the database. To enable these utilities to connect to the Oracle 12C database, create a **sqlnet.ora** in the **$ORACLE_ HOME/network/admin** folder in *both* the SA Client system and the SA Core Database server with the following contents:

```
# File:        sqlnet.ora
# Certified:   Oracle 12.1.0
# Purpose:     Configuration File for all Net8 Clients
# Notes:       None

LOG_DIRECTORY_SERVER=/u01/app/oracle/product/12.1.0/db_1/network/log
LOG_FILE_SERVER=sqlnet.log
TRACE_DIRECTORY_SERVER=/u01/app/oracle/product/12.1.0/db_1/network/trace
TRACE_FILE_SERVER=sqlnet.trc
NAMES.DIRECTORY_PATH= (TNSNAMES)
SQLNET.INBOUND_CONNECT_TIMEOUT=180
```

SA Database installation sample scripts

HPE Support can provide sample scripts for steps 1 through 5 of the Oracle Database Installation Steps.

Oracle/SA Installation Scripts, SQL Scripts, and configuration files

- **truth.sh**: A shell script that creates directories and then launches the **truth.sql** script. Running this script causes all the scripts to be run automatically, in the correct order.
- **truth.sql**: Prompts for passwords of the SYS and SYSTEM users and launches the remainder of the SQL scripts in this list.
- **CreateDB.sql**: Creates a database with the UTF8 character set and TIME_ZONE set to '+00:00'
- **CreateDBFiles.sql**: Creates the following tablespaces that are required by SA:
  - LCREP_DATA
  - LCREP_INDX
  - TRUTH_DATA
  - TRUTH_INDX
  - AAA_DATA
  - AAA_INDX
  - AUDIT_DATA
  - AUDIT_INDX
  - STRG_DATA
  - STRG_INDX

See "Model Repository (Database) disk space requirements" for additional tablespace sizing information.

- **CreateDBCatalog.sql**: Runs Oracle scripts to create data system catalog objects.
- **JServer.sql**: Sets up the Oracle Java environment.
- **CreateAdditionalDBFiles.sql**: Adds data and index files to certain tablespaces and allocates additional disk space. This script is optional, but recommended.
- **CreateUserOpsware_Admin.sql**: Creates the `opsware_admin` database user and grants permissions (privileges) to this user (required by SA).
- **postDBCreation.sq**: Creates the spfile file from the pfile file (parameter file).
- **init.ora**: Contains initialization parameters for the database. See "3. Specify the required initialization (init.ora) parameters".
- **tnsnames.ora**: Enables resolution of database names used internally by SA.
- **listener.ora**: Contains configuration parameters for the listener. SA by default listens on port 1521. You can change the default port during installation or by editing the tsnames.ora file.

> Note: The SA-supplied Oracle 12.1.0.1 database has a new **listener.ora** parameter:
>
> ```
> SUBSCRIBE_FOR_NODE_DOWN_EVENT_LISTENER=
> ```
>
> Default is OFF. This parameter must be set to OFF for non-RAC installations. For more information about this parameter, see the Oracle documents IDs 372959.1 and 437598.1.

bash_profile or **profile**: Sets environment variables and sets shell limits for the `oracle` Unix user.

opsware-oracle: A script residing in /etc/init.d that starts up and shuts down the database and listener.

> Note: The **/etc/init.d/opsware-sas** start script, which starts and stops the SA components, does not start and stop the database and listener. For more information on the **opsware-sas** start script, see “Start Script for SA” in the SA 10.60 Administration Guide.

Creating the database using the SA-supplied scripts

To create the Oracle database using the SA-supplied scripts:

1. Obtain the database creation scripts from your HPE Support representative.
2. Make any required changes to the scripts.
3. As `root`, create the Unix user `oracle` and log in to the server as the user `oracle`.

4. Copy the SA-supplied files to the **$ORACLE_BASE/admin/truth/create** directory.
5. Change the mode of the SA-supplied `truth.sh` script:
   ```
   chmod 755 truth.sh
   ```
6. Launch the SQL scripts that create the database by running the `truth.sh` script:
   ```
   ./truth.sh
   ```
7. After the scripts launched by `truth.sh` complete, check the log files in the **/u01/app/oracle/admin/truth/scripts/*.log** directory for errors.

SA-supplied Oracle RDBMS software and database setup

> Note: If you plan to install the Oracle RDBMS software and database yourself, you do not need to perform the tasks in this section. See "Non-SA-supplied Oracle software and database setup".

If you plan to use a SA-supplied Oracle database with the SA Model Repository, you should read the following sections for information about what the SA Installer does when installing the Oracle software and database during SA installation. The SA Installer performs all the tasks discussed below. You should also review "System requirements for Oracle database" before proceeding with this section.

SA-supplied RDBMS configuration details

When you install the SA-supplied Oracle RDBMS using the SA Installer Oracle installation option, the installer:

- Checks that all requirements are met on the host server (see "System requirements for Oracle database").
- Sets certain kernel parameters to required values (see "Modifiable kernel parameters").
- Creates the Unix user `oracle` locally in /etc/passwd.
- Creates the Unix groups `dba` and `oinstall` locally in /etc/group.
- Sets the `$ORACLE_HOME` environment variable to the `/u01/app/oracle/product/12.1.0.2/db_2` directory:
- Sets the `$ORACLE_SID` environment variable to `truth`.

- Creates a database with the UTF8 character set, `TIME_ZONE` set to `'+00:00'` and with required `init.ora` parameters.
- Creates the tablespaces and data and index files under the following directories:
  - /u01/oradata/truth
  - /u02/oradata/truth
  - /u03/oradata/truth
  - /u04/oradata/truth

  The system administrator can configure the /u01, /u02, /u03, /u04 directories before installing the Oracle RDBMS software.
- Gets the service name (TNS name) from the SA Installer interview (`truth.servicename` prompt) and inserts it into the tnsnames.ora file in $ORACLE_HOME/network/admin and /var/opt/oracle. The SA Installer changes the value of the `host` parameter in **`tsnames.ora`** to the value returned by the Unix **`hostname`** command.
- In the /$ORACLE_HOME/network/admin/listener.ora file, changes the value of the `host` parameter to the value returned by the Unix **`hostname`** command.
  The listener is password protected and OS authenticated. (The default password is `opsware`.) By default, it listens on port 1521.
- Creates the **`/etc/init.d/opsware-oracle`** script, which you can use to start up and shut down the database and listener.
  This script is linked to corresponding scripts in the /etc/rc*.d directories.
- Creates the user `opsware_admin` with the required privileges.
- After installation is complete, you can examine the logs that are created at /var/log/opsware/install_opsware.

Security

SA recommends that you change the default passwords for the following:

- the Unix user `oracle`
- the Oracle database users SYS and SYSTEM
  SA does not use the SYS and SYSTEM users.
- the Oracle listener
  In the /$ORACLE_HOME/network/admin/listener.ora file, SA sets the value of the host parameter to the value returned by the Unix hostname command. The listener is password protected and OS authenticated. The default password is `opsware`. By default, the Oracle listener uses port 1521.

SA-supplied Oracle installation

SA supports the following SA/Oracle database configurations:

- SA Core and Oracle database on a single host
- SA Core with the Oracle database on a remote database server

See "Customer installable SA Core configurations" for a description of supported SA Core/Oracle database configurations and installation instructions."SA Core installation"

Installing the Model Repository database on a remote server

To install or upgrade the Model Repository Oracle database on a remote server:

1. Perform the following tasks on the server on which you will run the SA Installer:
   a. Install the Oracle Full Client software.
   The steps below use /u01/app/oracle/product/12.1.0/client_1 as the Oracle Full Client home.

   > Note: The Oracle Full Client must be the same version as the Oracle database.

   b. Ensure that the Oracle Full Client software is owned by the OS user `oracle`.

   c. Copy the database server's **/var/opt/oracle/tnsnames.ora** file to the client machine's **/var/opt/oracle/tnsnames.ora**. Ensure that the hostname in the file resolves properly.

   d. If it does not exist, create **mkdir -p /var/opt/oracle** directory:

   e. Create the following symbolic link:
   ```
   # ln -s /var/opt/oracle/tnsnames.ora $ORACLE_HOME/network/admin/tnsnames.ora
   ```

   f. Ensure that the Unix user `oracle` has read-write permission on the tnsnames.ora file.

   g. Ensure that the SA Installer Core Definition File (CDF) has the correct path to the client **tnsnames.ora** file (`%truth.tnsdir`), oracle client home (`%db.orahome`), database server name/IP (`%db.host`), listener port (`%db.port`), SA Installer machines subdomain (`%truth.dcSubDom`), and so on. Based on the above steps your parameter values will be:

- `%truth.tnsdir=/var/opt/oracle`
- `%db.orahome=/u01/app/oracle/product/12.1.0/client_1`
- `%db.port=1521`
- `%truth.dcSubDom=prod.example.com`
- `db.host=192.168.9.99` (server on which the Oracle database is installed)

h. Ensure that the `COMPATIBLE` parameter is set correctly and that it matches the database version. For example, for database software that is version 12.1.0.1 ensure that `COMPATIBLE=12.1.0.1`. SA uses Oracle's Export Data Pump and Import Data Pump utilities during secondary core creation. These utilities require the `COMPATIBLE` parameter be specified correctly.

2. Perform the following tasks on the Model Repository host:

   a. Log in as the user `oracle`.

   b. Ensure that the listener is started with the command:
   `lsnrctl start <your_listener_name>`

Oracle RAC support

SA supports Oracle Real Application Clusters (RAC). Oracle RAC support requires a new installation of both Oracle and SA. Therefore, in order to enable Oracle RAC support in SA, you must first install Oracle RAC 11g, configured as described in the following sections:

- "Supported Oracle versions and operating systems" below
- "System requirements" on the next page
- "Setting up the Oracle RAC database/instances" on the next page

Supported Oracle versions and operating systems

Support for the Model Repository is limited to certain versions of Oracle running on certain versions of operating systems. HPE strongly recommends that you also apply the latest Oracle CPU or PSU patches.

See the SA 10.60 Support and Compatibility Matrix for a list of supported Oracle versions and operating systems.

System requirements

For information on system requirements for Oracle database, see "System requirements for Oracle database".

Setting up the Oracle RAC database/instances

SA supports any valid Oracle RAC configuration, such as any number of nodes, ASM or regular disks, and so on.

However, the Oracle database must be configured for using with SA. You require your Oracle database administrator's (DBA) help to configure the Oracle RAC/instances, the required initialization parameters, the required tablespaces, the `opsware_admin` database user, and the listener.ora and tnsnames.ora files.

Creating the database with the required initialization parameters

Perform the following tasks listed in the "Non-SA-supplied Oracle software and database setup" section:

- Modifiable Kernel Parameters
- Oracle database installation
    a. Create the database with the UTF8 database character set
    b. Set the database with `TIME_ZONE` to `'+00:00'`
    c. Create the database with the required initialization (`init.ora`) parameter
    d. Create the database with required tablespaces
    e. Create the database user `opsware_admin`

> **Note:** Use the tnsnames.ora file and file linking requirements listed in the following sections since they differ for the Oracle RAC environment from those listed in "Non-SA-supplied Oracle software and database setup".

"Non-SA-supplied Oracle software and database setup" describes the required database setup, Oracle initialization parameters, required tablespaces, database user `opsware_admin`, etc.

> **Note:** On an SA Oracle RAC DB installation, the admin should not modify the Management

> Gateway Properties File(s) while in operational mode. While the SA system is in operational mode, the remote Oracle DB connections are direct and do not use the RAC scan address.

Installing the Model Repository

In most production environments with Oracle RAC, you can perform the Model Repository installation from any SA server. The database server or RAC nodes in this case are considered to be remote.

The examples used in the following sections assume an SA server (rac1sa.dev.opsware.com) on which SA will be installed and a 2 node RAC configuration shown in below:

Sample RAC configurations

Identity	Host note	Name	Type	Address	Address Static or Dynamic	Resolved by
Node 1 Public	`rac1pub`	`rac1pub`	Public	192.168.173.210	Static	DNS
Node 1 Virtual	Selected by Oracle Clusterware	`rac1-vip`	Virtual	192.168.173.212	Static	DNS and/or host file
Node 1 Private	`rac1pub`	`rac1prv`	Private	`172.16.1.100`	Static	DNS, host file or none
Node 2 Public	`rac2pub`	`rac2pub`	Public	192-168-173-211	Static	DNS
Node 2 Virtual	Selected by Oracle Clusterware	`rac2-vip`	Virtual	192.168.173.213	Static	DNS and/or host file
Node 2 Private	`rac2pub`	`rac2prv`	Private	`172.16.1.101`	Static	DNS, host file or none
SCAN vip 1	Selected by Oracle Clusterware	`sa_ cluster1-scan`	Virtual	192.168.173.216	Static	DNS
SCAN vip 2	Selected by Oracle Clusterware	`sa_ cluster1-scan`	Virtual	192.168.173.217	Static	DNS
SCAN vip 3	Selected by Oracle Clusterware	`sa_ cluster1-scan`	Virtual	192.168.173.218	Static	DNS

Installing the Model Repository in a RACed environment

In an Oracle RAC environment, only one of the RAC nodes is used during the SA installation/upgrade process. The SA Installer connects to only one Oracle RAC instance to install/modify the Model Repository. During the regular SA operations, all RAC nodes are used.

Perform the following tasks on the SA server on which you will run the SA Installer; for example, rac1sa.dev.opsware.com.

1. **Model Repository hostname resolution**
   On the server where you will run the SA Installer, ensure that the Model Repository host name `truth` resolves to the remote database server, not to the server on which you will be running the SA Installer:

   In /**etc/hosts**, enter the public IP address of one of the RAC nodes/instances. For example the /etc/hosts file on rac1sa.dev.opsware.com would have the following entry:

   ```
   192.168.173.210 truth rac1pub rac1pub.dev.opsware.com
   ```

   > Note: If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. For example:
   >
   > ```
   > 192.168.173.216 truth sa_cluster1-scan sa_cluster1-scan.dev.opsware.com
   > ```
   >
   > If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

2. **Install the Oracle 11g Full Client on the SA Server**

   > Note: For Oracle 11.2.0.2, use the Oracle Full Client version 11.2.0.2.

   a. The SA Installer uses the Oracle Full Client to connect to the SA server and install the Model Repository. Below are sample commands for installing the Oracle full client.
   Create the database user `oracle` for the Oracle Full Client installation:

   ```
   root@rac1sa ~]# mkdir -p /u01/app/oracle
   root@rac1sa ~]# mkdir -p /u01/app/oraInventory
   root@rac1sa ~]# groupadd oinstall
   root@rac1sa ~]# groupadd dba
   root@rac1sa ~]# useradd -c "Oracle Client software owner" -g oinstall -G
   dba -d /u01/app/oracle -s /bin/bash oracle
   root@rac1sa ~]# chown -R oracle:oinstall /u01/app
   root@rac1sa ~]# chmod -R 775 /u01/app
   root@rac1sa ~]#passwd oracle (change oracle user password)
   ```

   b. Create the **.bash_profile** file.
   Considering the above example, create the **.bash_profile** file in **/u01/app/oracle**.

Temporarily comment out `ORACLE_HOME` and `ORACLE_PATH`. You must uncomment these entries after the Oracle client installation is complete.

Sample .bash_profile file

```
# .bash_profile
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
. ~/.bashrc
fi

# User specific environment and startup programs
PATH=$PATH:$HOME/bin
export PATH

#SA-OracleRAC parameters begin
#unset USERNAME
export ORACLE_BASE=/u01/app/oracle
#export ORACLE_HOME=$ORACLE_BASE/product/11.2.0/client_1
#PATH=$ORACLE_HOME/bin:$ORACLE_HOME/OPatch:$PATH
export PATH

if [ -t ]; then
stty intr ^C
fi

umask 022
#SA-OracleRAC parameters end
```

c. Install the Oracle Full Client.
Install the Oracle Full Client as described in your Oracle documentation. You can create a share to access the Oracle Full Client binaries.

d. Set up Terminals.
You need two X window terminals to install the Oracle Full Client:

Terminal 1: log in as root and enter the commands:

```
Terminal 1> xhost +
```

```
Terminal 2:  ssh –X oracle@<new_oracle_full_client_host>
```

e. Start Oracle Full Client installation
From Terminal 2, run the Oracle Universal Installer (OUI). The Oracle Full Client is installed at **/u01/app/oracle/product/12.1.0/client_1**.

f. Run the Oracle Universal Installer to install Oracle Full Client. The directories in this example assume an Oracle 11g Full Client on Linux.

```
cd /<location_of_oracle_full_client>

./runInstaller
```

g. At the Welcome Screen, click **Next**.

h. Specify the Inventory Directory and Credentials (`/u01/app/oraInventory` and `/u01/app/oinstall`).

i. For Select Installation Type, choose Administrator, click **Next**.

j. For `ORACLE_BASE` select **/u01/app/oracle**, click **Next**.

k. The Oracle Universal Installer performs some checks. If the checks are not successful, fix the issue and re-run this step. If the checks are successful click **Next**.

l. The Oracle OUI will list the products that are to be installed. Click **Install**.

m. The OUI shows the progress bar while installing.

n. On the Welcome to Oracle Net Configuration Assistant window click **Next**.

o. Click **Finish** when the installation completes.

p. You must run the following two configuration scripts as `root` after installation completes:

```
/u01/app/oraInventory/orainstRoot.sh

/u01/app/oracle/product/12.1.0/client_1/root.sh
```

q. Verify that the **.bash_profile** file for the user `oracle` is correct.

r. Uncomment `$ORACLE_HOME` and `$ORACLE_PATH`.

3. **Making changes to tnsnames.ora on an SA Server (Use tnsnames.ora-install_upgrade File)**
By default SA expects the tnsnames.ora file to be located in /var/opt/oracle.

a. Login as `root` on the SA server from which the installer will be run.

b. Enter the command:
```
mkdir -p /var/opt/oracle
```

c. Copy `tnsnames.ora` from the remote database server to the directory you created above. For the RAC environment, copy `tnsnames.ora` from RAC Node 1 (for example, `rac1pub.dev.opsware.com`).

To accommodate the remote Model Repository installation process, two sets of `tnsnames.ora` files are required on the SA server.

- tnsnames.ora-install_upgrade – this copy of `tnsnames.ora` is used during SA installation/upgrade. The file can be renamed.

- tnsnames.ora_install_upgrade – this copy of tnsnames.ora is used during normal SA operation. The file can be renamed.

You can use softlinks to point tnsnames.ora to either tnsnames.ora-install_upgrade or tnsnames.ora_install_upgrade. For example:

```
ln –s tnsnames.ora-install_upgrade tnsnames.ora
```

tnsnames.ora_install_upgrade sample file

```
# tnsnames.ora Network Configuration File:
/u01/app/oracle/product/12.1.0/db_1/network/admin/tnsnames.ora

# Generated by Oracle configuration tools.

RAC1SA_TRUTH =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac1pub.dev.opsware.com)
(PORT = 1521))

(CONNECT_DATA =

(SERVER = DEDICATED)

(SID = truth)

)

)

RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)(PORT=20002)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

Testing the connection from the SA host to the database

Before starting the Model Repository installation/upgrade, you can perform the following tests to verify that your tnsnames.ora file is configured correctly and if the SA Installer can connect to the database.

1. Verify that the SA server's /var/opt/oracle/tnsnames.ora file is configured correctly as described in Making Changes to tnsnames.ora on an SA Server (Use tnsnames.ora-install_upgrade File).
2. On the SA server:
   a. Log in as oracle or root or su – twist/spin – if these users exist.
   b. export ORACLE_HOME=/u01/app/oracle/product/12.1.0/client_1 (or where you installed the Oracle Full Client)
   c. export LD_LIBRARY_PATH=$ORACLE_HOME/lib
   d. export TNS_ADMIN=/var/opt/oracle

e. `set $PATH $ORACLE_HOME/bin path`

f. `sqlplus sys/password@RAC1SA_TRUTH as sysdba;`
where `rac1sa_truth` is the `service_name` or entry from the `tnsnames.ora` file

g. `connect opsware_admin/<password>@RAC1SA_truth`
If you are able to log on to the database, then all files are configured correctly.

SA Installer Core Definition File (CDF)

The installer should be run in 'Expert' mode so that several parameter values can be specified.

You can now start the installation of the SA Model Repository. Ensure that you have the correct parameters values for the installation interview or that you have a previous Core Definition File (CDF).

- `%db.sid: truth1` (Oracle SID of the instance where SA installer is going to connect to.)
- `%db.orahome: /u01/app/oracle/product/12.1.0/client_1`(Oracle client home)
- `%db.port: 1521`(Oracle listener port)
- `%db.host: 192.168.173.210` (server where Oracle RDBMS is installed)
- `%truth.servicename: rac1sa_truth` (value of service name from `tnsnames.ora` file)

You can now install the SA Core as described in the "SA Core installation".

Modify vault.conf SA Installer Core Definition File (CDF)

During the installation process, the vault might not re-start. Change the vault.conf to include the RACed environment connect string. Refer to vault.conf File changes.

Post SA installation process

After you install the SA Core, perform the following tasks in order to use all the nodes in the Oracle RAC environment.

Making changes to tnsnames.ora on the SA Server (Use tnsnames.ora_install_upgrade file)

After SA Core installation is complete, the `tnsnames.ora` file should point/link to the `tnsnames.ora_install_upgrade file`.

In an Oracle RAC environment, only one of the RAC nodes or instances is used during the installation/upgrade process. The SA Installer connects to only one Oracle instance to modify the Model Repository. During normal SA operations, all the RAC nodes are used.

To accommodate the remote database installation process, two sets of `tnsnames.ora` files are required on the SA server.

- tnsnames.ora-install_upgrade – this copy of `tnsnames.ora` is used during SA installation/upgrade. You can rename the file.
- tnsnames.ora_install_upgrade – this copy of `tnames.ora` is used during normal SA operation. You can rename the file.
  You can use softlinks to point `tnsnames.ora` to either `tnsnames.ora-install_upgrade` or `tnsnames.ora_install_upgrade`:

  ```
  ln –s tnsnames.ora_install_upgrade tnsnames.ora
  ```

tnsnames.ora_install_upgrade sample file

> Note: If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

Make a note of the text that is in bold letters. This `tnsnames.ora` file is used during normal SA operation and contains the RAC parameters.

tnsnames.ora_install_upgrade sample file - with Clusterware setup

If you have set up Oracle Clusterware, use the following:

#This entry is for connecting to RAC virtual machines. This entry is used by SA during operation of SA.

```
RAC1SA_TRUTH =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = sa_cluster1-scan.dev.opsware.com)(PORT = 1521))
(LOAD_BALANCE = yes)
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth1)
(FAILOVER_MODE =)
(TYPE = SELECT)
(METHOD = Preconnect)
(RETRIES = 180)
(DELAY = 5))
)
)
```

```
#This entry is for connecting to node2 via service_name. This is for DBA
convenience. This is not used by SA.

RAC2SA_TRUTH =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac2pub.dev.opsware.com)(PORT = 1521))

(CONNECT_DATA =

(UR=A)

(SERVER = DEDICATED)

(SERVICE_NAME = truth2)

)

)
```

#This entry is for connecting to node1 via `service_name`. This is for DBA convenience. This is not used by SA.

```
TRUTH1 =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac1pub.dev.opsware.com)(PORT = 1521))

(CONNECT_DATA =


(SERVER = DEDICATED)

(SERVICE_NAME = truth)

)

)
```

During installation, the SA Installer adds an SA Gateway entry into `tnsnames.ora` file (linked to `tnsnames.ora.install-upgrade`) on the Primary SA Core.

After installation completes, copy that entry into the `tnsname.ora.operational` file. If this entry is not present in the `tnsname.ora.operational` file, Multimaster Mesh transactions will not flow. The following is a sample gateway entry from `tnsnames.ora`:

```
RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)

(PORT=20002)

(PROTOCOL=tcp))

(CONNECT_DATA=(SERVICE_NAME=truth)))
```

tnsnames.ora_install_upgrade sample file - without Clusterware setup

If you have not set up Oracle Clusterware, use the following:

#This entry is for connecting to RAC virtual machines.

```
RAC1SA_TRUTH =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))

(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))

(LOAD_BALANCE = yes)

(CONNECT_DATA =

(SERVER = DEDICATED)

(SERVICE_NAME = truth)

(FAILOVER_MODE =)

(TYPE = SELECT)

(METHOD = Preconnect)

(RETRIES = 180)

(DELAY = 5))

)

)

LISTENERS_TRUTH =

(ADDRESS_LIST =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))

(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))

)
```

#This entry is for connecting to node2 via `service_name`. This entry is optional. This is for DBA convenience. This is not used by SA.

```
RAC2SA_TRUTH2 =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))

(CONNECT_DATA =

(SERVER = DEDICATED)

(SERVICE_NAME = truth)

(INSTANCE_NAME = truth2)
)
)
LISTENER_TRUTH2 =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
```

#This entry is for connecting to node1 using `service_name`. This entry is optional. This is for DBA convenience. This is not used by SA.

```
TRUTH1 =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = truth)
(INSTANCE_NAME = truth1)
)
)
LISTENER_TRUTH1 =
(ADDRESS = (PROTOCOL = TCP)(HOST = rac1-vip.dev.opsware.com)(PORT = 1521))
```

During installation, the SA Installer adds an SA Gateway entry into `tnsnames.ora` file (linked to `tnsnames.ora.install-upgrade`) on the Primary SA Core.

After installation completes, copy that entry into the `tnsname.ora.operational` file. If this entry is not present in the `tnsname.ora.operational` file, Multimaster Mesh transactions will not flow. The following is a sample gateway entry from `tnsnames.ora`:

```
RAC2SA_TRUTH=(DESCRIPTION=(ADDRESS=(HOST=192.168.173.214)
(PORT=20002) (PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

Use softlinks to link the file to `tnsnames.ora` file after SA installation is complete and you are ready to start SA in operational mode.

vault.conf file changes

> Note: If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

In an Oracle RAC environment, the `vault.conf` file must be modified after SA installation is complete. Modify `/etc/opt/opsware/vault/vault.conf` to specify the complete `tnsnames.ora` definition instead of the SID. For example:

- If you have set up Oracle Clusterware, use the following:
  Before:

  ```
  db.sid: truth
  ```

  After:

  ```
  #truth.sid: truth1

  truth.sid: (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
  (HOST = sa_cluster1-scan)(PORT = 1521))

  (LOAD_BALANCE = yes)

  (CONNECT_DATA =(SERVER = DEDICATED)

  (SERVICE_NAME = truth)

  (FAILOVER_MODE = (TYPE = SELECT)

  (METHOD = Preconnect)(RETRIES = 180)(DELAY = 5))))
  ```

- If Oracle Clusterware is not set up, use the following:

  ```
  #truth.sid: truth1

  truth.sid:(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)

  (HOST =rac1-vip.dev.opsware.com)(PORT = 1521)) (ADDRESS = (PROTOCOL = TCP)

  (HOST = rac2-vip.dev.opsware.com)(PORT = 1521))
  (LOAD_BALANCE = yes)

  (CONNECT_DATA = (SERVER = DEDICATED)
  (SERVICE_NAME = truth)

  (FAILOVER_MODE = (TYPE = SELECT)
  (METHOD = Preconnect) (RETRIES = 180)(DELAY = 5))))
  ```

- Also, ensure that these values are correct:
  truth.port: 1521

  ```
  truth.host: 192.168.173.210 (database server IP)

  truth.servicename: rac1sa_truth (tnsnames.ora enter)
  ```

- Restart the vaultdaemon:
  ```
  /etc/init.d/opsware-sas restart vaultdaemon
  ```

da.conf file changes

As of SA 9.10 and later, the Application Deployment Manager reads database connection information from the `tnsnames.ora` file.

In SA 9.10 and 9.1x, the default was `SID =Truth` unless changed by the user; for example, in `/etc/opt/opsware/da/da.conf`:

`truth.sid=truth1` (this is the Oracle SID of the instance on RAC node)

opsware_start.config file changes

This file is located in:

`/opt/opsware/oi_util/startup/opsware_start.config`

> Note: If you have set up Oracle Clusterware, you should use the Clusterware IP address rather than a single database node IP address. If you have set up SCAN name, you should use the SCAN address rather than the database node IP address.

- `TRUTH_HOST="192.168.173.210"` - If Clusterware is not set up, then set the `TRUTH_HOST` value to one of the node's hostnames or public IPs.
- `TRUTH_HOST="sa_cluster1-scan.dev.opsware.com"` - If Clusterware is set up, then set the `TRUTH_HOST` value to the Clusterware scan name.

Setting up a Secondary SA Core in an Oracle RACed environment

During the interview process, the installer asks for the secondary cores' database host information. Enter the IP or host name of the secondary cores single RACed node. During the install process, the installer connects to the database via a single node only.

Upgrading the Model Repository in a RACed environment

To upgrade the Model Repository in an Oracle RAC environment, follow the same procedure as "Installing the Model Repository". If you are doing a remote database installation, ensure that you modify the `tnsnames.ora` file on the server on which the SA Installer is run. HPE recommends that you test the connection as described in "Testing the connection from the SA host to the database".

Setting the Oracle database server OS time zone to a non-UTC

The Oracle Standard, Enterprise or RACed database servers can be set to the non-UTC time zone. For more information, see KM01925296.

Garbage collection

The Garbage Collector (GC) is a set of stored procedures written in PL/SQL that runs in the database on a schedule. The GC procedures look at the `AUDIT_PARAMS` table to determine the retention period to use to delete the old data. The GC PL/SQL procedures are managed by Oracle's `dba_scheduler_jobs`.

Data retention period

When GC runs, it looks at the values in the `AUDIT_PARAMS` table to determine what retention period to use when deleting objects.

> Note: The `AUDIT_PARAMS` table is not replicated, so there is a possibility that these retention periods may become unsynchronized, which can cause severe Multimaster conflict issues. You must ensure that the values in the `AUDIT_PARAMS` table are exactly the same for all the cores in a mesh.

```
# Sqlplus "/ as sysdba"

SQL> col name format a20;

SQL> col value format a20;

SQL> col AUDIT_PARAM_ID format a15;

SQL> select AUDIT_PARAM_ID, NAME, VALUE from audit_params;
```

The parameters from `AUDIT_PARAMS` table and their default values are:

```
AUDIT_PARAM_ID  NAME                 VALUE

--------------- -------------------- --------------------

2               DAYS_WAY                30              (These are the completed way sessions)

3               DAYS_CHANGE_LOG         180             (These are the server history events)

4               LAST_DATE_WAY           02-NOV-16

5               LAST_DATE_CHANGE_LOG    05-JUN-16

6               DAYS_AUDIT_LOG          180             (These are the audit logs)

7               LAST_DATE_AUDIT_LOG     180

8               DAYS_WLM                30              (These are completed WLM jobs)

9               LAST_DATE_WLM           02-NOV-16
```

> Note: As of SA 9.10, the DAY_TRAN parameter that controlled retention time for transactions was removed. To control transaction retention time, instead use the system configuration parameter vault.garbageCollector.daysToPreserve.
>
> Select the **Administration** tab in the SA Client, then select System Configuration in the navigation panel. Select Model Repository Multimaster Component. Locate and change the value.

> The value for LAST_DATE_WAY , LAST_DATE_CHANGE_LOG , LAST_DATE_AUDIT_LOG , and LAST_DATE_WLM parameters should be the date when the system was installed - 30 days.

> For a fresh core installation, the default value of LAST_DATE_AUDIT_LOG is 180. After the audit is run, the value will be the date of the last audit job.

Modifying the retention period values

To update the data, run a SQL command similar to the following example as user LCREP:

```
# su - oracle

# sqlplus "/ as sysdba"

SQL> grant create session to lcrep;

SQL> connect lcrep/<password>

SQL> update AUDIT_PARAMS set value=30 where name = 'DAYS_AUDIT_LOG';

SQL> commit;
```

> Note: The values in the AUDIT_PARAMS table must be exactly the same for all the cores in a mesh.

Viewing GC DBA_SCHEDULER_JOBS

When the Model Repository is installed, the SA Installer sets up these jobs, which perform garbage collection.

GC jobs can be viewed by logging in to SQL*Plus and running the following SQL commands:

```
# Su - oracle

# Sqlplus "/ as sysdba"

SQL> set line 200

SQL> col job_name format a50

SQL> col owner format a14

SQL> col last_date format a17

SQL> col next_date format a17
SQL> col job_action format a50


SQL>select job_name, owner, to_char(LAST_START_DATE, 'MM/DD/YY HH:MI:SS') last_
date,to_char(next_run_date, 'MM/DD/YY HH:MI:SS') next_date, job_action

from dba_scheduler_jobs where owner='GCADMIN';

JOB_NAME                 OWNER   LAST_DATE         NEXT_DATE         JOB_ACTION

------------------------ ------- ----------------- ----------------- --------------
   --------------------------

WLMPURGE_GC              GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 WLMPURGE.GC_
   JOBS

STORAGEINITIATORPURGE_GC GCADMIN 04/02/12 09:47:30 04/03/12 10:47:30
   STORAGEINITIATORPURGE.GC_

   STORAGEINITIATORS

AUDITPURGE_GC            GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 AUDITPURGE.GC_
   AUDITLOGS

CHANGELOGPURGE_GC        GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00
   CHANGELOGPURGE.GC_CHANGELOGS

WAYPURGE_GC              GCADMIN 04/02/12 09:00:02 04/04/12 09:00:00 WAYPURGE.GC_
   SESSIONS
```

where:

`WAYPURGE.GC_SESSIONS` - Performs a `sessions` garbage collection

`CHANGELOGPURGE.GC_CHANGELOGS` - Performs a `changelogs` garbage collection

`AUDITPURGE.GC_AUDITLOGS` - Performs `auditlogs` garbage collection

`STORAGEINITIATORPURGE.GC_STORAGEINITIATORS` - Performs `storage data` garbage collection

`WLMPURGE.GC_JOBS` - Performs WLM garbage collection

Manually running GC jobs

You can run GC jobs by logging in to SQL*Plus and entering the following:

```
# Su - oracle

# Sqlplus "/ as sysdba"


SQL> grant create session to gcadmin
SQL> connect gcadmin/<password>

SQL> exec dbms_scheduler.run_job('<job_name_value>');

For example, this sample command runs the waypurge_gc job:

SQL> exec dbms_scheduler.run_job('WAYPURGE_GC');
```

Database monitoring strategy

Since the Model Repository is a critical component of SA, the DBA should implement a monitoring strategy. The DBA can write custom monitoring scripts or use third-party products.

This section contains example commands for monitoring the Oracle database used by the Model Repository. When issuing the commands shown in this section, you must be logged on to the server as the user `oracle`:

```
$ su - oracle
```

The SQL commands shown in this section are entered in the `sqlplus` command-line utility. To run `sqlplus`, log on as `oracle` and enter the following command:

```
$ sqlplus "/ as sysdba"
```

Verifying if the database instances are up and responding

To verify if the database instances are up and running:

1. Enter the following command to check if the Oracle processes are running:
   ```
   ps -ef | grep ora_
   ```
   This `ps` command should generate output similar to the following lines:
   ```
   oracle   14674     1  0 Apr18 ?        00:00:00 ora_pmon_truth

   oracle   14676     1  0 Apr18 ?        00:00:00 ora_psp0_truth

   oracle   14678     1  0 Apr18 ?        00:00:00 ora_vktm_truth

   oracle   14682     1  0 Apr18 ?        00:00:00 ora_gen0_truth

   oracle   14684     1  0 Apr18 ?        00:00:00 ora_diag_truth
   ```

```
    oracle   14686      1  0 Apr18 ?        00:00:00 ora_dbrm_truth
    oracle   14688      1  0 Apr18 ?        00:05:57 ora_dia0_truth
    oracle   14690      1  0 Apr18 ?        00:00:00 ora_mman_truth
    oracle   14692      1  0 Apr18 ?        00:00:00 ora_dbw0_truth
    oracle   14694      1  0 Apr18 ?        00:00:01 ora_lgwr_truth
    oracle   14696      1  0 Apr18 ?        00:00:28 ora_ckpt_truth
    oracle   14698      1  0 Apr18 ?        00:00:04 ora_smon_truth
    oracle   14700      1  0 Apr18 ?        00:00:00 ora_reco_truth
    oracle   14702      1  0 Apr18 ?        00:00:13 ora_mmon_truth
    oracle   14704      1  0 Apr18 ?        00:00:13 ora_mmnl_truth
    oracle   14728      1  0 Apr18 ?        00:00:00 ora_qmnc_truth
    oracle   14775      1  0 Apr18 ?        00:00:01 ora_cjq0_truth
    oracle   14779      1  0 Apr18 ?        00:00:00 ora_q000_truth
    oracle   14781      1  0 Apr18 ?        00:00:00 ora_q001_truth
    oracle   14832      1  0 Apr18 ?        00:00:00 ora_smco_truth
    oracle   22619      1  0 22:38 ?        00:00:00 ora_w000_truth
```

2. Verify if the database status is `ACTIVE` by entering the following command in `sqlplus`:
   ```
   SQL>select database_status from v$instance;
   ```

3. Verify if the open mode is `READ WRITE` by entering the following command in `sqlplus`:
   ```
   SQL>select name, log_mode, open_mode from v$database;
   ```

Verifying if the data files are online

Enter the following commands to verify if the data files are online, in SQL*Plus, :

```
SQL>Col file_name format a50

SQL>Col status format a10

SQL>Set line 200

SQL>Select file_id, status, bytes, file_name from dba_data_files order by
SQL>tablespace_name;
```

The status should be AVAILABLE for all the data files.

Verifying if the listener is running

To verify if the listener is running:

1. Check to see if the Oracle listener processes are running by entering the following command:

   ```
   ps -ef | grep tns


   oracle   11664     1  0 Mar22 ?        00:08:05
   /u01/app/oracle/product/12.1.0/db_1/bin/tnslsnr LISTENER -inherit

   oracle   22725 22706  0 22:44 pts/2    00:00:00 grep tns
   ```

2. Check the status of the listener with the `lsnrctl` command:

   ```
   lsnrctl status
   ```

   The listener should be listening on port 1521 (default), or on the port that you have designated that the Oracle listener process use, with the TCP protocol, and should be handling the instance named truth. The `lsnrctl` command should generate output similar to the following lines:

   ```
   ...

   Connecting to (ADDRESS=(PROTOCOL=tcp)

   (HOST=per1.performance.qa.example.com)(PORT=1521))

   . . .

   Instance "truth", status READY, has 1 handler(s) for this service...
   ```

3. Test connectivity to the instance from the Data Access Engine (spin) and Web Services Data Access Engine (twist) hosts by running the `tnsping` utility:

   ```
   tnsping truth
   ```

   The `OK` statement displayed by the `tnsping` utility confirms that the listener is up and can connect to the instance. The `tnsping` utility should generate output similar to the following lines:

   ```
   ...

   Used parameter files:


   Used HOSTNAME adapter to resolve the alias

   Attempting to contact (DESCRIPTION=(CONNECT_DATA=(SERVICE_
   NAME=truth.performance.qa.example.com))(ADDRESS=(PROTOCOL=TCP)
   (HOST=192.168.165.178)(PORT=1521)))
   ```

```
OK (0 msec)
```

```
Attempting to contact (DESCRIPTION=(ADDRESS=(HOST=localhost)(PORT=1521)
(PROTOCOL=tcp))(CONNECT_DATA=(SERVICE_NAME=truth)))
```

```
OK (0 msec)
```

As an alternative to running the `tnsping` utility in this step, you can check the connectivity by running `sqlplus` and connecting to the database instance with the service name (TNS alias), for example:

```
sqlplus myuser/mypass@truth
```

Examining the log files

To examine the log files:

1. Look for errors in the `alert_<SID>.log` file.
   For each instance, locate the `alert_<SID>.log` file in the background dump destination directory:

   $ORACLE_BASE/diag/rdbms/<SID>/<SID>/trace/

   This is an example `bdump` directory for an instance with the `truth` SID:

   /u01/app/oracle/diag/rdbms/truth/truth/trace/

2. Look for errors in the other log and trace files, located in various directories under:
   $ORACLE_BASE/diag/rdbms/<SID>/<SID>

Checking for sufficient free disk space in tablespaces

To check for sufficient disk space:

1. Enter the following commands in `sqlplus`:

   ```
   SQL>set line 200
   ```

   ```
   SQL>column dummy noprint
   ```

   ```
   SQL>column pct_used format 999.9 heading "Pct|Used"
   ```

   ```
   SQL>column name format a16 heading "Tablespace Name"
   ```

   ```
   SQL>column mbytes format 999,999,999 heading "Current|File Size|MB"
   ```

```
SQL>column used format 999,999,999 heading "Used MB "
SQL>column free format 999,999,999 heading "Free MB"
SQL>column largest format 999,999,999 heading "Largest|Contigous|MB"
SQL>column max_size format 999,999,999 heading "Max Possible|MB"
SQL>column pct_max_used format 999.999 heading "Pct|Max|Used"
SQL>break on report
SQL>compute sum of Mbytes on report
SQL>compute sum of free on report
SQL>compute sum of used on report


SQL>SELECT
    nvl(df.tablespace_name,'UNKOWN') name, df.mbytes_alloc Mbytes,
    df.mbytes_alloc-nvl(fs.mbytes_free,0) used, nvl(fs.mbytes_free,0) free,
    ((df.mbytes_alloc-nvl(fs.mbytes_free,0)) / df.mbytes_alloc) * 100 pct_used,
    nvl(df.largest,0) largest, nvl(df.mbytes_max,df.mbytes_alloc) Max_Size,
    ((df.mbytes_alloc-nvl(fs.mbytes_free,0)) / df.mbytes_max) * 100 pct_max_
used
FROM
    (   SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_alloc, max(bytes)
/1024/1024 largest,
            sum(decode(autoextensible,'YES',greatest(bytes,maxbytes),bytes))
/1024/1024 Mbytes_max
        FROM
            dba_data_files GROUP BY tablespace_name
    ) df,
    ( SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_free
        FROM dba_free_space GROUP BY tablespace_name
    ) fs
WHERE
    df.tablespace_name = fs.tablespace_name(+)
UNION
```

```
SELECT
    D.tablespace_name name, D.mbytes_alloc Mbytes, ((ss.used_blocks * F.block_size) / 1024 / 1024) used,
    D.mbytes_alloc - ((ss.used_blocks * F.block_size) / 1024 / 1024) free,
    ((D.mbytes_alloc-nvl((D.mbytes_alloc - ((ss.used_blocks * F.block_size) / 1024 / 1024)),0)) / D.mbytes_alloc) * 100 pct_used,
    nvl(((G.max_blocks * F.block_size) / 1024 / 1024),0) largest, Max_Mbytes Max_Size,
    ((D.mbytes_alloc-nvl((D.mbytes_alloc - ((ss.used_blocks * F.block_size) / 1024 / 1024)),0)) / D.Max_Mbytes) * 100 pct_pct_used
FROM
    (   SELECT tablespace_name, used_blocks, free_blocks, max_size
        FROM v$sort_segment
    ) ss,
    (   SELECT tablespace_name, sum(bytes)/1024/1024 Mbytes_alloc,
            sum(decode(autoextensible,'YES',greatest(bytes,maxbytes),bytes))/1024/1024 Max_Mbytes
        FROM dba_temp_files GROUP BY tablespace_name
    ) D,
    (   SELECT B.name, C.block_size, SUM (C.bytes) / 1024 / 1024 mb_total
        FROM v$tablespace B, v$tempfile C
        WHERE B.ts#= C.ts# GROUP BY B.name, C.block_size
    ) F,
    (   SELECT B.name, max(blocks) max_blocks, sum(blocks) total_blocks
        FROM v$tablespace B, v$tempfile C
        WHERE B.ts#= C.ts# GROUP BY B.name
    ) G
WHERE ss.tablespace_name = D.tablespace_name and ss.tablespace_name = F.name and ss.tablespace_name = G.name;
```

In the output generated by the preceding commands, compare the numbers under the `Used` and `Free` headings.

2. To list the existing data, index, and temporary files, enter the following commands in `sqlplus`:
   ```
   SQL>Select file_id, bytes, file_name from dba_data_files;
   ```
3. If a tablespace has auto-extended to its maximum size and is running out of disk space, then add new data files by entering the `ALTER TABLESPACE` command in `sqlplus`.
   The following example commands add data files to four of the tablespaces. For a full list of tablespaces and data files, see the output generated by the commands in the preceding two steps.
   ```
   SQL>ALTER TABLESPACE AAA_DATA

   SQL>ADD DATAFILE '/u01/oradata/truth/aaa_data10.dbf'

   SQL>SIZE 32M AUTOEXTEND ON NEXT 128M MAXSIZE 4000M ;


   SQL>ALTER TABLESPACE "AAA_INDX"

   SQL>ADD DATAFILE '/u02/oradata/truth/aaa_indx11.dbf'

   SQL>SIZE 32M AUTOEXTEND ON NEXT 128M MAXSIZE 4000M ;


   SQL>ALTER TABLESPACE "UNDO"

   SQL>ADD DATAFILE '/u03/oradata/truth/undo12.dbf' SIZE 32M AUTOEXTEND ON NEXT
   128M MAXSIZE 4000M ;


   SQL>ALTER TABLESPACE "TEMP" ADD

   SQL>TEMPFILE '/u04/oradata/truth/temp14.dbf' SIZE 32M AUTOEXTEND ON NEXT 128M
   MAXSIZE 4000M ;
   ```

Enabling the collection of Oracle Automatic Optimizer statistics

As of SA 10.0 the schema and index statistics collection for SA database user `AAA`, `TRUTH` etc. has been moved from `dba_jobs` to Oracle's Automatic Optimizer Statistics Collection.

SA relies on Oracle’s Automatic Optimizer statistics collection to collect schema statistics used to avoid database performance degradation. By default, Oracle’s Automatic Optimizer statistics collection should be enabled.

To verify if the Oracle Automatic Optimizer statistics collection is enabled:

1. Enter the following commands in SQL*Plus:

   ```
   # su - oracle

   # sqlplus "/ as sysdba"


   SQL>set line 200

   SQL>col status format a10

   SQL>SELECT status FROM dba_autotask_client where client_name='auto optimizer
   stats collection';

   The output from the above statement should be as follows:

   STATUS

   ----------

   ENABLED
   ```

2. If the status is not `ENABLED`, execute the following statement to enable Oracle’s Automatic Optimizer statistics collection.

   ```
   SQL>EXEC DBMS_AUTO_TASK_ADMIN.ENABLE(client_name => 'auto optimizer stats
   collection',operation => NULL, window_name => NULL);
   ```

Verifying if the database jobs (System/Index statistics and garbage collection) ran successfully

When the Model Repository is installed, the SA Installer sets up the System/Index Statistics and the Garbage Collection jobs in Oracle's `dba_scheduler_jobs` which then runs these jobs at specified time-intervals. The jobs perform system/ index statistics collection and garbage collection. If the system/index statistics collection jobs do not run successfully, database performance degrades. If the garbage collection jobs do not run, old data accumulates and requires additional disk space. Performance can also be affected.

To verify if the jobs in `DBA_SCHEDULER_JOBS` ran successfully:

1. Enter the following commands in SQL*Plus:

   ```
   SQL>set line 200

   SQL>col job_name format a50

   SQL>col owner format a14
   ```

```
SQL>col last format a17

SQL>col next format a17

SQL>col state format a10

SQL>col job_action format a50


SQL>select job_name, owner, to_char(LAST_START_DATE, 'MM/DD/YY HH:MI:SS')

last, to_char(next_run_date, 'MM/DD/YY HH:MI:SS') next, state, job_action

from dba_scheduler_jobs where owner in ('OPSWARE_ADMIN', 'LCREP', 'GCADMIN');
```

In the output generated from the preceding statement, the value of the `JOB_ACTION` column indicates the type of job. The jobs owned by `GCADMIN` perform the garbage collection. The job owned by `LCREP` performs index statistics collection and the job owned by `OPSWARE_ADMIN` performs system statistics collection. Sample output looks like this:

```
JOB_NAME             OWNER         LAST              NEXT              STATE
      JOB_ACTION

-------------------- ------------- ----------------- ----------------- --------
    -- ---------------------------------

WLMPURGE_GC          GCADMIN       04/03/12 09:00:00 04/04/12 09:00:00
    SCHEDULED  WLMPURGE.GC_JOBS

STORAGEINITIATOR     GCADMIN       04/03/12 09:00:00 04/02/12 09:47:30
    SCHEDULED  STORAGEINITIATORPURGE.GC_

PURGE_GC
      STORAGEINITIATORS

AUDITPURGE_GC        GCADMIN       04/03/12 09:00:00 04/04/12 09:00:00
    SCHEDULED  AUDITPURGE.GC_AUDITLOGS

CHANGELOGPURGE_GC    GCADMIN       04/03/12 09:00:00 04/04/12 09:00:00
    SCHEDULED  CHANGELOGPURGE.GC_CHANGELOGS

WAYPURGE_GC          GCADMIN       04/03/12 09:00:00 04/04/12 09:00:00
    SCHEDULED  WAYPURGE.GC_SESSIONS

LCREP_INDEX_STATS    LCREP         04/02/12 11:00:00 04/03/12 11:00:00
    SCHEDULED  gather_lcrep_stats

OPSWARE_ADMIN_SYSTEM OPSWARE_ADMIN 04/02/12 06:00:00 04/03/12 06:00:00
    SCHEDULED  gather_opsware_admin_sys_stats

_STATS


7 rows selected.
```

where:

- JOB_NAME - name of the job
- OWNER - the user who with permissions to run the job
- LAST - last date-time when the job was run
- NEXT - next date the job will run
- STATE - The status of the scheduled job:
  - disabled - The job is disabled
  - scheduled - The job is scheduled to be executed
  - running - The job is currently running
  - completed - The job has completed, and is not scheduled to run again
  - broken - The job is broken
  - failed - The job was scheduled to run once and failed
  - retry scheduled - The job has failed at least once and a retry has been scheduled to be executed
  - succeeded - The job was scheduled to run once and completed successfully
  - JOB_ACTION - the procedure that the job runs

Changes to the database statistics job

Starting with Oracle 10g, the `DBMS_JOB` package was superceded by the improved Oracle Scheduler (`dbms_scheduler`) package. Although Oracle still supports the `DBMS_JOB` package for backward compatibility, Oracle will make no further enhancements to the package. Since the `DBMS_SCHEDULER` provides better functionality, all the SA jobs that used the `DBMS_JOB` package have been redesigned in this release to use the `DBMS_SCHEDULER` package. The affected jobs can be found in the `dba_scheduler_jobs` table. These changes are only relevant to new SA 10.x Cores and cores upgraded to SA 10.x.

To view the jobs and changes made, you can run the following from SQL*Plus:

```
# Su - oracle

# Sqlplus "/ as sysdba"

SQL>set line 200

SQL>col owner format a14

SQL>col job_action format a50

SQL>col job_name format a50
SQL>select job_name, owner, job_action from dba_scheduler_jobs where owner in

('OPSWARE_ADMIN', 'LCREP', 'GCADMIN');
```

Your output should be as follows:

```
JOB_NAME                                      OWNER         JOB_ACTION

-------------------------------------------   ------------- -----------------------
   --

WLMPURGE_GC                                   GCADMIN       WLMPURGE.GC_JOBS

STORAGEINITIATORPURGE_GC                      GCADMIN
   STORAGEINITIATORPURGE.GC_
                                                               STORAGEINITIATORS

AUDITPURGE_GC                                 GCADMIN       AUDITPURGE.GC_AUDITLOGS

CHANGELOGPURGE_GC                             GCADMIN       CHANGELOGPURGE.GC_
                                                               CHANGELOGS

WAYPURGE_GC                                   GCADMIN       WAYPURGE.GC_SESSIONS

LCREP_INDEX_STATS                             LCREP         gather_lcrep_stats

OPSWARE_ADMIN_SYSTEM_STATS                    OPSWARE_ADMIN gather_opsware_admin_

                                                            sys_stats


7 rows selected.
```

Running dba_scheduler_jobs manually

If you need to run the System/Index Statistics and the Garbage Collection jobs manually, you must first grant the following privilege.

```
SQL> grant create session to lcrep, gcadmin;
```

To run the statistics collection jobs manually in SQL*Plus, use the commands shown below. If you copy and paste the following command examples, replace the variables like `schema_user_value` with the values of the **schema_user** column displayed by the preceding select statement. Substitute the variables such as `job_name_value` with the values of the `job` column displayed by the same select statement.

```
SQL> connect <schema_user_value>/<password>

SQL> exec dbms_scheduler.run_job('<job_name_value>');
```

After you are done running the jobs, you should revoke the privileges granted above. Log in to SQL*Plus and enter the following command:

```
SQL> revoke create session from lcrep, gcadmin;
```

Changing the time jobs are run

`dba_scheduler_jobs` are run at UTC time. To change the time when the jobs are run, follow these instructions:

```
sqlplus "/ as sysdba"

SQL>set line 300

SQL>col job_name format a30

SQL>col owner format a14

SQL>col last format a17

SQL>col next format a17

SQL>col repeat_interval format a40

SQL>col job_action format a30


SQL>select job_name, owner, to_char(LAST_START_DATE, 'MM/DD/YY HH:MI:SS') last, to_
char(next_run_date, 'MM/DD/YY HH:MI:SS') next, repeat_interval, job_action from
dba_scheduler_jobs where owner in ('OPSWARE_ADMIN', 'LCREP', 'GCADMIN');

The above statement provides information about a job. Note the job name and the
owner that has the privilege to run this job.
```

The output of the above statement is similar to the following (formatting is compressed due to space limitations):

```
JOB_NAME                      OWNER     LAST              NEXT              REPEAT_
    INTERVAL        JOB_ACTION

------------------------------ -------  ----------------- ----------------- -------
    --------------- --------------

WLMPURGE_GC                    GCADMIN  04/02/12 09:00:02 04/04/12 09:00:00 TRUNC
    (SYSDATE+1)+

                                                                            9/24
                   WLMPURGE.GC_JOBS

STORAGEINITIATORPURGE_GC       GCADMIN  04/02/12 09:47:30 04/03/12 10:47:30
    SYSDATE+1/24           STORAGE


                   INITIATOR


                   PURGE.GC_


                   STORAGE
                   INITIATORS

AUDITPURGE_GC                  GCADMIN  04/02/12 09:00:02 04/04/12 09:00:00 TRUNC
    (SYSDATE+1)+9/24  AUDITPURGE.GC_


                   AUDITLOGS

CHANGELOGPURGE_GC              GCADMIN  04/02/12 09:00:02 04/04/12 09:00:00 TRUNC
    (SYSDATE+1)+9/24  CHANGELOGPURGE.


                   GC_CHANGELOGS

WAYPURGE_GC                    GCADMIN  04/02/12 09:00:02 04/04/12 09:00:00 TRUNC
    (SYSDATE+1)+9/24  WAYPURGE.GC_


                   SESSIONS

LCREP_INDEX_STATS              LCREP    04/01/12 11:00:04 04/03/12 11:00:00 TRUNC
    (SYSDATE+2)+11/24 gather_lcrep_


                   stats

OPSWARE_ADMIN_SYSTEM_STATS     OPSWARE  04/02/12 06:00:01 04/03/12 06:00:00 TRUNC
    (SYSDATE+1) +

                               _ADMIN                                       18/24 +
    mod(abs(to_    gather_opsware

                                                                            number
    (to_char)        admin_sys_stats


    (sysdate + 1,'D'))

                                                                            - 7) +
    2,7)


7 rows selected.
```

In this example the user `lcrep` changes the time/interval at which the job is run. Any other user can be substituted for the user `lcrep`.

```
sqlplus "connect / as sysdba"

SQL> grant create session to lcrep;

Grant succeeded.
```

In the example:

```
job name=LCREP_INDEX_STATS

owner = lcrep
```

In this example, the job `LCREP_INDEX_STATS` runs at 11:00 a.m. UTC. To change this to 9:00 a.m. UTC, the command is:

```
SQL> connect lcrep/<password_for_lcrep>

Connected.
```

SQL> exec dbms_scheduler.set_attribute('LCREP_INDEX_STATS', attribute=>'REPEAT_INTERVAL', value=>'TRUNC(SYSDATE+2)+9/24');

Monitoring database users

To monitor database users:

1. To check the database users, enter the following command in `sqlplus`:

   ```
   # su - oracle

   $ sqlplus "/ as sysdba"

   SQL>Select username, account_status, default_tablespace,

   temporary_tablespace from dba_users;
   ```

Monitoring the ERROR_INTERNAL_MSG table

Various SA internal PL/SQL procedures write exceptions to the `truth.ERROR_INTERNAL_MSG` table. You should monitor this table for errors (daily checks are recommended) on all Model Repository (Oracle) databases.

Executing the SQL below lists the data in `error_internal_msg` from the last fifteen days.

> Note: You can remove the `WHERE` clause if you want to display all data in the `truth.ERROR_INTERNAL_MSG` table.

```
# Su - oracle

# Sqlplus "/ as sysdba"

SQL> set line 200

SQL> col ERR_ID format 999999

SQL> col ERR_USER format a8

SQL> col ERR_TABLE format a25

SQL> col ERR_TABLE_PK_ID format a10
```

```
SQL> col ERR_CODE format 9999999

SQL> col ERR_TEXT format a20

SQL> col ERR_INFO format a30


SQL> select ERROR_INTERNAL_MSG_ID ERR_ID,

ERR_DATE,

ERR_USER,

ERR_TABLE,

ERR_TABLE_PK_ID,

ERR_CODE,

ERR_TEXT,

DELETE_FLG,

ERR_INFO

from ERROR_INTERNAL_MSG

where ERR_DATE > sysdate - 15

order by ERR_DATE;
```

Rebuilding the SHADOW_FOLDER_UNIT table

The procedure SHADOW_FOLDER_UNIT_RELOAD is provided in case the contents of SHADOW_FOLDER_UNIT table becomes out of synchronization or there are multiple records of the type (shadow_folder_unit.folder_id = -1).

The table can be rebuilt without stopping the system. Simply connect as user TRUTH, TWIST, SPIN, or OPSWARE_ADMIN and issue the command:

```
SQL>exec SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD
```

Check the results from monitoring the ERROR_INTERNAL_MSG table. If the results contain:

```
'ERR_TABLE' = 'UNIT_RELATIONSHIPS'
```

Perform the following:

1. Check if there are records in `truth.SHADOW_FOLDER_UNIT` of the type (`folder_id = -1`).

   ```
   SQL> connect / as sysdba
   SQL>  select count(*) from shadow_folder_unit where folder_id = -1;
   ```

2. If the above SQL returns a value greater than zero, then run the following during low database usage time:

   ```
   SQL> grant create session to truth;
   SQL> connect truth/<password>
   SQL> exec SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD;
   ```

3. Run the SQL from "Monitoring the ERROR_INTERNAL_MSG table" and check if the procedure has listed any faulty records. `SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD` is idem potent therefore the faulty records can be fixed and you can rerun `SHADOW_FOLDER_UNIT_UTIL.SHADOW_FOLDER_UNIT_RELOAD`.
   HPE recommends that you gather table statistics after the data reload:

   ```
   SQL> connect truth/<password>
   SQL> exec dbms_stats.gather_table_stats (
                   ownname=> 'TRUTH',
                   tabname=> 'SHADOW_FOLDER_UNIT',
                   estimate_percent=> DBMS_STATS.AUTO_SAMPLE_SIZE,
                   cascade => true);
   ```

4. Revoke the permissions given to user `truth`:

   ```
   SQL> connect / as sysdba
   SQL> revoke create session from truth;
   ```

Oracle database backup methods

It is important that you back up the database on a regular basis. Be sure to use more than one backup method and to test your recovery process.

You can use the following methods to back up the Oracle database:

- **Export-Import**: An export extracts logical definitions and data from the database and writes the information to a file. Export-import does not support point-in-time recoveries. Do not use Export-Import as your only backup and recovery strategy.

See the information on the `Export-Import` subdirectory in "Oracle/SA Installation Scripts, SQL Scripts, and configuration files".

- **Cold or Off-Line Backups**: This procedure shuts the database down and backs up all data, index, log, and control files. Cold or off-line backups do not support point-in-time recoveries.
- **Hot or Online Backups**: During these backups, the database must be available and in `ARCHIVELOG` mode. The tablespaces are set to backup mode. This procedure backs up tablespace files, control files, and archived redo log files. Hot or online backups support point-in-time recoveries.
- **RMAN Backups**: While the database is either off-line or on-line, use the `rman` utility to back up the database.

Regardless of your backup strategy, remember to back up all required Oracle software libraries, parameter files, password files, and so forth. If your database is in `ARCHIVELOG` mode, you also need to back up the archived log files.

For more information on backing up Oracle databases, refer to the documentation on the Oracle website.

Troubleshoot system diagnosis errors

If an additional privilege (permission) has been made manually to the database, when SA performs a system diagnosis on the Data Access Engine, an error message might be generated. For example, if an additional grant has been made to the `truth.facilities` table, the following error appears:

```
Test Information

Test Name: Model Repository Schema

Description: Verifies that the Data Access Engine's version of the schema

matches the Model Repository's version.

Component device: Data Access Engine (spin.blue.qa.example.com)

Test Results: The following tables differ between the Data Access Engine and the
Model Repository:  facilities.
```

To fix this problem, revoke the grant. For example, if you need to revoke a grant on the `truth.facilities` table, log on to the server with the database and enter the following commands:

```
su - oracle

sqlplus "/ as sysdba"

SQL>grant create session to truth;
SQL>connect truth/<truth passwd>;

SQL>revoke select on truth.facilities from spin;

SQL>exit

sqlplus "/ as sysdba"

SQL>revoke create session from truth;
```

Useful SQL

The following SQL commands help you manage information in the Oracle database.

BIN$ objects

If the SA Installer discovers the existence of `BIN$` objects in the database, enter the following SQL commands:

```
SQL>show parameter recyclebin;

SQL>SELECT owner,original_name,operation,type FROM dba_recyclebin;

connect <owner>/password

SQL>purge recyclebin;

or

SQL>purge table BIN$xxx;
```

By default, `recyclebin` is set to `OFF`.

SA Core installation

This section describes the installation tasks for SA Cores.

> Caution: You must verify that your SA Core and satellite host servers meet the requirements listed in "System requirements for installation ". If you do not, your installation may fail or core performance may be affected.

SA Core installation overview

This section describes how to install an SA Core. This guide describes the following samples of core installations:

1. SA Core with a Local SA-supplied Database
2. SA Core with a Remote Customer-supplied Oracle Database
3. SA Core with a Remote Customer-supplied Database and Additional Slice Component Bundles
4. SA First (Primary) Core with a Secondary Core (Multimaster Mesh)

For an existing core you can also perform the following:

1. Installing Additional Slice Component Bundles
2. Installing a Satellite

If you are installing a standalone core or the First Core of a Multimaster Mesh, you must perform the tasks described in this section.

There are certain additional post-installation tasks you may need to perform after installing the core, see "SA Core post-installation tasks".

> If you are installing the subsequent cores of a *Multimaster Mesh,* you must complete the tasks described in "Install SA first (primary) core with a secondary Core (multimaster mesh)" to add additional cores to your mesh. If you have a requirement for more than one Secondary Core in a mesh, you must contact HPE Professional Services or a certified HPE Consultant.

A First Core has all the components required to be the *primary core* of a Multimaster Mesh. You simply need to add a Secondary Core configured to manage servers and communicate with the First Core. In a Multimaster Mesh installation, a First Core's role is not much different than any other core's role in the mesh, however, it does have additional centralized Core Components that oversee communication between the various cores as well as manage conflicts and load balancing.

Installation phases

A typical SA Core installation has the following phases:

1. *Before Installation*: Ensure that you:
   - Have decided on an appropriate Core Configuration, see "SA Core configuration for your facility".
   - Ensure that all core host installation prerequisites have been met
   - Have the information needed to complete the SA Installer interview
   - Have all necessary permissions to complete the installation
   - Have the SA installation media.
   - Invoke the SA Installer only from the SA Product Software media or mounted copy
     For more information, see "System requirements for installation ".
2. *Database Installation*: The Model Repository requires that an Oracle database is installed and available before the SA Installer is run. You can:
   - Install the *SA-supplied Oracle database* that is provided with the SA product software and installed with the SA Core.
   - Use a *self-installed Oracle database installation* that you have configured for use with SA. This database must be installed and running before you begin the SA Core installation and reserved for use only by SA.
   - Install a database using the *Oracle Universal Installer* before beginning the SA installation and configure it for use with SA. This database must be only used by SA.
     If you plan to use an existing non-SA-supplied Oracle database installation it must be configured for SA, see "Oracle setup for the Model Repository").
3. *SA Installation Interview*: When you install an SA Core, you are required to complete the SA Interview during which you are asked to provide the values for certain SA configuration parameters. At the end of the interview, SA automatically saves the configuration information to a Core Definition file (CDF). This CDF may also be used later during Secondary Core (multimaster Mesh), and Satellite installation and during SA Core upgrades.
4. SA *Core Component Installation*: After you complete the SA Interview, the SA Installer installs the SA Core Components on your host server(s).

5. *After Installation*: You must complete the post-installation tasks. For more information, "SA Core post-installation tasks".

> **Note:** If the SA Installer encounters an error, the installation stops. Correct all the errors before you retry the installation. For information about restarting an interrupted installation, see "Restart an interrupted installation".

Oracle database installation options

A functioning, properly configured Oracle 12c database must be available *before* you begin the SA installation process. You can choose to:

- See the SA Support and Compatibility Matrix for supported Oracle versions.
- Use the SA-supplied Oracle 12c database and allow the SA Installer to install and pre-configure the database. If you choose to install the SA-supplied Oracle database, the SA Installer guides you through the process as described in this section.
  The SA-supplied Oracle database requires that certain system and Oracle environment variables be specified for use with SA. See "SA-supplied Oracle RDBMS software and database setup".
- Use the Oracle Universal Installer to install a non-SA-supplied Oracle 12c database. However, you must manually configure this database for use with SA. For required Oracle configuration information, see "Non-SA-supplied Oracle software and database setup". If you choose to use the Oracle Universal Installer to install Oracle, you must install the database before running the SA Installer, and have all database-related information required by the Installer Interview, such as passwords, the path to `ORACLE_HOME`, and so on.
- Use an existing Oracle 12c installation. This database must be for the exclusive use of SA. You must manually configure this database for use with the SA Model Repository. For more information about the required configuration, see "Non-SA-supplied Oracle software and database setup". You may need to contact your local Oracle DBA for assistance in integrating SA with your pre-existing Oracle database.
- If you are not using a remote Oracle database, the Model Repository component must be installed on the same server as the Oracle database for both First and Secondary Cores.

TLS hardening

During the SA installation, you are allowed to select the minimal version of the TLS protocol that will be used by the core components:

1. TLSv1 (compatible with previous SA versions)
2. TLSv1.1 (default)
3. TLSv1.2

> **Important:**
> In a multimaster mesh, you must set all your cores and satellites to the same TLS level. In case you choose to use the default option, you can harden your cores at a later time. For more information on how to do this, see the SA 10.60 Administration Guide.

FIPS compliance options

HPE Server Automation (SA) complies with the Federal Information Processing Standards publication 140-2, a security standard that enables government entities to procure equipment that uses validated cryptographic modules. During installation you can choose to enable FIPS by setting the `fips.mode` parameter to **enabled**.

You will be prompted during the installation to specify whether FIPS should be enabled or not.

Under normal security conditions, HPE recommends using SHA256 with a key length of 2048. Higher security requirements could require FIPS with a key length of 4096 or other hash functions from SHA-2 family. Note that use of FIPS or other hash functions from SHA-2 family can impact core performance. Contact your Security Administrator for more information.

> **Note:** In FIPS mode, sufficient entropy stemming from the character device /dev/random must be available on the core servers, to ensure proper startup and functionality of SA components.

See FIPS 140-2 compliance.

Cryptographic material options

SA 10.60 and later supports two certificate modes for installing an SA core:

- **self-signed** certificate mode installation
- **third-party** certificate mode installation

In **self-signed** certificate mode, SA uses its own Certificate Authorities (CAs) to automatically sign all the SA Core components certificates.

In **third-party** certificate mode, SA generates Certificate Signing Requests (CSRs) for the SA certificates. You are responsible for managing these CSRs and for providing SA with the certificates issued by your trusted CA. The SA Core installation completes only after SA can pick up the valid certificates from your specified location.

To switch from self-signed to third-party certificate mode, upgrade your SA Core and Agents, then run a Core Recertification job. This will replace all certificates signed by self-signed CAs with certificates signed by third-party CAs.

> - Your selected certificate mode applies to all the SA Cores and Satellites in the SA mesh. This means that you cannot target only specific cores for third-party certification and keep others under SA certification.
> - SA certificates are unique for each Core, Satellite and managed server. SA Core and Satellite components have unique certificates based on the server they are installed on. For example, on a Core with two slices installed on two servers, the slice certificates of the first server are different from the slice certificates of the second server.

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,
> ```
> 16.77.42.65 (oracle_sas, truth_mm_overlay)
> 16.77.41.24 (infrastructure, word_uploads)
> 16.77.43.252 (slice, osprov)
> 16.77.45.21 (satellite)
> ```
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and

> ```
> 16.77.43.252:
> 16.77.42.65 hostname1.example.com hostname1
> 16.77.41.24 hostname2.example.com hostname2
> 16.77.43.252 hostname3.example.com hostname3
> ```
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

Starting with SA 10.60, if you want to use cryptographic material from a previous SA installation (SA 10.0 or earlier), you can no longer simply copy the existing crypto file due to enhancements to the way SA handles encryption.

You can, however, copy the crypto file from an existing SA 10.1 or later SA Core. You can do so by copying the crypto file `/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e` and the `/etc/opt/opsware/crypto/security.conf` file to the same locations on the server that will host the SA Core or First Core (Multimaster Mesh) before beginning the installation. During installation, do not have the installer generate cryptographic material and when you are prompted, provide the password for this cryptographic material.

Mounting the SA installation media

The SA installation/upgrade media is organized into separate categories in the downloaded file structure, for example:

- `oracle_sas` (HPE Server Automation Database)
  The media used to install the Oracle database
- `primary` (HPE Server Automation Product Software)
  The media used to install the SA Core Components
- `upload` (HPE Server Automation Agents and Utilities)
  The media used to upload and install SA Core content and tools
- `sat_base` (HPE Server Automation Satellite Base)
  The media used to install the SA Satellite components, it does not include the OS Provisioning components and is therefore smaller and can be helpful when you are transferring the media over the network.
- `sat_osprov` (HPE Server Automation Satellite Base including OS Provisioning)
  The media used to install the SA Satellite and the Satellite’s OS Provisioning components.

Initial invocation of the hpsa* scripts for core install/upgrade for SA Cores must be from the primary media, Satellites from the sat_base or sat_osprov media.

The SA Installer requires that the media directory structure be maintained, for example:

```
<mountpoint>/<user_defined_prefix>-<media_name>/disk001/opsware_installer/hpsa*.sh
```

where <user_defined_prefix>-<media_name> is, for example, hpsa-primary, hpsa-sat_base, etc. HPE recommends the prefix hpsa and the media category identifiers shown above (sat_base,primary, etc.). *The hyphen after* hpsa *is required even if you do not append a prefix*.

SA is delivered as media that can be copied to a local disk or mounted as an NFS mount point. You must mount all media on a host where install script will be invoked. If media is mounted as follows the SA installer will auto mount it on local or remote core host(s) as needed.

If you use a different directory structure, the SA Installer will prompt you for the path each time it needs to access the media.

Install SA Core with a local SA-supplied database

This section describes installing all SA components and the SA-supplied Oracle database on the same server. This is the simplest and easiest installation method. You can use the right-hand column to indicate that a phase is completed:

Core installation phases

Phase	Complete
"Phase 1: Preparing to install the SA Core"	
"Phase 2: Run the SA installer"	
"Phase 3: Specify the Core components Host/Select installation type"	
"Phase 4: Select the interview type and provide SA parameter values"	
"Phase 5: Installing the SA components"	

Phase 1: Preparing to install the SA Core

1. You will need the *SA Product Software* media, the Agent and Utilities media and the *Oracle_SA* installation media.
2. The server on which the SA components and the Oracle database are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the SA Support and Compatibility Matrix.
3. On the server where you will install SA, mount the following media: *Product Software* (primary), the Agent and Utilities media (upload) and the *Oracle_SA* (oracle_sas), or NFS-mount a directory that contains a copy of the media contents.
   a. Open a terminal window and log in as a user with `root` permissions.
   b. Change to the root directory: `cd /`

> The SA Installer must have *read/write root access* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA installer

On the server on which you plan to install SA and the Oracle database, run the install script:

```
/<distro>/opsware_installer/hpsa_install.sh
```

where `<distro>` is the full path to the Product Software (primary) media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See "Installer logs" on page 64.

Phase 3: Specify the Core components Host/Select installation type

1. The following menu displays:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:
   ```

   `192.168.136.36` (this is the IP address of the host on which the installer is invoked)

   ```
   Please select one of the following options:

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

   Enter the option number or one of the following directives:
   (<c>ontinue, <p>revious, <h>elp, <q>uit)
   ```

   > **Note:** Since this example installation uses the host the installer is invoked on for all Core Components, type `c` and press Enter to continue. You can invoke the installation from a remote machine by selecting `2` to delete the localhost IP address followed by `1` to add the remote host IP address.

2. After the host preparation completes, the following menu displays:

   ```
   Install Type
   ============

   1. Typical Primary Core
   2. Custom Primary Core
   3. Typical Secondary Core
   4. Custom Secondary Core

   Enter the option number or one of the following directives:
   (<p>revious, <h>elp, <q>uit)
   ```

   Enter `1` (Typical Primary Core) and **Enter** to continue.

3. The following menu appears:

   ```
   Oracle Installation
   ===================
   ```

```
1. Install Oracle with SA
2. Use Existing Oracle Database

Enter the option number or one of the following directives:
(<p>revious, <h>elp, <q>uit)
```

Enter `1` (Install Oracle with SA) and press **Enter** to continue.

4. Select the TLS version.

```
Cryptographic Protocol Selection for the Server Automation Components
[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.
=======================================================================
1. TLSv1
2. TLSv1.1
3. TLSv1.2

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[2]:
```

Select 2 (TLSv1.1) and press **Enter** to continue.

5. Select a certificate mode to use in SA and press **Enter** to continue.

```
Select which certificate mode SA will run in.

============================================

1. self-signed

2. 3rd party

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,
>
> ```
> 16.77.42.65 (oracle_sas, truth_mm_overlay)
> 16.77.41.24 (infrastructure, word_uploads)
> 16.77.43.252 (slice, osprov)
> ```

> `16.77.45.21 (satellite)`
>
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
>
> ```
> 16.77.42.65 hostname1.example.com hostname1
> 16.77.41.24 hostname2.example.com hostname2
> 16.77.43.252 hostname3.example.com hostname3
> ```
>
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

Phase 4: Select the interview type and provide SA parameter values

1. The following menu appears:

   ```
   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)
   ```

   Enter `1` (Simple Interview) and **Enter** to continue.

2. You are prompted to supply values for the following SA parameters:
   - `truth.oaPwd`: an SA administrator password (the default username is `admin`). The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.
   - `fips.mode`: This parameter specifies whether to enable FIPS mode for this SA installation.
   - `crypto.hash_algorithm`: The hashing algorithm [SHA1, SHA224, SHA256, SHA384, or SHA512] for SA cryptographic module
   - `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
   - `crypto.legacyCertificateValidity`: the validity period of the temporary self-signed

SA Agent certificate. This parameter is displayed only if you have chosen the **third-party** certification mode and you will use your own CA to sign the certificates. For more information, see Cryptographic material options.

- `bootagent.host`: the host on which to install the OS Provisioning Boot Server component.
- `decrypt_passwd`: A password for the SA cryptographic material. This prompt is displayed only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.
- `truth.dcNm:` A name for your SA facility.
- `windows_util_loc`: The location for the Microsoft Patching utilities.
- `word.store.host`: The IP address of the NFS server for the Software Repository
- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)

For more information about these parameters, see the "SA Core parameter reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter. If the value is acceptable, the next prompt displays:

```
Interview Parameters
====================

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 10 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization: []
```

> The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

```
Parameter 2 of 10 (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n
```

```
Parameter 3 of 10: (crypto.hash_algorithm)
Please enter the hashing algorithm for SA cryptographic module. Press TAB for a
list of possible values. [SHA256]:
```

```
Parameter 4 of 10: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:
```

```
Parameter 5 of 10 (crypto.legacyCertificateValidity)
```

```
Please enter the number of days for which a Legacy Certificate will be valid.
[1]:
```

> - The `crypto.legacyCertificateValidity` parameter is displayed only if you have chosen the **third-party** certification mode to use an external Certificate Authority for signing the SA certificates. For information on the SA certification modes, see Cryptographic material options.
> - Change the current default value of one day to a more relevant period of time.

```
Parameter 6 of 10: (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []
```

```
Parameter 7 of 10 (windows_util_loc)
Please enter the directory path containing the Microsoft patching utilities.
Press Ctrl-I for a list of required files or enter “none” if you do not wish to
upload the utilities at this time (none).: []
```

> These utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering “none”. However, if in the future, you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see Server patching.

```
Parameter 8 of 10 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [192.168.136.39]:
```

```
Parameter 9 of 10 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:
```

```
Parameter 10 of 10 (bootagent.host)
```

```
Please enter the OS Provisioning Boot Server ip or hostname [192.168.136.39]:
```

```
You are asked to re-enter any required passwords for confirmation.
```

> Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in "System requirements for installation ".

When you have supplied values for all parameters, the following message displays:

```
All parameters have values. Do you wish to finish the interview? (y/n):
```

Enter `y` and press **Enter** to continue. If you enter `n`, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press `Ctrl-C`.

3. You can now install the database and SA Components.

Phase 5: Installing the SA components

1. The following screen appears:

```
Install Components
==================

Oracle RDBMS for SA
Model Repository, First Core
Core Infrastructure Components
Slice
OS Provisioning Components
Software Repository - Content (install once per mesh)

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

Enter `c` and press **Enter** to begin the prerequisite checks.

> Before SA begins the installation, it performs a prerequisite check that validates that the host on which you are installing SA meets the minimum requirements (see "SA Installer Prerequisite Checker"). The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

> If your host fails the prerequisite check, the installation can fail or core performance may be negatively affected. If your host fails the prerequisite check or displays warnings, correct the problem(s) or contact HPE Support.

2. The prerequisite check may display messages similar to the following:

   ```
   Prerequisite Checks
   ==============

   Results for <IP_address>:

           WARNING Insufficient swap space (18 GBytes).
                   24 Gbytes is the recommended for Oracle.

           WARNING File system ‘/’ has 29447 MBytes available and 154050 is
                   recommended.

           WARNING Nothing listening at db.host:db.port (ip_address).
                   Note: Can be ignored if core install will be performed
                   using hpsa_install script.

   Enter the option number or one of the following directives:
   (<c>ontinue, <p>revious, <h>elp, <q>uit)
   ```

   The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

   If your server passes the prerequisite check, enter `c` and press **Enter** to begin the installation.

   You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, the Core Description File (CDF) is automatically saved.

3. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:

   a. Configure the `/etc/opt/opsware/crypto/csr.conf` file with the attributes of the **Subject** field and the **Subject Alternative Name** extension of the SA certificates.

      The csr.conf file enables you to configure your CSRs. If you choose not to configure this file, the default values will be used.

> Do not change the **subject@CN** entry as SA will not work with any other value for the **CN** attribute.

```
Certificate Signing Request (CSR) configuration

===============================================

Please review and edit the CSR configuration in
/etc/opt/opsware/crypto/csr.conf on the server that hosts the Model
Repository component [192.168.92.8]. This file defines the attributes of the
Subject field and the Subject Alternative Name extension of the SA
certificates.

You can continue with the install process once this file contains the right
settings for your organization. SA will use the attributes defined in this
file to generate the Subject field of the CSRs that will have to be signed
by your CA.

Enter one of the following directives

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

b. Enter the location where you want the OCT component to generate the *.csr files.

```
Select path where to generate CSRs

=============================

Specify the path on the Model Repository server where SA will generate the
CSR files

[/var/tmp/csrFiles]:

CSRs were generated in the /var/tmp/csrFiles directory on the server that
hosts the Model Repository component [192.168.136.39].

Please have them signed by your CA. You can resume the install process after
all CSRs are signed.

Make sure you copy all certificates in the same directory on the core's
Model Repository server.

You will be prompted for the path to this directory in the next step of the
install process.
```

Submit these files to your CA for signing, and place the issued certificates in a folder of your choice.

After generating the cryptographic material, SA places the CSRs created for that instance in a

subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

c. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Post-installation tasks

Complete the tasks described in "SA Core post-installation tasks"

Install SA Core with a remote customer-supplied Oracle database

This section describes installing all SA components on the same host with an existing remote non-SA-supplied Oracle database.

> **Note:** Because this layout uses a customer supplied database, the remote Oracle database must have been installed and configured as described in "Non-SA-supplied Oracle software and database setup" before you begin the SA Core installation.

> **Note:** Before starting the SA installation process, it is also required to manually install and configure the Oracle Client software on the server that will host the Model Repository SA component. Details with Oracle Client required configurations can be found in the "Non-SA-supplied Oracle software and database setup" section.

You can use the right-hand column to indicate that a phase is completed:

Core installation phases

Phase	Complete
"Phase 1: Prepare to install the SA Core"	
"Phase 2: Run the SA installer"	
"Phase 3: Specify Core components Host/Select installation type"	
"Phase 4: Select the interview type and provide SA parameter values"	
"Phase 5: Install the SA components"	

Phase 1: Prepare to install the SA Core

1. You will need the *SA Product Software* media and the Agent and Utilities media.
2. The server on which the SA Core Components are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system. See the SA Support and Compatibility Matrix.
3. On the server where you will install the SA, mount the following media: *Product Software* (primary) and Agent and Utilities (upload) or NFS-mount a directory that contains a copy of the media: Open a terminal window and log in as a user with `root` privileges.

   Change to the root directory:

   ```
   cd /
   ```

> The SA Installer must have *read/write root access* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Run the SA installer

On the server on which you plan to install SA and the Oracle database, run the install script:

```
/<distro>/opsware_installer/hpsa_install.sh
```

where `<distro>` is the full path to the Product Software (primary) media.

You see messages displayed on screen as the SA Installer loads the required files.

Logs for the installation are automatically stored. See "Installer logs" on page 64.

Phase 3: Specify Core components Host/Select installation type

1. The following menu appears:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:
   ```

   `192.168.136.36` (this is the IP address of the host on which the installer is invoked)

   ```
   Please select one of the following options:

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

   Enter the option number or one of the following directives:
   (<c>ontinue, <p>revious, <h>elp, <q>uit)
   ```

   Since this sample installation uses the host, the installer is invoked for all Core Components. Type `c` and press **Enter** to continue. You can invoke the installation from a remote machine by selecting 2 to delete the localhost IP address followed by 1 to add the remote host IP address.

   When you are satisfied with the entries, press `C` to continue.

   At this point, the SA Installer attempts to set up NFS mounts to the installation media and prepare the server for installation.

2. The following menu appears:

   ```
   Install Type
   ============

   1. Typical Primary Core
   2. Custom Primary Core
   3. Typical Secondary Core
   4. Custom Secondary Core

   Enter the option number or one of the following directives:
   (<p>revious, <h>elp, <q>uit)
   ```

   Enter `1` (Typical Primary Core) and **Enter** to continue.

3. The following menu appears:

   ```
   Oracle Installation
   ===================

   1. Install Oracle with SA
   2. Use Existing Oracle Database

   Enter the option number or one of the following directives:
   (<p>revious, <h>elp, <q>uit)
   ```

   Enter `2` (Use Existing Oracle Database) and press **Enter** to continue.

4. Select the TLS version.

   ```
   Cryptographic Protocol Selection for the Server Automation Components
   [WARNING] Please make sure that all the cores and satellites from the mesh are
   at the same TLS level.
   ========================================================================
   1. TLSv1
   2. TLSv1.1
   3. TLSv1.2

   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit)[2]:
   ```

   Select 2 (TLSv1.1) and press **Enter** to continue.

5. Select a certificate mode to use in SA and press **Enter** to continue.

   ```
   Select which certificate mode SA will run in.

   =============================================

   1. self-signed

   2. 3rd party

   Enter the option number or one of the following directives

   (<p>revious, <h>elp, <q>uit)[1]:
   ```

   > In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
   > Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
   >
   > Example: to install an SA mesh with the following topology,

> `16.77.42.65 (oracle_sas, truth_mm_overlay)`
> `16.77.41.24 (infrastructure, word_uploads)`
> `16.77.43.252 (slice, osprov)`
> `16.77.45.21 (satellite)`
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
> `16.77.42.65 hostname1.example.com hostname1`
> `16.77.41.24 hostname2.example.com hostname2`
> `16.77.43.252 hostname3.example.com hostname3`
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

Phase 4: Select the interview type and provide SA parameter values

1. The following menu appears:

   ```
   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)
   ```

   Enter `1` (Simple Interview) and **Enter** to continue.

2. You are prompted to supply values for the following SA parameters:
   - `truth.oaPwd`: an SA administrator password (the default username is `admin`). The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.
   - `fips.mode`: This parameter specifies whether to enable FIPS mode for this SA installation.
   - `crypto.hash_algorithm`: The hashing algorithm [SHA1, SHA224, SHA256, SHA384, SHA512] for SA cryptographic module.

- crypto.key_length: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
- crypto.legacyCertificateValidity: the validity period of the temporary self-signed SA Agent certificate. This parameter is displayed only if you have chosen the **third-party** certification mode and you will use your own CA to sign the certificates. For more information, see Cryptographic material options.
- bootagent.host: the host on which to install the OS Provisioning Boot Server component.
- decrypt_passwd: A password for the SA cryptographic material.
- truth.dcNm: A name for your SA facility.
- windows_util_loc: The location for the Microsoft Patching utilities.
- db.host: the IP address of the remote database server.
- db.sid: the SID of the Oracle instance containing the Model Repository
- db.port: the port on which the database is listening
- word.store.host: The IP address of the NFS server for the Software Repository.
- word.store.path: The absolute path on the NFS server for Software Repository (/var/opt/opsware/word)

For more information about these parameters, see the "SA Core parameter reference".

You see these prompts (the prompts display one at a time); after you provide a value and press enter, and if the value is acceptable, the next prompt displays:

```
Interview Parameters
====================

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 16: (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization.: []
```

> The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

```
Parameter 2 of 16: (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n
```

```
Parameter 3 of 16: (crypto.hash_algorithm)
Please enter the hashing algorithm for SA cryptographic module. Press TAB for a
list of possible values. [SHA256]:
```

```
Parameter 4 of 16: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:
```

```
Parameter 5 of 16: (crypto.legacyCertificateValidity)

Please enter the number of days for which a Legacy Certificate will be valid.
[1]:
```

> - The `crypto.legacyCertificateValidity` parameter is displayed only if you have chosen the **third-party** certification mode to use an external Certificate Authority for signing the SA certificates. For information on the SA certification modes, see Cryptographic material options.
> - Change the current default value of one day to a more relevant period of time.

```
Parameter 6 of 16: (decrypt_passwd)
Please enter the password for the cryptographic material.: []
```

```
Parameter 7 of 16: (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []
Parameter 8 of 16: (windows_util_loc)
Please enter the directory path containing the Microsoft patching utilities.
Press Ctrl-I for a list of required files or enter “none” if you do not wish to
upload the utilities at this time (none).: []
```

> These utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering “none”. However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the "Server Patching" in the SA 10.60 User Guide.

```
Parameter 9 of 16: (db.host)
Please enter the IP address of the database host: []

Parameter 10 of 16: (truth.servicename)
Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.rose2]:


Parameter 11 of 16: (db.sid)
Please enter the SID of the Oracle instance containing the Model Repository
[truth]:


Parameter 12 of 16: (db.port)
Please enter the port on which the database is listening. [1521]:


Parameter 13 of 16: (db.orahome)
Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0.2/db_2]:


Parameter 14 of 16: (word.store.host)
Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [192.168.136.39]:


Parameter 15 of 16: (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:


Parameter 16 of 16: (bootagent.host)
Please enter the OS Provisioning Boot Server ip or hostname [192.168.136.49]:
```

You are asked to re-enter any required passwords for confirmation.

When you have supplied values for all parameters, the following message displays:

```
All parameters have values.  Do you wish to finish the interview? (y/n):
```

Enter y and press Enter to continue. If you enter n, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3. You can now install the SA Components.

Phase 5: Install the SA components

1. The following screen appears:

```
Install Components
==============
Model Repository, First Core
Core Infrastructure Components
Slice
OS Provisioning Components
Software Repository - Content (install once per mesh)

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

   Enter c and press **Enter** to begin the prerequisite checks.

> Before SA begins the SA component installation, it performs prerequisite checks that the host on which you are installing SA meets the minimum requirements for the installation. The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on. If your host fails the prerequisite check, the installation can fail or core performance may be negatively affected. If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. Correct the problem and retry the installation or, if you are unable to resolve the problem, contact HPE Support.

2. If the prerequisite check completes successfully, you may still see some messages similar to the following:

```
Prerequisite Checks
==============

Results for <IP_address>:
        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

        WARNING File system ‘/’ has 29447 MBytes available and 154050 is
                recommended.

        WARNING Nothing listening at db.host:db.port (ip_address).
                Note: Can be ignored if core install will be performed
                using hpsa_install script.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press **Enter** to begin the installation.

You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

3. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:

   a. Configure the `/etc/opt/opsware/crypto/csr.conf` file with the attributes of the **Subject** field and the **Subject Alternative Name** extension of the SA certificates.

      The csr.conf file enables you to configure your CSRs. If you choose not to configure this file, the default values will be used.

      > Do not change the **subject@CN** entry as SA will not work with any other value for the **CN** attribute.

      ```
      Certificate Signing Request (CSR) configuration

      ===============================================

      Please review and edit the CSR configuration in
      /etc/opt/opsware/crypto/csr.conf on the server that hosts the Model
      ```

```
Repository component [192.168.92.8]. This file defines the attributes of the
Subject field and the Subject Alternative Name extension of the SA
certificates.

You can continue with the install process once this file contains the right
settings for your organization. SA will use the attributes defined in this
file to generate the Subject field of the CSRs that will have to be signed
by your CA.

Enter one of the following directives

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

b. Enter the location where you want the OCT component to generate the *.csr files.

```
Select path where to generate CSRs

=============================

Specify the path on the Model Repository server where SA will generate the
CSR files

[/var/tmp/csrFiles]:

CSRs were generated in the /var/tmp/csrFiles directory on the server that
hosts the Model Repository component [192.168.136.39].

Please have them signed by your CA. You can resume the install process after
all CSRs are signed.

Make sure you copy all certificates in the same directory on the core's
Model Repository server.

You will be prompted for the path to this directory in the next step of the
install process.
```

Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05` `csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

c. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
```

```
====================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Post-installation tasks

You must now complete the tasks described in "SA Core post-installation tasks".

Installing SA Core with a remote customer-supplied database and additional slice component bundles

> **Note:** Because this layout uses a customer supplied database, the remote Oracle database must have been installed and configured as described in "Non-SA-supplied Oracle software and database setup" before you begin the SA Core installation.

> **Note:** Before starting the SA installation process it is also required to manually install and configure the Oracle Client software, on the server that will host the Model Repository SA component. Details with Oracle Client required configurations can be found in the "Non-SA-supplied Oracle software and database setup" section.

This section describes installing all SA components on one host with an existing remote customer-supplied Oracle database that you have installed yourself and additional Slice Component bundle instances. You can use the right-hand column to indicate that a phase is completed:

Core installation phases

Phase	Complete
"Phase 1: Preparing to install SA Core"	
"Phase 2: Running the SA installer"	
"Phase 3: Specifying the Core component hosts"	
"Phase 4: Selecting the installation type"	

Core installation phases, continued

Phase	Complete
"Phase 5: Selecting the interview type and provide SA parameter values"	
"Phase 6: Installing the SA components and the Oracle Database"	

Phase 1: Preparing to install SA Core

1. You will need the *SA Product Software* media and the Agent and Utilities media.
2. The servers on which the SA Core Components are to be installed must be running a supported Red Hat Enterprise Linux or SUSE Enterprise Server Linux operating system.
3. On the server where you will install the SA Core, mount the following media: *Product Software* (primary) and the Agent and Utilities media, or NFS-mount a directory that contains a copy of the media:
   a. Open a terminal window and log in as a user with root privileges.
   b. Change to the root directory:
      ```
      cd /
      ```

> The SA Installer must have *read/write root access* to the directories in which the SA components, including NFS-mounted network appliances are to be installed.

Phase 2: Running the SA installer

On a server on which you plan to install SA components, run the install script:

```
/<distro>/opsware_installer/hpsa_install.sh
```

where `<distro>` is the full path to the *Product Software* (primary) media.

You see messages displayed on screen as the SA Installer loads the required files. Logs for the installation are automatically stored. See "Installer logs".

Phase 3: Specifying the Core component hosts

For this example installation, we'll use four hosts for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

Core component layout

Server	Core Component to be Installed
192.168.136.39	Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.40, 192.168.136.41, 192.168.136.42	Slice
192.168.136.39	SA Provisioning Media Server
192.168.136.39	SA Provisioning Boot Server, Slice version

1. The following screen appears:

   ```
   Specify Hosts to Install
   ========================
   ```

   `192.168.136.39` (this is the IP address of the host on which the installer is invoked)

   ```
   Please select one of the following options:

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

   Enter the option number or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit): 1

   Enter number of hosts to add:
   ```

2. You are asked to specify the number of hosts that will be involved in the installation:

   ```
   Enter number of hosts to add:
   ```

   Enter the appropriate number. For this example, we add three hosts in addition to the default host:

   ```
   Enter number of hosts to add: 3
   ```

3. The following screen appears:

   ```
   Adding Hosts
   ============
   ```

```
Parameter 1 of 3
Hostname/IP []:
```

Enter the hostname or IP address of the first server that will host an SA Core Component(s) and press Enter.

Do the same for all remaining servers. You see this message:

```
All values are entered.  Do you wish to continue? (Y/N) [Y]:
```

Enter Y to continue.

For this example, we add the hosts:

```
192.168.136.40

192.168.136.41

192.168.136.42
```

4. A screen similar to the following appears:

```
Specify Hosts to Install
========================

Currently specified hosts:


        192.168.136.39
        192.168.136.40
        192.168.136.41
        192.168.136.42

Please select one of the following options:

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

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

5. You are asked to provide the OS credentials for each remote host in the list shown in Step 4:

```
Host Passwords
==============

Parameter 1 of 6

192.168.136.40 user [root]:

Parameter 2 of 6

192.168.136.40 password []:*****
```

You are prompted for the credentials for each specified host. After you provide all required credentials, you see the message:

```
All values are entered. Do you wish to continue? (Y/N) [Y]:
```

Enter `Y` to continue.

After you provide all required credentials, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

Phase 4: Selecting the installation type

1. After the SA Installation media is mounted for all servers, the following menu appears:

   ```
   Install Type
   ============
   
   1. Typical Primary Core
   2. Custom Primary Core
   3. Typical Secondary Core
   4. Custom Secondary Core
   
   Enter the option number or one of the following directives:
   (<p>revious, <h>elp, <q>uit)
   ```

   Enter `1` (Typical Primary Core) and **Enter** to continue.

2. The following menu appears:

   ```
   Oracle Installation
   ===================
   
   1. Install Oracle with SA
   2. Use Existing Oracle Database
   
   Enter the option number or one of the following directives:
   (<p>revious, <h>elp, <q>uit)
   ```

   Enter `2` (Use Existing Oracle Database) and **Enter** to continue.

3. The following is displayed:

   ```
   Host/Component Layout
   =====================
   
   1. Model Repository, First Core
   2. Infrastructure and Software Repository Content
   ```

```
3. Slice
4. OS Provisioning Components

Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Note that no host (IP address) is associated with the components.

4. You now must associate the core components with the servers (IP addresses) they are to be installed on. To do so, you enter the component's number at the prompt. For example, enter `1` to add the host for the Oracle database and the Model Repository, enter `2` for the Multimaster Infrastructure Components, and so on.
5. Screens similar to the following display as you assign component hosts:

```
Host Assignment for Model Repository, First Core
===========================================================

1. 192.168.136.39
2. 192.168.136.40
3. 192.168.136.41
4. 192.168.136.42

Enter the number of the host or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
```

Enter `1` to select 192.168.136.39 for the Model Repository. You are returned to the Host Component Layout screen and can select the next component and assign its host. Do the same for all remaining components.

When you have assigned hosts for all components, you see a screen similar to this:

```
Install Components

=====================

1. Model Repository, First Core                :192.168.136.39

2. Multimaster Infrastructure Components:      :192.168.136.39

3. Software Repository Storage and Content     :192.168.136.39

4. Slice                                       :192.168.136.40,

                                                192.168.136.41,

                                                192.168.136.42

5. OS Provisioning Media Server:               :192.168.136.39
```

```
6. OS Provisioning Boot Server, Slice version:  :192.168.136.39


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

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

> The Slice Component bundle (option 4) has multiple host IP addresses listed as the Slice components can have multiple instances to improve performance.

Enter `c` and press **Enter** to continue.

6. Select the TLS version.

```
Cryptographic Protocol Selection for the Server Automation Components
[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.
========================================================================
1. TLSv1
2. TLSv1.1
3. TLSv1.2

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[2]:
```

Select 2 (TLSv1.1) and press **Enter** to continue.

7. Select a certificate mode to use in SA and press **Enter** to continue.

```
Select which certificate mode SA will run in.

=============================================

1. self-signed

2. 3rd party

Enter the option number or one of the following directives

(<p>revious, <h>elp, <q>uit)[1]:
```

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,

> `16.77.42.65 (oracle_sas, truth_mm_overlay)`
> `16.77.41.24 (infrastructure, word_uploads)`
> `16.77.43.252 (slice, osprov)`
> `16.77.45.21 (satellite)`
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
> `16.77.42.65 hostname1.example.com hostname1`
> `16.77.41.24 hostname2.example.com hostname2`
> `16.77.43.252 hostname3.example.com hostname3`
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

Phase 5: Selecting the interview type and provide SA parameter values

1. The following menu appears:

   ```
   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)
   ```

   Enter `1` (Simple Interview) and **Enter** to continue.

2. You are prompted to supply values for the following SA parameters:
   - `truth.oaPwd`: an SA administrator password (the default username is `admin`). The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.
   - `fips.mode`: This parameter specifies whether to enable FIPS mode for this SA installation.
   - `crypto.hash_algorithm`: The hashing algorithm [SHA1, SHA224, SHA256, SHA384, SHA512] for SA cryptographic module.

- `crypto.key_length`: the key length [2048 or 4096] used for hashing algorithm of SA cryptographic module.
- `crypto.legacyCertificateValidity`: the validity period of the temporary self-signed SA Agent certificate. This parameter is displayed only if you have chosen the **third-party** certification mode and you will use your own CA to sign the certificates. For more information, see Cryptographic material options.
- `bootagent.host`: the host on which to install the OS Provisioning Boot Server component.
- `decrypt_passwd`: A password for the SA cryptographic material. You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.
- `truth.dcNm:` A name for your SA facility.
- `windows_util_loc`: The location for the Microsoft Patching utilities.
- `word.store.host`: The IP address of the NFS server for the Software Repository.
- `word.store.path`: The absolute path on the NFS server for Software Repository (`/var/opt/opsware/word`)
- `db.host:` the IP address of the database server.
- `db.sid`: the SID of the Oracle instance containing the Model Repository
- `db.port`: the port on which the database is listening

For more information about these parameters, see the "SA Core parameter reference".

You see these prompts (the prompts display one at a time; after you provide a value and press enter you see a message, `Validating...`, and if the value is acceptable, the next prompt displays:

```
Interview Parameters
====================

Navigation Keys:
Use <Ctrl>P to go to the previous parameter.
Use <Ctrl>N to go to the next parameter.
Use >Tab> to view help on the current parameter.
Use <Ctrl>C to interrupt the interview.

Parameter 1 of 16: (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
```

```
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization.: []
```

> The password you specify here will be used as the default password for all SA features that require a password until you explicitly change the defaults.

```
Parameter 2 of 16: (fips.mode)
Do you want SA to be in FIPS mode? (y/n) [n]: n
```

```
Parameter 3 of 16: (crypto.hash_algorithm)
Please enter the hashing algorithm for SA cryptographic module. Press TAB for a
list of possible values. [SHA1]:
```

```
Parameter 4 of 16: (crypto.key_length)
Please enter the key length [2048 or 4096] used for hashing algorithm of SA
cryptographic module. [2048]:
```

```
Parameter 5 of 16 (crypto.legacyCertificateValidity)
```

```
Please enter the number of days for which a Legacy Certificate will be valid.
[1]:
```

> - The `crypto.legacyCertificateValidity` parameter is displayed only if you have chosen the **third-party** certification mode to use an external Certificate Authority for signing the SA certificates. For information on the SA certification modes, see Cryptographic material options.
> - Change the current default value of one day to a more relevant period of time.

```
Parameter 6 of 16: (decrypt_passwd)
Please enter the password for the cryptographic material.: []
```

> You will see this prompt only if you are using your own crypto file and not allowing SA to automatically generate the crypto file.

```
Parameter 7 of 16: (truth.dcNm)
Please enter the short name of the facility where the Opsware Installer is
being run (no spaces).: []
```

```
Parameter 8 of 16: (windows_util_loc)
Please enter the directory path containing the Microsoft patching utilities.
Press Ctrl-I for a list of required files or enter “none” if you do not wish to
upload the utilities at this time (none).: []
```

> - These utilities are required if you plan to use SA to install Windows operating system patches/hotfixes and/or to manage Windows-based servers with SA. If you do not intend to use SA for these tasks, you can bypass the upload of these files by entering “none”. However, if in future you decide to use SA for Windows patching or to manage Windows servers, you will be required to install these files from the SA Client. For information about uploading these files from the SA Client, see the " Server Patching" in the SA 10.60 User Guide.
> - Uploading the Microsoft patching utilities is optional, however, if you expect to have Windows-based managed servers, you should follow the instructions for obtaining these files as described in "System requirements for installation ".

```
Parameter 9 of 16: (db.host)
Please enter the IP address of the database server: []

Parameter 10 of 16: (truth.servicename)
Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.rose2]:

Parameter 11 of 16:(db.sid)
Please enter the SID of the Oracle instance containing the Model Repository
[truth]:

Parameter 12 of 16: (db.port)
Please enter the port on which the database is listening. [1521]:

Parameter 13 of 16: (db.orahome)
Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0/db_1]:
/u01/app/oracle/product/12.1.0/client_1/

Parameter 14 of 16: (word.store.host)
Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [192.168.136.39]:

Parameter 15 of 16: (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:

Parameter 16 of 16: (bootagent.host)
Please enter the OS Provisioning Boot Server ip or hostname [192.168.136.39]:
```

You are asked to re-enter any required passwords for confirmation.

When you have supplied values for all parameters, the following message displays:

```
All parameters have values. Do you wish to finish the interview? (y/n):
```

Enter `y` and press **Enter** to continue. If you enter `n`, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

3. You are now ready to begin the SA Component installation.

Phase 6: Installing the SA components and the Oracle Database

1. A screen similar to the following appears:

```
Install components

==================

Model Repository, First Core : 192.168.136.39
Multimaster Infrastructure Components : 192.168.136.39
Software Repository Storage : 192.168.136.39
Slice : 192.168.136.40, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server : 192.168.136.39
OS Provisioning Boot Server, Slice version : 192.168.136.39
Software Repository - Content (install once per mesh): 192.168.136.39

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Enter c and press Enter to begin the prerequisite checks.

> If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:
>
> ```
> Slice Network Interface Configuration
> =====================================
>
> Parameter 1 of 2 (Slice: 192.168.136.38)
> ```

> ```
> Please select the interface to use for 192.168.136.38
>
> 1) eth2 -- 192.168.136.55
> 2) eth1 -- 192.168.136.77
> 3) eth0 -- 192.168.136.38 (default)
>  [3]:
>
> Parameter 2 of 2 (Slice: 192.168.136.41)
>
> Please select the interface to use for 192.168.136.41
>
> 1) eth0 -- 192.168.136.41 (default)
> 2) eth2 -- 192.168.136.54
> 3) eth1 -- 192.168.136.76
>  [1]:
> ```
>
> Select the appropriate network interface for each host by entering the associated number from the list.
>
> When you have configured all interfaces, you see the message:
>
> ```
> All values are entered. Do you wish to continue? (Y/N) [Y]:
> ```
>
> Enter `y` and press Enter to continue. You can edit the list again by pressing `n` and Enter.

2. The prerequisite check begins.

> Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see "SA Installer Prerequisite Checker"). The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.
>
> If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, the installation can fail or core performance may be negatively affected. Correct the problem and retry the installation or, if you are unable to resolve the problem, contact HPE Support.

3. If the prerequisite check completes successfully, you may still see some messages similar to the following:

```
Prerequisite Checks
==============
Results for <IP_address>:
        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.
        WARNING File system ‘/’ has 29447 MBytes available and 154050 is
                recommended.
        WARNING Nothing listening at db.host:db.port (ip_address).
                Note: Can be ignored if core install will be performed
                using hpsa_install script.
Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter to begin the installation.

4. You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, you the Core Description File (CDF) is automatically saved.

5. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:
   a. Configure the `/etc/opt/opsware/crypto/csr.conf` file with the attributes of the **Subject** field and the **Subject Alternative Name** extension of the SA certificates.

      The csr.conf file enables you to configure your CSRs. If you choose not to configure this file, the default values will be used.

      > Do not change the **subject@CN** entry as SA will not work with any other value for the **CN** attribute.

      ```
      Certificate Signing Request (CSR) configuration
      ```

```
===============================================

Please review and edit the CSR configuration in
/etc/opt/opsware/crypto/csr.conf on the server that hosts the Model
Repository component [192.168.92.8]. This file defines the attributes of the
Subject field and the Subject Alternative Name extension of the SA
certificates.

You can continue with the install process once this file contains the right
settings for your organization. SA will use the attributes defined in this
file to generate the Subject field of the CSRs that will have to be signed
by your CA.

Enter one of the following directives

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

b. Enter the location where you want the OCT component to generate the *.csr files.

```
Select path where to generate CSRs

=============================

Specify the path on the Model Repository server where SA will generate the
CSR files

[/var/tmp/csrFiles]:

CSRs were generated in the /var/tmp/csrFiles directory on the server that
hosts the Model Repository component [192.168.136.39].

Please have them signed by your CA. You can resume the install process after
all CSRs are signed.

Make sure you copy all certificates in the same directory on the core's
Model Repository server.

You will be prompted for the path to this directory in the next step of the
install process.
```

Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05` `csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.

When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

c. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
===================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Post-installation tasks

You must now complete the tasks described in "SA Core post-installation tasks".

Installing additional slice component bundles

You can install additional Slice Component bundles on an existing SA Core in order to improve the scalability. To install an addition Slice Component bundle to an installed SA core, perform the following tasks.

> **Note:** When adding a new Slice Component bundle to an existing core, SA services are restarted on all servers that are part of the core.

1. On any core server in the SA Core in which you plan to install the additional Slice Component bundle, run the install script, specifying the Core Description File (CDF) you generated when you installed the core by using the `-c` argument and the full path to the file:

   ```
   /<distro>/opsware_installer/hpsa_install.sh -c /usr/tmp/hpsa_cdf.xml
   ```

   where `<distro>` is the full path to the *Product Software* (primary) media. You see messages displayed on screen as the SA Installer loads the required files.

   Logs for the installation are automatically stored. See "Installer logs".

2. You see a screen similar to the following:

   ```
   Specify Hosts to Install
   ```

```
========================

Currently specified hosts:

       192.168.136.36 (oracle_sas)
       192.168.136.38 (slice)
       192.168.136.39 (infrastructure)
       192.168.136.40 (osprov)

Please select one of the following options:

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

Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): 1
Enter number of hosts to add (or enter "0" to edit the list): 1
```

Enter `1` to add the IP address of the server that will host the additional Slice Component bundle.

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,
> `16.77.42.65 (oracle_sas, truth_mm_overlay)`
> `16.77.41.24 (infrastructure, word_uploads)`
> `16.77.43.252 (slice, osprov)`
> `16.77.45.21 (satellite)`
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
> `16.77.42.65 hostname1.example.com hostname1`
> `16.77.41.24 hostname2.example.com hostname2`

> `16.77.43.252 hostname3.example.com hostname3`
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

For example:

```
Adding hosts
============

Parameter 5 of 5
Hostname / IP []: 192.168.136.43

All values are entered. Do you wish to continue? (Y/N) [Y]: Y
```

3. After you have specified the host server's IP address, the Specify Hosts to Install screen looks similar to this:

```
Specify Hosts to Install
========================

Currently specified hosts:

       192.168.136.36 (oracle_sas)
       192.168.136.38 (slice)
       192.168.136.39 (infrastructure)
       192.168.136.40 (osprov)
       192.168.136.43

Please select one of the following options:

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

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

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

Note that the last IP address in the list is the IP address you just entered however, no component is assigned to that IP address for installation.

To assign the Slice Component bundle to the IP address you just specified, enter `c` and press Enter to continue.

You are prompted to provide the host password for each host in the list.

The installer validates each password, then you see messages displayed as the installer prepares the server for installation.

4. When the set up completes, you see a screen similar to the following:

```
Install Type

============


1. Typical Primary Core


Enter the option number or one of the following directives

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

Accept the default.

> The Install Type is stored in the Core Definition File (CDF) when you install the SA First Core and is the default for subsequent installations and upgrades. You cannot use a Typical Installation type for the SA Core and a Custom Installation type for subsequent installations. Both installs must be of the same Installation type.

5. You see a screen similar to the following:

```
Host/Component Layout

=====================


Installed Components


Oracle RDBMS for SAS                                 : 192.168.136.36

Model Repository, First Core                         : 192.168.136.36

Core Infrastructure Components                       : 192.168.136.39
```

```
Slice                                             : 192.168.136.38

OS Provisioning Components                        : 192.168.136.40

Software Repository - Content (install once per mesh): 192.168.136.39


------------------------------------------


Select a component to assign


1. Slice


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

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

In this case, since all other components have already been installed and only the Slice Component bundle can have multiple instances, only the Slice option is displayed. Select `1` and press Enter.

6. You see a screen similar to the following:

```
Host Assignment for Slice

=========================


1 ( ) 192.168.136.36

2 ( ) 192.168.136.39

3 ( ) 192.168.136.40

4 ( ) 192.168.136.43


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

(<c>ontinue, <a>ll, <u>nselect all, <p>revious, <h>elp, <q>uit): 4
```

Enter the line number associated with the IP address you specified above. An asterisk appears next to your selection.

```
Host Assignment for Slice

=========================
1 ( ) 192.168.136.36

2 ( ) 192.168.136.39

3 ( ) 192.168.136.40

4 (*) 192.168.136.43


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

(<c>ontinue, <a>ll, <u>nselect all, <p>revious, <h>elp, <q>uit): c
```

Enter `c` then press Enter to continue.

7. You see a screen similar to the following:

```
Host/Component Layout

=====================


Installed Components


Oracle RDBMS for SAS                                 : 192.168.136.36

Model Repository, First Core                         : 192.168.136.36

Core Infrastructure Components                       : 192.168.136.39

Slice                                                : 192.168.136.38

OS Provisioning Components                           : 192.168.136.40

Software Repository - Content (install once per mesh): 192.168.136.39


------------------------------------------


Select a component to assign


1. Slice [192.168.136.43]


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

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

Enter c then press Enter to continue.

8. ⚠ Select the same TLS version as on the primary core and press **Enter** to continue.

```
Cryptographic Protocol Selection for the Server Automation Components

[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.
======================================================================
1. TLSv1
2. TLSv1.1
3. TLSv1.2

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[3]:
```

9. You see a screen similar to the following where you can modify installation parameters if necessary:

```
Interview Parameters
====================


Navigation keys:
Use <ctrl>p to go to the previous parameter.
Use <ctrl>n to go the next parameter.
Use <tab> to view help on the current parameter.
Use <ctrl>c to abort the interview.


All prompts have values.  What would you like to do:


1. Re-enter values
2. Continue


Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Enter c then press **Enter** to continue.

After a prerequisite check, the Slice Component bundle is installed on the host you specified. You see some messages displayed as the installation proceeds and a completion message when the installation is finished.

10. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:
    a. Enter the location where you want the OCT component to generate the *.csr files.

    ```
    Select path where to generate CSRs

    =============================

    Specify the path on the Model Repository server where SA will generate the
    CSR files

    [/var/tmp/csrFiles]:

    CSRs were generated in the /var/tmp/csrFiles directory on the server that
    hosts the Model Repository component [192.168.136.39].

    Please have them signed by your CA. You can resume the install process after
    all CSRs are signed.

    Make sure you copy all certificates in the same directory on the core's
    Model Repository server.

    You will be prompted for the path to this directory in the next step of the
    install process.
    ```

    Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
    After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
    When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

    b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

    ```
    Enter the path to the directory containing the custom certificates.
    ===================================================================
    ```

```
Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Install SA first (primary) core with a secondary Core (multimaster mesh)

This section provides an installation summary for a Single Host SA First (Primary) Core with a secondary Core (Multimaster Mesh). The cores in a mesh can be installed with any of the configurations described in the samples above.

Phase 1: Installing the SA first (primary) Core

Decide the configuration you will use and follow the instructions described in the configuration samples.

After the first (primary) Core installation is complete, you can install secondary Cores for your Multimaster Mesh.

Overview of the secondary Core installation process

The following are the typical phases of installing a secondary Core:

1. *Prepare for Installation*: Ensure that all installation prerequisites have been met, that you have the information needed to complete the Installer interview, that you have all necessary permissions to complete the installation, and that you have the SA installation media. For more information, see "System requirements for installation "

2. On the first core infrastructure host, define a new facility and export first Core Model Repository content: During this phase you define the facility in which the new secondary Core is to be installed, export the First Core's Model Repository content, and copy the resulting export files to the new secondary Core host.

> When adding a new facility to an existing core that was previously patched, the new core will have the core’s base version installed (not the patch version, for example 10.0, not 10.0x or 10.10, not 10.1x). After the secondary Core is created, you must apply the desired patch.

3. On the server that will host the new secondary Core, install the Oracle database and install the secondary Core Components: During this phase you can install the SA-supplied Oracle database for the secondary Core(s) Model Repository. This database is automatically configured to work with the SA Model Repository. See "Oracle setup for the Model Repository" *f*or information about the SA Oracle database configuration differs from a default Oracle configuration.
   Alternatively, you can install a database using the Oracle Universal Installer or use an existing Oracle 12c database installation (Oracle 10 and 9*i* are not supported) and select to use an existing database during installation. However, there are database configuration requirements that must be met in order for such databases to be compatible with the SA Model Repository.

   See "Oracle setup for the Model Repository".

   You will also install the secondary Core's components and import the Model Repository content that was exported from the First Core into the database.

4. *Post Installation Tasks*: During this phase you must perform various post-installation tasks to complete the configuration of the new secondary Core.

> Before proceeding with the installation, confirm that you have addressed the issues in "Phase 2: Prepare to add the secondary Core".

Phase 2: Prepare to add the secondary Core

This section describes adding secondary Cores that, with an existing first Core, create a Multimaster Mesh of SA Cores that can coordinate server management. The cores in a mesh can be installed with the same configurations as the primary cores. See the sample configurations described in the section above.

> If you will be defining and installing multiple Facilities and secondary Cores, you must install only one secondary Core at a time. In other words, you must define each secondary Core’s Facility then completely install its core components and content before defining another Facility and installing another secondary Core. Simultaneous definition/installation of Facilities/cores is not supported.

To prepare to add a secondary Core, perform the following tasks:

1. Locate the *SA Product Software* (primary) and, if you will install the SA-supplied Oracle database used by the SA Model Repository, the *Oracle_SA* media.
2. On the First Core’s Infrastructure Component server and on the server that will host the new secondary Cores Model Repository, mount the SA*Product Software* (primary) and *Oracle_SA* media or NFS-mount the directory that contains a copy of the media.

Prepare the environment

1. Ensure that the following folders have enough free space for the database export:
   - Database server path - `<DATA_PUMP_DIR>`
   - Database server path - `/var/tmp`
   - Model Repository server path - `/var/tmp`
   - Model Repository server path specified by installer parameter - `<truth.dest>`

   To estimate the export size, run the following command:

   ```
   <install_media>-primary/disk001/opsware_installer/tools/calculate_export_
   size.sh <ORACLE_HOME> <sid> <oracle_admin_password> <service_name>
   ```

   You can find the values for the required parameters in the CDF file of the primary core.

   Example: calculate_export_size.sh /u01/app/oracle/product/12.1.0/db_1 truth password truth.PrimaryCore
2. Before starting the primary database export, ensure that the COMPATIBLE parameters in the primary and secondary database `init.ora` file are set correctly. SA recommends setting the COMPATIBLE parameter to the Oracle RDBMS software version. Refer to the Oracle documentation for information on how the COMPATIBLE parameter affects the Data Pump Export-Import process.
3. The Oracle Data Pump Export-Import process also depends on the Oracle Client version (`expdp` and `impdp`). For remote database installations, SA strongly recommends the Oracle Full Client be the same version as the Oracle RDBMS software. Refer to the Oracle documentation for information about how the Oracle Client version affects the Data Pump Export-Import process.

> The Installer must have *read/write root* access to the directories where it installs SA components, even on NFS-mounted network appliances.

Phase 3: Export first core files to a TAR.GZ file and copy to the new secondary Core host

In this phase, you export First Core files (CDF, cryptographic material) into a TAR.GZ file that must be copied to the new secondary Core.

1. On the First Core host, create a directory in which the TAR.GZ file will be saved. You can specify a custom location or accept the default:

   ```
   /var/opt/opsware/truth
   ```

   ```
   cd /
   ```

2. On the server that hosts the First Core's *Infrastructure Component* host, invoke the Add Datacenter to Mesh script (hpsa_add_dc_to_mesh.sh).
   Specify the full path to the Facility definition script.

   For example:

   ```
   /<distro>/opsware_installer/hpsa_add_dc_to_mesh.sh
   ```

   where `<distro>` is the full path to the *Product Software* (primary) media.

   A screen similar to the following appears:

   ```
   ---------------------------------------

   add_dc_to_mesh will be performed on the following identified core host(s). If
   there is any inconsistency then try again with the correct CDF.


   16.77.42.65  (oracle_sas, truth_mm_overlay)

   16.77.41.24  (infrastructure, word_uploads)

   16.77.43.252  (slice, osprov)


   ---------------------------------------

   Do you want to continue (Y/N) [Y]:
   ```

   Type `Y` and press **Enter** to continue.

3. Provide the OS credentials for each host in the list shown below:

   ```
   Host Passwords
   ==============

   Parameter 1 of 2

   <ip_address> user [root]:

   Parameter 2 of 2

   <ip_address> password []:******
   ```

   You are prompted for the credentials for each specified host. SA validates each credential. After you provide all required credentials, you see the following message:

   ```
   All values are entered. Do you wish to continue? (Y/N) [Y]:
   ```

   Enter `Y` to continue.

   After you provide all required credentials, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

   > For the next step, the secondary Core will use the FIPS compliance settings you specified during the installation of the Primary Core. You will not be prompted for FIPS enablement during the secondary Core installation.

4. Select the type of Oracle installation for the secondary Core.

   ```
   secondary Core Oracle installation
   ==================================

   1. Install Oracle with SA
   2. Use existing Oracle database
   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit): 2
   ```

   > **Note:** If you chose to use an existing Oracle database (remote customer-supplied database) for the secondary Core install, ensure that the secondary Core’s Oracle database has already been installed and configured before running the add_dc_to_mesh process. The remote Oracle database must have been configured as described in "Non-SA-supplied Oracle software and database setup".

5. Provide values for the following Interview parameters:

   > **Note:** You must provide the value of **newCore.dcDispNm** parameter within double quotes.

   ```
   Interview Parameters
   ```

```
====================

Navigation keys:

Use <ctrl>p to go to the previous parameter.

Use <ctrl>n to go the next parameter.

Use <tab> to view help on the current parameter.

Use <ctrl>c to abort the interview.

Parameter 1 of 11 (truth.dest)

Please enter the full path to the directory where the export file will be saved
[/var/opt/opsware/truth/]:

Parameter 2 of 11 (newCore.dcNm)

Please enter the short name of the new facility you would like to define (no
spaces) []: SLAVE

Parameter 3 of 11 (newCore.dcDispNm)

Please enter the long name for the facility that you are adding to the mesh.
[SLAVE]:

Parameter 4 of 11 (newCore.dbHost)

Please enter the hostname/IPaddress of the server where you are planning to
install the Oracle database in the new facility. []: 16.77.1.191

Parameter 5 of 11 (newCore.dbPort)

Please enter the port on which the database is listening for the new facility
[1521]:

Parameter 6 of 11 (newCore.dbSid)

Please enter the SID of the Oracle instance containing the Model Repository for
the new facility [truth]:
```

> Parameters 5 and 6 are only displayed if you chose to use an existing (non-

> SA supplied) Oracle database for the secondary Core.

```
Parameter 7 of 11 (newCore.mgwIP)

Please enter the IP address of the server where you are planning to install the
Infrastructure component in the new facility (or where the management gateway
will be installed). []: 16.77.1.192


Parameter 8 of 11 (newCore.dcSubDom)

Please enter the subdomain for the facility you are about to create (lowercase,
no spaces) [slave.com]:


Parameter 9 of 11 (newCore.servicename)

Please enter the tnsname of the Model Repository instance that you will be
installing in the new facility [truth.SLAVE]:


Parameter 10 of 11 (db.port)

Please enter the port on which the database is listening. [1521]: 1521


Parameter 11 of 11 (db.orahome)

Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0/client_1]:
```

> Parameters 10 and 11 refer to the port and `ORACLE_HOME` directory for the Primary Core Model Repository.

You are asked to re-enter any required passwords for confirmation.

After you have entered or accepted all required values, you see this prompt:

```
All values are entered. Do you wish to continue? (Y/N) [Y]:

End of interview.
```

Type `Y` to continue. If you need to re-enter a value, type `N`.

6. Specify the way in which the file transfer between the cores will be done:

   ```
   File transfer mode
   ```

```
==============================================================

Do you want to manually transfer files from the primary to the secondary Core?
[N]:
```

For **manual file transfer**, manually copy all necessary files from the primary core to the secondary Core servers once the add_dc_to_mesh process is complete. With an **auto file transfer**, all files will be transferred automatically between cores.

If you choose to manually transfer files, a message containing instructions on how to perform this will be printed. After the add_dc_to_mesh process is complete, you can still find this message in the log files. The instructions will be similar to the following:

```
When running the manual add_dc process, you will need to manually copy the
files necessary for the secondary Core install from the primary core servers to
the secondary Core servers.
The list of files that need to be copied is:
1.Truth files
 Truth files need to be copied from the primary core’s truth server on the
server on which the secondary Core install will run.
 These files are:
        - truth.SLAVE.tar.gz
        - cdf.SLAVE.xml
 They can be found on the primary core’s truth in the /var/opt/opsware/truth/
directory.

2.Database export
 The db export files (*.dmp) need to be copied from the primary core’s database
server on the secondary Core’s database server.
 If you choose to install the secondary DB server with SA, you will need to
copy these *.dmp files in a temporary directory on the server, eg.
/var/tmp/dbExport.
 If you will use an existing Oracle server for the secondary Core, you will
need to copy these files in the datapump directory.
 To determine the datapump directory path, run the following query on the
secondary Core’s Oracle server:
        select DIRECTORY_PATH from dba_directories where DIRECTORY_NAME=’DATA_
PUMP_DIR’;
```

> **Note:** If you choose to automatically transfer files, you will need to supply the credentials for the secondary Core’s Oracle server and Infrastructure server in the next steps. If, for some reasons, the add_dc_to_mesh process fails after exporting the Model Repository, you will need to manually copy the files specified above on the secondary Core servers and restart the primary core’s services if necessary.

7. The following prompts (up until prompt 12) will be displayed only if you have selected the

automatic file transfer mode:

```
Primary core database is on <dbserver_ip_address>. Credentials are needed.
===============================================================

Parameter 1 of 2
<dbserver_ip_address> username [root]:

Parameter 2 of 2
<dbserver_ip_address> password []:****
Re-enter the password to confirm:
```

Supply the OS credentials for the primary core’s database server if you are using a remote database. Re-enter the password for confirmation.

8. Specify the OS credentials for the secondary Core’s database server.

   ```
   secondary Core database is on 16.77.1.191. Credentials are needed.
   ======================================================================

   Parameter 1 of 2
   16.77.1.191 user []: root

   Parameter 2 of 2
   16.77.1.191 password []: *******

   All values are entered.  Do you wish to continue? (Y/N) [Y]:
   ```

9. Provide the path on the secondary Core’s Oracle server where you want the DB export to be copied to.

   ```
   Specify the path on the secondary Core's oracle server where to copy the DB
   export
   =====================================================================
   Specify the path on the secondary Core's oracle server where to copy the DB
   export [/var/tmp/dbDump]:
   ```

   If you choose to **install the secondary DB server with SA**, copy these *.dmp files in a temporary directory on the server, example, `/var/tmp/dbDump`.

   If you will **use an existing Oracle server for the secondary Core**, copy these files in the datapump directory. To determine the datapump directory path, run the following query on the secondary Core's Oracle server:

   ```
   "select DIRECTORY_PATH from dba_directories where, DIRECTORY_NAME='DATA_PUMP_
   DIR';"
   ```

10. Provide the OS credentials for the secondary Core’s Infrastructure server

```
Secondary Management Gateway Server is on 16.77.1.192. Credentials are needed.
=====================================================================
Parameter 1 of 2
16.77.1.192 user []: root

Parameter 2 of 2
16.77.1.192 password []: *******

All values are entered.  Do you wish to continue? (Y/N) [Y]: Y
```

If you entered the same IP/hostname for both the secondary Oracle and Infrastructure servers, this step (10) will be skipped.

11. Specify the path on the secondary Core’s Infrastructure server where the installer will copy the First Core files (the tar.gz archive).

    ```
    Specify the path on the secondary Core's Management Gateway Server where to
    copy the truth files
    =====================================================================
    Specify the path on the secondary Core's Management Gateway Server where to
    copy the truth files [/var/tmp/truthFiles]:
    ```

    These files need to be copied on the server on which the secondary Core install will run. If you do not want to run the secondary Core install on the Infrastructure server, you will then need to manually copy these on the server on which you want to run the installer after the add_dc_to_mesh process finishes.

12. The following screen is displayed:

    ```
    Ready to perform add DC to mesh
    ===============================

    Actions that will be performed:
    -------------------------
      Define New Facility, Update Gateway Config
      Export Model Repository (truth)

    Enter one of the following directives
    (<c>ontinue, <p>revious, <h>elp, <q>uit):
    ```

    Type **c** to continue or press **Enter** to continue.

    A number of informational messages are displayed as the process continues.

    ```
    [INFO] ******************************************************************

    [INFO] Database export files *.dmp and *.log will be available on database
    server
    ```

```
[INFO] under directory: /u01/app/oracle/admin/truth/dpdump/

[INFO] File source_db_charset.txt is now available on this server in: [INFO]
/var/opt/opsware/truth/
[INFO] The Database export *.dmp files

[INFO] (truth*_exp.dmp, aaa*_exp.dmp, gcadmin*_exp.dmp, lcrep*_exp.dmp,lcrep_
tables*_exp.dmp)
[INFO] and *.log files are now available on the Primary database server. [INFO]
*******************************************************************
```

After completion, the script places a `truth.SLAVE.tar.gz` file in the `/var/opt/opsware/truth` the directory (or the custom location you specified for the export file path (`truth.dest`)). If you chose to manually copy this `TAR.GZ` file, you will need to copy it on the server on which you plan to run the secondary Core install. Otherwise, the installer copies it automatically on the secondary Core's Infrastructure server, in the path that you provided during the interview.

13. Continue to Phase 4.

Phase 4: Prepare the files necessary for the secondary Core installation

If you choose to **manually transfer** files in the interview from the previous phase, you must copy the `First Core Files tar.gz` archive and the secondary Core's CDF file from the primary core's Model Repository server on the server on which you will run the secondary Core installation. You will use this CDF file during the secondary Core install.

You must also copy the database export files (*.dmp files) from the primary core's database server (these files can be found in the datapump directory) to the secondary Core's Oracle database server. If you choose to install the secondary database server with SA, you will need to copy these `*.dmp` files in a temporary directory on the server. For example: `/var/tmp/dbExport`.

If you are using an existing Oracle server for the secondary Core, you must copy these files in the datapump directory. To determine the datapump directory path, run the following query on the secondary Core's Oracle server:

```
"select DIRECTORY_PATH from dba_directories where DIRECTORY_NAME='DATA_PUMP_DIR';".
```

If you choose to **automatically transfer** files in the interview from the previous phase, the installer copies the files in the appropriate locations. For the `First Core Files tar.gz` archive, this location is on the secondary Core's Management Gateway server. If you do not plan on running the secondary

Core install from the secondary Core's Management Gateway server, you will have to manually copy the `TAR.GZ` file on the server on which the installer will run.

The steps in "Samples of secondary Core installations (Phase 5)" below assume you have already mounted the SA primary distribution for the secondary Core.

Samples of secondary Core installations (Phase 5)

This section describes the following samples of secondary Core installations that can be performed in Phase 5:

- "Phase 5a: Install all secondary Core components on a single host"
  All secondary Core Components and SA-supplied Oracle database on the same host
- "Phase 5b: Install all secondary Core Components on a single host, remote Non-SA-supplied Oracle database"
  All secondary Core Components installed on a single host, remote Non-SA-supplied Oracle database on a separate host
- "Phase 5c: Install the secondary Core components on multiple hosts, remote non SA-supplied database on remote database server"
  secondary Core Components distributed to different hosts, non-SA-supplied database on a remote database host

Phase 5a: Install all secondary Core components on a single host

This section describes installing all SA Core Components and the SA-supplied Oracle database on a single host. If you plan to install components on different hosts, see "Phase 5b: Install all secondary Core Components on a single host, remote Non-SA-supplied Oracle database".

During this phase, the First Core Model Repository content exported during Step 4 is imported into the secondary Core's Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA secondary Core Components installed.

> If you plan to use a remote Oracle database, there are specific configuration tasks you must perform on the database before installing the secondary Core. See Appendix A: Oracle Setup for the Model Repository and the installation procedure described in "Phase 5c: Install the secondary

Core components on multiple hosts, remote non SA-supplied database on remote database server".

1. Invoke the SA Installer and specify (`-c` argument) the CDF copied in Phase 4:

   ```
   <distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml
   ```

   where `<distro>` is the full path to the *Product Software* (primary) media.

2. Press `c` to continue for the following informational messages displayed:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:

   <newCore4_IP_Address>

   Please select one of the following options:
   1. Add/edit host(s)
   2. Delete host(s)

   Enter the option number or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit):c.
   ```

   > In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
   > Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
   >
   > Example: to install an SA mesh with the following topology,
   > `16.77.42.65 (oracle_sas, truth_mm_overlay)`
   > `16.77.41.24 (infrastructure, word_uploads)`
   > `16.77.43.252 (slice, osprov)`
   > `16.77.45.21 (satellite)`
   > add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
   > `16.77.42.65 hostname1.example.com hostname1`
   > `16.77.41.24 hostname2.example.com hostname2`
   > `16.77.43.252 hostname3.example.com hostname3`
   > The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

3. Enter the credentials for the new secondary Core host and press **Enter** for the following message displayed:

   ```
   Host Passwords

   ==============

   Parameter 1 of 2
   <newCore4_IP_Address> user [root]:
   Parameter 2 of 2
   <newCore4_IP_Address> password []:**
   ```

   The password is validated and a number of informational messages display as the script continues.

   > **Note:** This step appears only if you are running the installer on a server that is not the secondary Core server.

4. Select option **1**, Typical secondary Core, and press **Enter** for the following message displayed:

   ```
   Install Type
   ============

   1. Typical secondary Core
   2. Custom secondary Core

   Enter the option number or one of  the following directives

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

5. Select option `1`, Install Oracle with SA for the following message displayed:

   ```
   Oracle Installation

   ===================


   1. Install Oracle with SA

   2. Use existing Oracle database


   Enter the option number or one of the following directives

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

   Press `c` to continue.

6. ⚠ Select the same TLS version as on the primary core and press **Enter** to continue.

   ```
   Cryptographic Protocol Selection for the Server Automation Components
   [WARNING] Please make sure that all the cores and satellites from the mesh are
   ```

```
at the same TLS level.
========================================================================
1. TLSv1
2. TLSv1.1
3. TLSv1.2

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[2]:
```

7. Type `1` to select **Simple Interview** for the following message displayed:

   ```
   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
   ```

   Press `c` to continue.

8. Provide values for the following interview parameters:

   ```
   Interview Parameters
   ====================


   Navigation keys:
   Use <ctrl>p to go to the previous parameter.
   Use <ctrl>n to go the next parameter.
   Use <tab> to view help on the current parameter.
   Use <ctrl>c to abort the interview.


   Parameter 1 of 7 (truth.oaPwd)
   ```

```
Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization. []:
*************


Parameter 2 of 7 (decrypt_passwd)

Please enter the password for the cryptographic material [*******]:


Parameter 3 of 7 (truth.dcNm)

Please enter the short name of the facility where Opsware Installer is being
run (no spaces) [rose2]:


Parameter 4 of 7 (windows_util_loc)

Please enter the directory path containing the Microsoft patching utilities.
Press Control-I for a list of required files or enter "none" if you do not wish
to upload the utilities at this time [none]:


Parameter 5 of 7 (word.store.host)

Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [newCore4_IP_Address]:


Parameter 6 of 7 (word.store.path)

Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:


Parameter 7 of 7 (bootagent.host)

Please enter the OS Provisioning Boot Server ip or hostname [16.77.1.191]:


Enter the option number or one of the following directives

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

Since you specified the CDF file from the First Core Model Repository export, you can accept the defaults, enter `2` and press `c` to continue.

You are asked to re-enter any required passwords for confirmation.

Press **c** to continue for the following message displayed:

```
Install components

==================


Oracle RDBMS for SA

Model Repository, Additional Core

Core Infrastructure Components

Slice

OS Provisioning Components


Enter one of the following directives

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

9. The prerequisite check begins.

   If the prerequisite check completes successfully, you may still see some messages similar to the following:

```
Prerequisite Checks
==============

Results for <IP_address>:

        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

     WARNING File system ‘/’ has 29447 MBytes available and 154050 is
             recommended.

     WARNING Nothing listening at db.host:db.port (ip_address).
             Note: Can be ignored if core install will be performed
             using hpsa_install script.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

   The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press **Enter**.

10. Enter the file name and path for the `TAR.GZ` file you copied on the local server in Phase 4 for the following message displayed:

    ```
    Enter the file path to the truth.*.tar.gz package.

    =====================

    Path to package file truth.SLAVE.tar.gz on the local server
    [/var/tmp/truthFiles/truth.SLAVE.tar.gz]:
    ```

    Press **Enter**. The content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. When the installation completes, the Core Description File (CDF) is automatically saved.

11. Supply the path to the directory containing the database export files on the core’s Oracle database server.

    ```
    Enter the path to the directory containing the database export files.
    ==================================================================

    Path to the directory containing the database export files on the secondary
    Core's Model Repository server [/var/tmp/dbDump]:
    ```

12. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:

    a. Enter the location where you want the OCT component to generate the *.csr files.

    ```
    Select path where to generate CSRs

    =============================

    Specify the path on the Model Repository server where SA will generate the
    CSR files

    [/var/tmp/csrFiles]:

    CSRs were generated in the /var/tmp/csrFiles directory on the server that
    hosts the Model Repository component [192.168.136.39].
    ```

```
Please have them signed by your CA. You can resume the install process after
all CSRs are signed.

Make sure you copy all certificates in the same directory on the core's
Model Repository server.

You will be prompted for the path to this directory in the next step of the
install process.
```

Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
===================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

The script displays process messages and a completion message. During this process, the Installer registers the new secondary Core's Facility with the First Core's Model Repository, automatically generating a unique ID for the Facility.

Phase 5b: Install all secondary Core Components on a single host, remote Non-SA-supplied Oracle database

Use the following procedure to install all SA secondary Core Components on a single server. The Non-SA-supplied Oracle database is installed on a different host.

> **Note:** The remote Oracle database must have been configured as described in "Non-SA-supplied Oracle software and database setup" before you begin the secondary SA Core installation.

During this phase, the First Core Model Repository content exported during Step 4 is imported into the secondary Core's Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA secondary Core Components installed.

1. Invoke the SA Installer specifying (`-c` argument) the CDF copied in Phase 4: `<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml` , where `<distro>` is the full path to the installation media.

   You see messages displayed on screen as the SA Installer loads the required files.

2. The following message is displayed.

   ```
   Specify Hosts to Install

   ========================


   Currently specified hosts:


   <newCore4_IP_Address>


   Please select one of the following options:


   1. Add/edit host(s)

   2. Delete host(s)


   Enter the option number or one of the following directives

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

   Press **c** to continue.

   > In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
   > Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
   >
   > Example: to install an SA mesh with the following topology,
   > ```
   > 16.77.42.65 (oracle_sas, truth_mm_overlay)
   > 16.77.41.24 (infrastructure, word_uploads)
   > 16.77.43.252 (slice, osprov)
   > ```

> `16.77.45.21 (satellite)`
>
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
>
> ```
> 16.77.42.65 hostname1.example.com hostname1
> 16.77.41.24 hostname2.example.com hostname2
> 16.77.43.252 hostname3.example.com hostname3
> ```
>
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

3. Provide the credentials for the secondary Core host:

   ```
   Host Passwords
   ==============

   Parameter 1 of 2
   <IP_address> user [root]:
   Parameter 2 of 2
   <IP_address> password []: **
   ```

   You are prompted for the user and password for the specified host. After you provide all required credentials, the message appears:

   ```
   All values are entered. Do you wish to continue? (Y/N) [Y]:
   ```

   Enter `Y` to continue.

   After you provide all required credentials, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

   > **Note:** This step appears only if you are running the installer on a server that is not the secondary Core server.

4. After the SA Installation media is mounted for all servers, the following menu displays:

   ```
   Install Type

   ============


   1. Typical secondary Core

   2. Custom secondary Core


   Enter the option number or one of the following directives

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

Select Option 1, `Typical secondary Core` and press `c` to continue.

5. Select **2**, `Use existing Oracle database` for the following screen displayed:

   ```
   Oracle Installation

   ===================


   1. Install Oracle with SA

   2. Use existing Oracle database


   Enter the option number or one of the following directives

   (<p>revious, <h>elp, <q>uit): 2
   ```

   Press `Enter` to continue.

6. ⚠ Select the same TLS version as on the primary core and press **Enter** to continue.

   ```
   Cryptographic Protocol Selection for the Server Automation Components
   [WARNING] Please make sure that all the cores and satellites from the mesh are
   at the same TLS level.
   ==========================================================================
   1. TLSv1
   2. TLSv1.1
   3. TLSv1.2

   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit)[2]:
   ```

7. Select the Interview Type from the following message displayed:

   ```
   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):
```

Type `1` for the Simple Interview and press **Enter** to continue.

8. Provide values for the following interview parameters:

```
Interview Parameters

====================


Navigation keys:

Use <ctrl>p to go to the previous parameter.

Use <ctrl>n to go the next parameter.

Use <tab> to view help on the current parameter.

Use <ctrl>c to abort the interview.


Parameter 1 of 12 (truth.oaPwd)
Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization. []:
************* *************
Re-enter the password to confirm: *************

Parameter 2 of 12 (decrypt_passwd)
Please enter the password for the cryptographic material [*************]:


Parameter 3 of 12 (truth.dcNm)
Please enter the short name of the facility where Opsware Installer is being
run (no spaces) [SLAVE]:

Parameter 4 of 12 (windows_util_loc)
Please enter the directory path containing the Microsoft patching utilities.
Press Control-I for a list of required files or enter "none" if you do not wish
to upload the utilities at this time [none]:

Parameter 5 of 12 (db.host)
Please enter the hostname/IPaddress of the Oracle database server.
[192.168.136.39]:

Parameter 6 of 12 (truth.servicename)
```

```
Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.SLAVE]:

Parameter 7 of 12 (db.sid)
Please enter the SID of the Oracle instance containing the Model Repository
[truth]:

Parameter 8 of 12 (db.port)
Please enter the port on which the database is listening. [1521]:

Parameter 9 of 12 (db.orahome)
Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0.2/db_2]:

Parameter 10 of 12 (word.store.host)
Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [192.168.136.38]:

Parameter 11 of 12 (word.store.path)
Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:

Parameter 12 of 12 (bootagent.host)
Please enter the OS Provisioning Boot Server ip or hostname [192.168.136.40]:


Enter the option number or one of the following directives

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

Since you specified the CDF file from the First Core Model Repository export, you can accept the defaults and press `c` to continue.

You are asked to re-enter any required passwords for confirmation.

When you have supplied values for all parameters, the following message displays:

```
All parameters have values. Do you wish to finish the interview? (y/n):
```

Enter `y` and press **Enter** to continue. If you enter `n`, you are presented with each parameter again with the value you entered as the default. You can then change the value or accept the default. If you need to exit the installation, press Ctrl-C.

a. A screen similar to the following displays:

   ```
   Install components

   ==================
   Model Repository, Additional
   ```

```
Core Core Infrastructure
Components Slice
OS Provisioning Components
```

```
Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Enter c and press **Enter** to begin the prerequisite checks.

> If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:
>
> ```
> Slice Network Interface Configuration
> =====================================
>
> Parameter 1 of 2 (Slice: 192.168.136.38)
>
> Please select the interface to use for 192.168.136.38
>
> 1) eth2 -- 192.168.136.55
> 2) eth1 -- 192.168.136.77
> 3) eth0 -- 192.168.136.38 (default)
>  [3]:
> ```
>
> Select the appropriate network interface for each host by entering the associated number from the list.
>
> When you have configured all interfaces, you see the message:
>
> ```
> All values are entered. Do you wish to continue? (Y/N) [Y]:
> ```
>
> Enter y and press Enter to continue. You can edit the list again by pressing n and Enter.

9. The prerequisite check begins.

> Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see "SA Installer Prerequisite Checker"). The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

> If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HPE Support.

10. If the prerequisite check completes successfully, you may still see some messages similar to the following:

    ```
    Prerequisite Checks
    ==============

    Results for <IP_address>:

            WARNING Insufficient swap space (18 GBytes).
                    24 Gbytes is the recommended for Oracle.

         WARNING File system ‘/’ has 29447 MBytes available and 154050 is
                 recommended.

         WARNING Nothing listening at db.host:db.port (ip_address).
                 Note: Can be ignored if core install will be performed
                 using hpsa_install script.

    Enter the option number or one of the following directives:
    (<c>ontinue, <p>revious, <h>elp, <q>uit)
    ```

    The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

    If your server passes the prerequisite check, enter `c` and press **Enter** to begin the installation.

11. Enter the file name and path for the `TAR.GZ` file you copied on the local server in Phase 4 for the following message displayed:

    ```
    Enter the file path to the truth.*.tar.gz package.

    =====================


    Path to package file truth.SLAVE.tar.gz on the local server
    [/var/tmp/truthFiles/truth.SLAVE.tar.gz]
    ```

    Press **Enter**. The content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. After the extraction complete, the SA Installer begins the secondary Core installation.

12. A confirmation screen is displayed, similar to the one below. Make sure that all the presented requirements are met.

    ```
    Make sure you copied the database dump files on the secondary Core's Oracle
    server.
    Please check that the files are in the following directory:
    /u01/app/oracle/admin/truth/dpdump/
    Please also make sure that the oracle user has read permissions for the
    database dump files and write permissions on the folder.
    Enter one of the following directives
    (<c>ontinue, <p>revious, <h>elp, <q>uit): c
    ```

13. You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, the Core Description File (CDF) is automatically saved.
14. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:
    a. Enter the location where you want the OCT component to generate the *.csr files.

    ```
    Select path where to generate CSRs

    =============================

    Specify the path on the Model Repository server where SA will generate the
    CSR files

    [/var/tmp/csrFiles]:

    CSRs were generated in the /var/tmp/csrFiles directory on the server that
    hosts the Model Repository component [192.168.136.39].

    Please have them signed by your CA. You can resume the install process after
    all CSRs are signed.

    Make sure you copy all certificates in the same directory on the core's
    Model Repository server.

    You will be prompted for the path to this directory in the next step of the
    install process.
    ```

Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
===================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Upon completion, a message displays indicating successful installation.

Phase 5c: Install the secondary Core components on multiple hosts, remote non SA-supplied database on remote database server

Use the following procedure to install all SA Core Components on different host servers, for example, Slice Component bundle and/or Model Repository on different servers than the infrastructure components. It also uses an existing remote non-SA-supplied Oracle database. For information about configuring a non-SA-supplied Oracle database for use with SA, see Non-SA-Supplied Oracle Software and Database Setup.

During this phase, the First Core Model Repository content exported during Step 4 is imported into the secondary Core’s Model Repository, the cryptographic material is extracted to the appropriate location on the host and the SA secondary Core Components installed.

1. Invoke the SA Installer specifying the CDF (`-c` argument) copied in Phase 4:

   ```
   <distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf.newCore4.xml
   ```

   where `<distro>` is the full path to the installation media.

You see messages displayed on screen as the SA Installer loads the required files.

For this example installation, we’ll use six remote servers for the core component installation. You will, of course, modify this for your particular system requirements. Components will be installed as follows:

Core component layout

Server	Core Component to be Installed
192.168.136.36	Model Repository
192.168.136.39	Multimaster Infrastructure Components
192.168.136.39	Software Repository Storage and Content
192.168.136.38, 192.168.136.41, 192.168.136.42	Slice
192.168.136.40	SA Provisioning Media Server
192.168.136.40	SA Provisioning Boot Server, Slice version

2. After a few informational messages display, a screen similar to the following displays:

```
Specify Hosts to Install
========================


Currently specified hosts:


<newCore4_IP_Address>


Please select one of the following options:


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


Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):1
```

Enter `1` and press **Enter** to continue.

3. You are asked to specify the number of hosts that will be involved in the installation:

   ```
   Enter number of hosts to add:
   ```

   Enter the appropriate number. For this example, we use six hosts:

   ```
   Enter number of hosts to add: 5
   ```

4. Enter the hostname or IP address of the first server that will host an SA Core Component(s):

   ```
   Adding Hosts
   ============

   Parameter 1 of 5
   Hostname/IP []:
   ```

   Press **Enter**.

   Do the same for all remaining servers. You see this message:

   ```
   All values are entered.  Do you wish to continue? (Y/N) [Y]:
   ```

   Enter Y to continue.

   For this example, we add the hosts:

   ```
    192.168.136.36

    192.168.136.38

    192.168.136.39

    192.168.136.40

    192.168.136.41

    192.168.136.42
   ```

   A screen similar to the following displays:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:

          192.168.136.36
           192.168.136.38
           192.168.136.39
           192.168.136.40
           192.168.136.41
           192.168.136.42

   Please select one of the following options:
   ```

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

```
Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,
> ```
> 16.77.42.65 (oracle_sas, truth_mm_overlay)
> 16.77.41.24 (infrastructure, word_uploads)
> 16.77.43.252 (slice, osprov)
> 16.77.45.21 (satellite)
> ```
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
> ```
> 16.77.42.65 hostname1.example.com hostname1
> 16.77.41.24 hostname2.example.com hostname2
> 16.77.43.252 hostname3.example.com hostname3
> ```
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

5. At this point you can press `2` to delete a host or `1` to add/edit a hostname/IP address. When you choose 1 for an existing list of hosts, you see this prompt:
   ```
   Enter number of hosts to add (or enter "0" to edit the list):
   ```

   When you are satisfied with the entries, type `C` and press **Enter** to continue.

6. Provide the credentials for each host in the list shown in Step 4:

   ```
   Host Passwords
   ==============
   Parameter 1 of 10
   <IP_address> user [root]:
   Parameter 2 of 10
   <IP_address> password []: *******
   ```

   You are prompted for the user ID and password for each specified host. Type the password (which will be obfuscated) and press **Enter**. After you provide all required credentials, the SA Installer attempts to set up NFS mounts to the installation media and prepares each specified server for the installation.

7. After the host preparation completes, the following menu displays:

   ```
   Install Type
   ============

   1. Typical secondary Core
   2. Custom secondary Core

   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit):
   ```

   Select Option 1, `Typical secondary Core` and press **Enter** to continue.

8. Select 2, Use existing Oracle database for the Oracle installation type:

   ```
   Oracle Installation
   ===================

   1. Install Oracle with SA
   2. Use existing Oracle database

   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit): 2
   ```

   Press **Enter** to continue.

9. Enter the associated number of the following component:

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

   1. Model Repository, Additional Core
   2. Core Infrastructure Components
   3. Slice
   4. OS Provisioning Components
   ```

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

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

You use this menu to assign the host on which the SA Core Components are to be installed.

Press the associated number for the component (for example, `1` for the Model Repository). You will see a menu that lists the available hosts and the name of the component to be assigned. It will look similar to this:

```
Host Assignment for Model Repository, Additional Core

=====================================================


1. 192.168.136.36
2. 192.168.136.38
3. 192.168.136.39
4. 192.168.136.40
5. 192.168.136.41
6. 192.168.136.42


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

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

10. Type the number associated with the hostname/IP address of the server you want to host the current SA Core Component and press enter.
    Selecting 1 assigns the Model Repository to the IP address, 192.168.136.36. You will be returned to the Host Component Layout menu. Note that the Model Repository displays the hostname/IP address it was assigned to:

```
Host/Component Layout

=====================


1. Model Repository, Additional Core   :192.168.136.36

2. Core Infrastructure Components      :192.168.136.39

3. Slice                               :192.168.136.38, 192.168.136.41,
                                       :192.168.136.42

4. OS Provisioning Components          :192.168.136.40
```

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

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

Repeat this step for each component listed on the Host Component Layout menu.

You can assign multiple Slice Component bundles to the same host or to different hosts (you must assign at least one):

```
Host Assignment for Slice

=========================


1 ( ) 192.168.136.36

2 ( ) 192.168.136.39


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

(<c>ontinue, <p>revious, <a>ll, <u>nselect all, <h>elp, <q>uit):
```

After you have assigned a Slice Component bundle to a host, an asterisk is displayed next to the hostname/IP address:

2 (*) `192.168.136.39`

After you have assigned a hostname/IP address for all components, enter `c` at the prompt and press **Enter** to continue.

11. ⚠ Select the same TLS version as on the primary core and press **Enter** to continue.

```
Cryptographic Protocol Selection for the Server Automation Components
[WARNING] Please make sure that all the cores and satellites from the mesh are
at the same TLS level.
========================================================================
1. TLSv1
2. TLSv1.1
3. TLSv1.2

Enter the option number or one of the following directives
(<p>revious, <h>elp, <q>uit)[2]:
```

12. Select the Interview Type from the following message displayed:

```
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):
```

Type `1` for the Simple Interview and press **Enter** to continue.

13. Provide values for the following interview parameters:

```
Interview Parameters

====================


Navigation keys:

Use <ctrl>p to go to the previous parameter.

Use <ctrl>n to go the next parameter.

Use <tab> to view help on the current parameter.

Use <ctrl>c to abort the interview.


Parameter 1 of 12 (truth.oaPwd)

Please enter the password for the opsware_admin user. This is the password used
to connect to the Oracle database. If you are installing Oracle with SA the
opsware_admin user will be created with this password. Make sure the password
complexity matches the security guidelines in your organization. []:
*************


Parameter 2 of 12 (decrypt_passwd)

Please enter the password for the cryptographic material [*******]:


Parameter 3 of 12 (truth.dcNm)

Please enter the short name of the facility where Opsware Installer is being
run (no spaces) [SLAVE]:
```

```
Parameter 4 of 12 (windows_util_loc)

Please enter the directory path containing the Microsoft patching utilities.
Press Control-I for a list of required files or enter "none" if you do not wish
to upload the utilities at this time [none]:


Parameter 5 of 12 (db.host)

Please enter the hostname/IPaddress of the Oracle database server.
[192.168.136.37]:


Parameter 6 of 12 (truth.servicename)

Please enter the service name of the Model Repository instance in the facility
where Opsware Installer is being run [truth.SLAVE]:


Parameter 7 of 12 (db.sid)

Please enter the SID of the Oracle instance containing the Model Repository
[truth]:


Parameter 8 of 12 (db.port)

Please enter the port on which the database is listening. [1521]:


Parameter 9 of 12 (db.orahome)

Please enter the path of the ORACLE_HOME directory of your Model Repository
(truth) server. [/u01/app/oracle/product/12.1.0/db_1]:
/u01/app/oracle/product/12.1.0/client_1


Parameter 10 of 12 (word.store.host)

Please enter the IP address of the NFS server for the Software Repository. For
satellite installs, please enter the IP address of the Software Repository
Cache. [192.168.136.39]:


Parameter 11 of 12 (word.store.path)

Please enter the absolute path on the NFS server for Software Repository
[/var/opt/opsware/word]:
```

```
Parameter 12 of 12 (bootagent.host)

Please enter the OS Provisioning Boot Server ip or hostname [192.168.136.40]:


Enter the option number or one of the following directives

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

You are asked to re-enter any required passwords for confirmation.

Since you provided the CDF you created when you installed the Primary SA Core, SA uses the default core configuration parameter values from that CDF as the default for this interview.

When you have supplied all required values, you see this prompt:

```
All values are entered. Do you wish to continue? (Y/N) [Y]:
```

Enter `Y` and press **Enter** to continue.

A screen similar to the following displays:

```
Install components

==================
Model Repository, First Core : 192.168.136.36
Multimaster Infrastructure Components : 192.168.136.39
Software Repository Storage : 192.168.136.39
Slice : 192.168.136.38, 192.168.136.41, 192.168.136.42
OS Provisioning Media Server : 192.168.136.40
OS Provisioning Boot Server, Slice version : 192.168.136.40
Software Repository - Content (install once per mesh): 192.168.136.39

Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Type `c` and press **Enter** to begin the prerequisite checks.

> If the server that will host your Slice Component bundle has more than one network interface installed, SA will detect the presence of two NICs and display a screen similar to the following:
>
> ```
> Slice Network Interface Configuration
> =====================================
>
> Parameter 1 of 2 (Slice: 192.168.136.38)
> ```

> ```
> Please select the interface to use for 192.168.136.38
>
> 1) eth2 -- 192.168.136.55
> 2) eth1 -- 192.168.136.77
> 3) eth0 -- 192.168.136.38 (default)
>  [3]:
>
> Parameter 2 of 2 (Slice: 192.168.136.41)
>
> Please select the interface to use for 192.168.136.41
>
> 1) eth0 -- 192.168.136.41 (default)
> 2) eth2 -- 192.168.136.54
> 3) eth1 -- 192.168.136.76
>  [1]:
> ```
>
> Select the appropriate network interface for each host by entering the associated number from the list.
>
> When you have configured all interfaces, you see the message:
>
> ```
> All values are entered. Do you wish to continue? (Y/N) [Y]:
> ```
>
> Enter `y` and press Enter to continue. You can edit the list again by pressing `n` and Enter.

14. The prerequisite check begins.

> Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation (see "SA Installer Prerequisite Checker"). The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.
>
> If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HPE Support.

15. If the prerequisite check completes successfully, you may still see some messages similar to the following:

    ```
    Prerequisite Checks
    ==============
    ```

```
Results for <IP_address>:

        WARNING Insufficient swap space (18 GBytes).
                24 Gbytes is the recommended for Oracle.

     WARNING File system ‘/’ has 29447 MBytes available and 154050 is
             recommended.

     WARNING Nothing listening at db.host:db.port (ip_address).
             Note: Can be ignored if core install will be performed
             using hpsa_install script.

Enter the option number or one of the following directives:
(<c>ontinue, <p>revious, <h>elp, <q>uit)
```

The Prerequisite check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them.

If your server passes the prerequisite check, enter `c` and press Enter to begin the installation.

16. Enter the file name and path for the `TAR.GZ` file you copied on the local server in Phase 4 for the following message displayed:

```
Enter the file path to the truth.*.tar.gz package.
==================================================
Path to package file truth.SLAVE.tar.gz on the local server
[/var/tmp/truthFiles/truth.SLAVE.tar.gz]:
```

Enter the file name and path for the TAR.GZ file you copied on the local server in Phase 4 and press **Enter**. The content and cryptographic material is extracted to the appropriate directories on the host. The SA installer also performs certain post-Oracle installation tasks and sets required file permissions. After the extraction complete, the SA Installer begins the secondary Core installation.

17. A confirmation screen is displayed, similar to the one below. Make sure that all the presented requirements are met.

```
Make sure you copied the database dump files on the secondary Core's Oracle
server.
Please check that the files are in the following directory:
/u01/app/oracle/admin/truth/dpdump/
Please also make sure that the oracle user has read permissions for the
```

```
database dump files and write permissions on the folder.
Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

18. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Model Repository server before the Core installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After the OCT install, follow the following two additional steps before the SA installation begins:

    a. Enter the location where you want the OCT component to generate the *.csr files.

    ```
    Select path where to generate CSRs

    =============================

    Specify the path on the Model Repository server where SA will generate the
    CSR files

    [/var/tmp/csrFiles]:

    CSRs were generated in the /var/tmp/csrFiles directory on the server that
    hosts the Model Repository component [192.168.136.39].

    Please have them signed by your CA. You can resume the install process after
    all CSRs are signed.

    Make sure you copy all certificates in the same directory on the core's
    Model Repository server.

    You will be prompted for the path to this directory in the next step of the
    install process.
    ```

    Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
    After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
    When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

    b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

    ```
    Enter the path to the directory containing the custom certificates.
    ===================================================================
    ```

```
Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

You see many messages displayed as the installation progresses, unless the installation fails, these messages are purely informational. The installation can take several hours based on the performance of your server. When the installation completes, the Core Description File (CDF) is automatically saved. Upon completion, a message displays indicating successful installation.

Secondary Core post-installation tasks

After you have added a new core to a Multimaster Mesh, you must perform the tasks described in this section.

Associate customers with the new facility

Associate the appropriate customers with each new Facility so that servers managed at that Facility are associated with the correct customer accounts. For more information, see the "Customer Account Administration" section in the SA 10.60 Administration Guide.

Update permissions for the new facility

After you have added a new Facility to your Multimaster Mesh, your SA users will not yet have the required permissions to access the new Facility. You must assign the required permissions to the user groups. For more information, see the "User Group and Setup" section in the SA 10.60 Administration Guide.

Verify multimaster transaction traffic

To verify Multimaster transaction traffic with the target facility:

1. Log in to the SA Client as any user who belongs to the `Opsware System Administrators` group.
2. From the Navigation panel, expand Multimaster Tools under Administration.
3. In the State View Window, note the status box for each facility's transaction.
   A *transaction* is a unit of change to a Model Repository database that consists of one or more updates to rows and has a globally unique transaction ID. If the number of Not Received transactions is not continually growing, the new SA Core is integrated into the Multimaster Mesh.

> It is normal for some transactions to display a not sent status for a short period.

4. Click **Refresh** to refresh the cached data until all transactions display green.

For more information, see the Multimaster Mesh Administration section in Administer.

Advanced SA installation information

> Note: The information in this section is only for the use HPE Professional Services, HPE-certified consultants, and/or HPE Technical Support.

The following topics are discussed in this section:

- "Distributing core components" below
- "Installing a Satellite with SA Provisioning components on separate hosts" on the next page
- "Extending a Satellite realm" on the next page

Distributing core components

If you plan to perform a custom installation in order to distribute SA Core Components in a layout other than those listed in "Customer installable SA Core configurations", you must be aware of the following restrictions.

Additional slice component bundles

When installing additional Slice Component bundles, due to SA Core Component boot order requirements, the Slice Component bundles cannot be installed on the Oracle database host unless the Multimaster Infrastructure Components are installed on the Oracle host.

Core component distribution restrictions

Due to SA Core Component start up order requirements (certain components must be up and running before certain other components can be started), the following core component layouts are valid and show component start order (A first, B second, etc.):

Supported custom core component layouts

Server	Core Components
A	Custom (customer installed) database
B	Model repository
C	Infrastructure Component bundle, Slice Component bundle
D	SA Provisioning components

Supported custom core component layouts, continued

Server	Core Components
A	SA-supplied database, Model repository
B	Infrastructure Component bundle, Slice Component bundle
C	SA Provisioning components
A	Custom (customer installed) database
B	Model repository
C	Multimaster Infrastructure Components
D	Software Repository
E	Slice Component bundle
F	SA Provisioning components

Installing a Satellite with SA Provisioning components on separate hosts

If you have a requirement that the SA Provisioning components be installed on a host other than the Satellite host, contact HPE Professional Services for assistance.

Extending a Satellite realm

> **Note:** It is very important that you understand how peer SA Agent Gateways work before attempting to extend a Satellite Realm. Misconfiguration could lead to significant, intermittent connectivity problems. If you require an extended Realm but do not have the required expertise to do so, contact HPE Professional Services or a certified HPE Consultant.

Realms are a sub-component of SA facilities. A single Facility can contain multiple realms, but a realm can reference only one Facility.

Realms are typically used to allow overlapping IP address space within a Facility in order to keep all SA Agents within a logical Facility (permissions boundary) while still providing flexibility for network reachability. For example, you may have two distinctly separate 10.0.1.x subnets that you must manage in SA under the same logical Facility. Facilities are security boundaries, while Realms inherit the boundaries of their parent facility.

Facility/realm relationships are unique to an Agent Gateway instance or peer group. If you have a facility with two realms, each facility/realm combination is managed by a completely separate group of Agent Gateways. Therefore, realms are a purely logical grouping construct for Agent Gateway configurations.

Typically when a core is installed, you assign a facility name. Then SA automatically creates a standard set of core Realms based on the facility name (`<facility_name>-agents`, `<facility_name>-mm`, etc). When you install an SA Satellite, you can choose either to start a new facility for the Satellite or to join an existing facility.

When you configure a Satellite with realm name `<facility_name>-agents`, you are effectively adding that Satellite as a peer to the SA Core's Agent Gateways that control the facility's `<facility_name>-agents` Realm which is the default Realm for agent management.

In some cases, you may need to extend a Realm. This can be done only by running the SA Installer in Expert mode to install the Satellite, which exposes all SA configuration parameters where you can then specify the extended Realm.

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.

- "Basics of satellite installation" below
- "Satellite installation requirements" below
- "Satellite installation" on page 266

Basics of satellite installation

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.

See Architecture for an introduction to SA Satellites.

Installation summary

The following is an overview of the Satellite installation process.

1. Locate and mount the *Satellite Base Including OS Provisioning media* or NFS-mount the directory that contains a copy of the media
2. Run the SA Installer specifying the Core Definition File (CDF) created during the Primary Core installation. The interview prompts you for information about your Satellite server environment, saves the information in a new Satellite CDF.
3. [Optional] Re-run the Installer to install SA Provisioning components on the Satellite.

Satellite installation requirements

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

- You adhere to the requirements in "SA Provisioning: DHCP proxying". This is only required if you plan to install the SA Provisioning Boot Server and Media Server components in the Satellite.
- The SA Core that will provide core component services to the Satellite are running and accessible during Satellite installation.
- The Satellite server has network connectivity to that Core's Management Gateway.
- You are a member of the System *Administrators* group and member of all user group with **Manage Gateway** permissions.
- You have root access to the parent Core's Model Repository host from where you can copy the files required for installing the Satellite:
  - if working in **self-signed** certification mode, copy the cryptographic material and the security configuration file.
  - if working in **third-party** certificate mode, use the **prep_satellite.sh** script to create a .*tar file with all the files required for the installation.

  > Your selected certificate mode applies to all the SA cores and satellites in the SA mesh. This means that you cannot target only specific cores forthird-party certification and keep others under SA certification.
  > For information on the SA certificate modes, see Cryptographic material options.

- The Satellite server uses UTC, as described in "Check the Core host(s) time and locale requirements". The Satellite server's system time is synchronized with the Primary Core host.
- The network storage configuration allows root Write access over NFS to the directories in which the Software Repository Cache will be installed. This is required if you plan to locate the Satellite's Software Repository Cache on a network storage device.
- Before running the Satellite Installer, ensure you have uninstalled any SA Server Agent installed on the server you plan to use for a new Satellite.
- After the installation process completes, the new Satellite server is owned by the customer "`Opsware`". Before beginning the installation, consider any effects this may have on access rights.

Satellite free disk space requirements

This section describes the free disk space (in addition to the operating files system) requirements for any SA Satellite.

Free disk space required for Satellite component directory

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

Required open ports

Ensure the ports listed in the following table are open so that the Satellite's Gateway can use them. The port numbers listed in the table are default values. You can select other values during the installation.

> Additional ports are required for installing the SA Provisioning Boot Server and Media Server on the Satellite. See "Check network requirements" for a list of these additional ports.

Open ports for a Satellite

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 `ident` service port, used by the Software Repository Cache.
8061	The port is used for Software Repository Accelerator (`tsunami`) component.

IPv6 networking option

To enable IPv6 networking, run the `enable_ipv6.sh` script as a post-installation step. This enables IPv6 on SA core and satellite gateways and OS provisioning components on SA 10.2 or later releases. The script is available on all core servers (infrastructure, slices, boot servers and satellite).
For more information, see "Enable IPv6 networking post installation".

For further information about IPv6 and the `enable_ipv6.sh` script, see the SA Remote Communications Administration section in the SA 10.60 Administration Guide.

For information about running the `enable_ipv6.sh` script post-installation, see "Enable IPv6 networking post installation".

Satellite installation

This section describes how to install a Satellite on a simple-topology system–a Satellite with a single core.

This topology has the following characteristics:

- The Satellite contains a single Software Repository Cache.
- The Satellite communicates with a single Management Gateway on a core server. No other gateways communicate with the Satellite. In other words, the Satellite is not part of a cascading Satellite installation in which one Satellite communicates with the core's Management Gateway while the cascaded Satellites communicate with the core using that Satellite's Gateway as an intermediary.

Required information

Depending on the interview level you choose (simple, advanced), you will be prompted to supply the following information during the installation process as shown in the following table.

Satellite installation required information checklist

Parameter	Requirement	Description
`truth.oaPwd`	opsware_admin user access	The opsware_admin password.
cast.admin.pwd	SA Administrator's access	The SA Administrator's password
satellite.dcNm	The Satellite Facility identification	The name of the new Satellite's facility.
satellite.realm_name	Realm name	The name of the new Realm to be serviced by the Satellite. SA uses the Realm name and the IP address of a managed server to uniquely identify a

Satellite installation required information checklist, continued

Parameter	Requirement	Description
		managed server. The Gateway Installer assigns the Realm name to the new Satellite facility. The Core and Satellite facility names must be different. The Realm name cannot contain spaces.
satellite.gateway_name	The name for a new or existing Satellite Gateway (name cannot contain spaces)	The name of the Gateway the Satellite will use for communicating with the Primary Core management Gateway or other Satellite Gateways (in a cascaded-Satellite topology).
satellite.proxy_port	The port used by Agents to contact the new Satellite.	The port number on which agents can contact the Satellite Gateway (Default: 3001).
satellite.parentgw.ip	A Core Management Gateway IP address	The IP address of a server running a Management Gateway.
satellite.parentgw. tunnel_listener_port	The Management Gateway's listener port	The port number through which tunnel connections to the Management Gateway will pass (Default port is 2001). The Management Gateway listens on this port for connection requests from the Satellite. In the Management Gateway Properties File, this port is specified with the `opswgw.TunnelDst` parameter. The path to the Core's Gateway Properties file is: `/etc/opt/opsware/opswgw-mgw0-<facility>/opswgw.properties`
satellite.parentgw. proxy_port	The port on which a Core's Management Gateway listens for connection requests.	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).
decrypt_passwd	Accessing Core cryptographic material	The password required to access the Core's cryptographic material.
word_root	Package Repository	The root directory for the Package Repository. For example:

Satellite installation required information checklist, continued

Parameter	Requirement	Description
	location (SA Provisioning)	`/var/opt/opsware/word`
word_tmp_dir	Software Repository	Directory where Package Repository will temporarily place content during uploads. For example: `/var/opt/opsware/word`
word.store.host	Software Repository	The host name of the server where Software Repository content is stored.
media_server. linux_media	Linux media location (SA Provisioning)	The pathname to the Linux media. For example: /media/opsware/linux
media_server. sunos_media	Solaris media location (SA Provisioning)	The pathname to the Solaris media. For example: /media/opsware/sunos
media_server. windows_media	Windows media location (SA Provisioning)	The pathname to the Windows media. For example: /media/opsware/windows
media_server.windows_ share_name	Windows Media location (SA Provisioning)	The share name to use for the Windows media sharing server Share names that are longer than 8 characters may give errors while browsing or may not be accessible to some older clients.
media_server.windows_ share_password	Windows Media location (SA Provisioning)	The password to write-protect the Windows media share. Import_media tool will prompt for this password each time it is run.
bootagent.host	SA Provisioning Boot Server	The SA Provisioning Boot Server IP or hostname.
agent_gw_list_args	Agent- Gateway communications	The list of Gateways on which the Satellite's agent will be installed. Specified by the IP address and port number (`ip:port`) on which Agents can contact the Gateway in the Satellite facility. Default <satellite_

Satellite installation required information checklist, continued

Parameter	Requirement	Description
		gateway>:3001.
`opswgw.ConfigPort`	Bandwidth configuration	The gateway Bandwidth Configuration Management port.
`opswgw.BwUsageChannelPort`	Bandwidth configuration	The gateway bandwidth usage channel port.
`agw_admin_port`	Bandwidth configuration	The port for the administrative interface of the Agent Gateway.

> You may want to name the Realm according to the physical location of the Satellite's data center, for example, the building, corporate site, or city. The SA Client lists the facility names of the core and its Satellites.

Satellite installation phases

This section provides a summary of the Satellite installation process. You can use the right-hand column to indicate that a phase is completed:

Satellite installation phases

Phase	Description	Complete
1	Prepare for Installation	
2	Complete the Installer Interview	
3	Install the Satellite	
4	Install the SA Provisioning Components (optional)	
5	Post-Satellite Installation Tasks	

Phase 1: Preparing for installation

1. Locate the SA Satellite installation media:
   - *sat_base* (HPE Server Automation Satellite Base) - The media used to install the SA Satellite components. This does not include the OS Provisioning components and is therefore smaller

and can be helpful when you are transferring the media over the network.

- *sat_osprov* (HPE Server Automation Satellite Base including OS Provisioning) - The media used to install the SA Satellite and the Satellite's OS Provisioning components. You can use this media for installing any Satellite.

2. On the server where you will install the new Satellite, mount the installation media or NFS-mount the directory that contains a copy of the media.

   > Requirements: The Installer must have *read/write root* access to the directories where it will install the SA Core Components, including NFS-mounted network appliances.

3. In a terminal window, log in as a user with **root** privileges.
4. Set up the environment for creating the CA certificates:

   if working in self-signed certificate mode

   i. Create the Realm directory: `mkdir -p /var/opt/opsware/crypto/cadb/realm`

   ii. Make sure you have copied the database of the cryptographic material (**opsware-crypto.db.e**) from any Core server in the facility to the Satellite server, as described in "Satellite installation requirements" on page 263.
   On the Core server, the database and the GZipped **prep_satellite.tar.gz** file are located under `var/opt/opsware/crypto/cadb/realm/`

   > **Important:** The database of cryptographic material must be copied on the Satellite server to the same directory path as on the core server. The directory and database must be readable by the root user.
   >
   > If you start installing a Satellite on a server that does not have a copy of the cryptographic material, the installer requires you to copy the material to the server before it can continue.
   >
   > In a Single-Core installation, the cryptographic material is located in the `/var/opt/opsware/crypto/cadb/realm` directory on the Primary Core. In a Multimaster Mesh installation, the cryptographic material can be copied from the `/var/opt/opsware/crypto/cadb/realm` directory on any server that hosts a core component. If you have stored the cryptographic material on a remote, non-SA Core server, copy the file from the remote server's `/var/opt/opsware/crypto/cadb/realm` directory.

   iii. Create the following directory on the Satellite host: `mkdir -p /etc/opt/opsware/crypto`

iv. From the core to which the satellite will connect, copy the `/etc/opt/opsware/crypto/security.conf` file to the same directory on the Satellite host.

v. Create the CDF directory: `mkdir -p /var/opt/opsware/install_opsware/cdf/cdf`

vi. From the Core's Infrastructure Component bundle host, copy the `/var/opt/opsware/install_opsware/cdf/cdf.xml` file to the same directory on the Satellite host.

if working in third-party certificate mode

i. On the Core's Infrastructure Component bundle host, run the following script. Make sure to specify the full path to the script.

```
<distro>/disk001/opsware_installer/tools/prep_satellite.sh --decrypt_pass
<crypto_password> --loc <location>
```

Satellite preparation script arguments

Argument	Description
--decrypt_pass	Specifies the password for accessing the core cryptographic material. You can find this install parameter in the `/var/opt/opsware/install_opsware/cdf/cdf.xml` file of the SA Core.
--loc	Specifies where to place the **prep_satellite.tar.gz** file which contains the necessary files for Satellite installation.

ii. From the core's Infrastructure Component bundle host, copy the previously created *.tar file to a temporary directory on the Satellite host.

iii. On the server where you will install the new Satellite, run the following script. Make sure to specify the full path to the script.

```
<distro>/disk001/opsware_installer/tools/preinstall_satellite_3rd_party.sh
--tar <tar_file>
```

Satellite preinstallation script arguments

Argument	Description
`--tar`	The **prep_satellite.tar.gz** file created with the **prep_satellite.sh** script.

> In third-party certificate mode, make sure that all the SA Core and Satellite hosts define the hostnames of all Core or Satellite hosts at the beginning of their `/etc/hosts` file. Otherwise, the SA installation will fail.
> Listing these hostnames in the `/etc/hosts` file enables SA to generate correct certificate signing requests (CSRs) for the SA hosts.
>
> Example: to install an SA mesh with the following topology,

> `16.77.42.65 (oracle_sas, truth_mm_overlay)`
> `16.77.41.24 (infrastructure, word_uploads)`
> `16.77.43.252 (slice, osprov)`
> `16.77.45.21 (satellite)`
> add the following lines at the beginning of the `/etc/hosts` file for `16.77.42.65`, `16.77.41.24` and `16.77.43.252`:
> `16.77.42.65 hostname1.example.com hostname1`
> `16.77.41.24 hostname2.example.com hostname2`
> `16.77.43.252 hostname3.example.com hostname3`
> The `16.77.45.21 (satellite)` server does not need to be listed here because this server is part of the mesh and not part of the Core.

5. Change to the root directory: `cd /`

Phase 2: Completing the installer interview

1. On the Satellite host, run the Installer script:

   ```
   # <distro>/disk001/opsware_installer/hpsa_add_satellite.sh -c
   /var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
   ```

   You must specify the full path to the script.

2. A screen similar to the following displays:

   ```
   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):
   ```

   At the components prompt, select the IDs of the components you want to install and assign each of them to a host. After all the components have been assigned to a host, press `c` to continue.

> The SA Provisioning Boot Server and Media Server entries only appear when you have initiated the Satellite installation from the SA *Satellite Base Including OS Provisioning media*. You may choose not to install the OS Provisioning components.

3. ⚠ Select the same TLS version as on the primary core and press **Enter** to continue.

   ```
   Cryptographic Protocol Selection for the Server Automation Components
   [WARNING] Please make sure that all the cores and satellites from the mesh are
   at the same TLS level.
   ========================================================================
   1. TLSv1
   2. TLSv1.1
   3. TLSv1.2

   Enter the option number or one of the following directives
   (<p>revious, <h>elp, <q>uit)[2]:
   ```

4. A screen similar to the following is displayed:

   ```
   Host/Component Layout
   ==============
   1. Satellite [192.168.220.134]
   2. OS Provisioning Boot Server [192.168.220.134]
   3. OS Provisioning Media Server [192.168.220.134]
   Enter the option number or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit): c
   ```

   Press `c` to continue.

5. The interview type selection screen is displayed:

   ```
   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):
   ```

Select `1` for a simple interview or `2` for an Advanced interview. The list in step 4 shows which parameters are modifiable in the Simple and Advanced interviews. The Expert interview is for the use of HPE Technical Support or Professional Services only.

6. Provide values for parameters presented during the interview or accept defaults.
   The parameter values requested during the interview depend on the interview mode:
   a. `(truth.oaPwd) Please enter the password for the opsware_admin user`
      - Simple and Advanced
   b. `(cast.admin.pwd) Enter the password for the SA admin user`
      - Advanced and Expert
   c. `(satellite.dcNm) Enter the new Satellite Facility name`
      - Simple and Advanced
   d. `(satellite.realm_name) Enter the new Satellite Realm name`
      - Expert
   e. `(satellite.gateway_name) Enter the name of the Satellite Gateway`
      - Expert
   f. `(satellite.proxy_port) Enter the port used by agents to contact the new Satellite`
      - Advanced and Expert
   g. `(satellite.parentgw.ip) Enter the IP address of the First Core Management Gateway`
      - Simple and Advanced
   h. `(satellite.parentgw.tunnel_listener_port) Enter the port number on which a Core's Management Gateway listens for connections from Satellite Gateways or the port on which a Satellite Gateway listens for connections from other Satellite Gateways (cascading satellite links)`
      - Advanced and Expert
   i. `(satellite.parentgw.proxy_port) Enter the port on which the Management Gateway listens for Satellite connections`
      - Advanced and Expert
   j. `(decrypt_passwd) Enter the password for the cryptographic material`
      - Advanced
   k. `(word_tmp_dir) Enter directory where Package Repository will temporarily place content during uploads. [/var/opt/opsware/wordbot_tmp/]`
      - Expert

l. `(word_root) Enter the root directory for the Package Repository [/var/opt/opsware/word]`
   - Expert

m. `(media_server.linux_media) Enter the pathname of the Linux media [/media/opsware/linux]`
   - Advanced and Expert SA Provisioning

n. `(media_server.sunos_media) Enter the pathname of the Solaris media [/media/opsware/sunos]`
   - Advanced and Expert SA Provisioning

o. `(media_server.windows_media) Enter the pathname of the Windows media [/media/opsware/windows]`
   - Advanced and Expert SA Provisioning

p. `(media_server.windows_share_name) Enter 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.) [OSMEDIA]`
   -Expert

q. `(media_server.windows_share_password) Enter a password to write-protect the Windows media share. Import_media tool will prompt for this password each time it is run`
   - Expert

r. `(bootagent.host)Enter the OS Provisioning Boot Server ip or hostname`
   - Simple and Advanced SA Provisioning

s. `(agent_gw_list_args)Enter the IP address and port number (ip:port) on which agents can contact the gateway in this facility`
   - Expert

7. Supply values for the parameters. When you have completed entering all of the required information, the Installer displays this message:
   `All parameters have values. Do you wish to finish the interview (y/n):`

   If you are satisfied with your answers, press y.

   If you want to review or change your answers, press n. The installer displays the prompts again, showing in brackets [ ] the values that you just entered during the interview.

   After modifying your responses, press `y` to finish the interview.

8. The Installer automatically saves your values into a CDF in `/var/tmp`.

Phase 3: Installing the Satellite components

1. A screen similar to the following is displayed:

   ```
   Install components
   ===================

   Satellite
   OS Provisioning Boot Server
   PS Provisioning Media Server

   Enter one of the following directives
   (<c>ontinue, <p>revious>, <h>elp, <q>uit): c
   ```

   Press `c` to continue.

2. Before starting the installation, SA performs a prerequisites check. This check validate that the host on which you are installing SA meets the minimum requirements for the installation:
   - the required packages are installed
   - the required environment variables are set
   - sufficient disk space is available, and so on.

   If your host fails the prerequisites check, the installation fails with an error message that describes the problem. In this case, correct the problem and retry the installation. If you are unable to resolve the problem, contact HPE support services.

   If the prerequisites check completes successfully, you may still see some messages similar to the following:

   ```
   Prerequisite Checks
   ==============
   Results for <IP_address>:
   WARNING File system ‘/’ has 29447 MBytes available and 154050 is recommended.

   Enter the option number or one of the following directives:
   (<c>ontinue, <p>revious, <h>elp, <q>uit):
   ```

   The Prerequisites check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, Core performance may be negatively affected if you continue without resolving them. If your server passes the prerequisite check, enter **c** and press **Enter** to start the installation.

3. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Satellite server before the Satellite installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:
   a. Enter the location where you want the OCT component to generate the *.csr files.

      ```
      Select path where to generate CSRs

      =============================

      Specify the path on the Model Repository server where SA will generate the
      CSR files

      [/var/tmp/csrFiles]:

      CSRs were generated in the /var/tmp/csrFiles directory on the server that
      hosts the Model Repository component [192.168.136.39].

      Please have them signed by your CA. You can resume the install process after
      all CSRs are signed.

      Make sure you copy all certificates in the same directory on the core's
      Model Repository server.

      You will be prompted for the path to this directory in the next step of the
      install process.
      ```

      Submit these files to your CA for signing and place the issued certificates in a folder of your choice.

      After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.

      When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

   b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

      ```
      Enter the path to the directory containing the custom certificates.
      ===================================================================
      ```

```
Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

Phase 4: Post-Satellite installation tasks

After you install the Satellite, perform the tasks listed in the following sections. For more information, see the "Satellite Administration" section in the SA 10.60 Administration Guide.

Facility permission settings

> This is an important step because until you set the facility permissions, you cannot view the new Satellite or view/modify the managed servers associated with the Satellite’s facility.

The SA Gateway Installer assigns the Realm name to the facility name of the Satellite. To access managed servers in the Satellite, an SA user must belong to a group that has the necessary permissions for the Satellite’s facility. For example, you might set the permissions for the Satellite facility to Read & Write for the Advanced Users group, enabling members of this group to modify the servers managed by the Satellite.

For further instructions, see the Setting the **Facility Permissions of a User Group** section in the SA 10.60 Administration Guide.

Checking the Satellite

To verify that the Core Management Gateway is communicating with the Satellite:

1. Log in to the SA Client as a member of a user 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 modify the Satellite properties file located in:

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

   If you are implementing a cascaded satellite setup with wordcache enabled, then you must manually add the following entries in the properties file (`opswgw.properties`) of the parent satellite:

   ```
   opswgw.EgressFilter=tcp:*:1003:*:<cascaded satellite realm name>
   ```

```
opswgw.EgressFilter=tcp:*:8061:*:<cascaded satellite realm name>
```

If you modify 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 group that has Read (or Read & Write) permission for the Satellite facility.
5. From the Navigation panel, click **Servers** > **Manage Servers**.
6. Verify that the **Manage Server** page displays the host name of the Satellite server.

DHCP configuration for SA Provisioning

After you install the SA Provisioning Boot Server component, you must set up a DHCP server. For more information, see "DHCP configuration for SA Provisioning".

Optional: Installing the OS Provisioning component for an already installed satellite

The SA Provisioning Boot Server and Media Server are required only if you want to use the SA Provisioning feature in the Satellite. The SA Provisioning Boot Server and Media Server can reside on a different server than the Satellite.

The OS Provisioning components are considered optional and can be installed at a later time.

Installing SA Provisioning components on the Satellite host

Phase 1: Completing the installer interview

1. If you are installing the SA Provisioning components on the same host as the Satellite, invoke the installer again with the `-c` option. This specifies the CDF created by the interview when you installed the satellite component:

   ```
   # <distro>/disk001//opsware_installer/hpsa_add_satellite.sh -c
   ```

```
/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

2. At the **Specify Satellite hosts** prompt, add the IP or hostname of the server where you want to install the SA Provisioning components. If the IP/hostname of Satellite where you want to add the SA Provisioning components is already listed, press **c** to continue, otherwise press **1** to add it to the list of hosts:

   ```
   Specify Satellite hosts:
   ========================
   Currently specified hosts:
    <ip_address>
   Please select one of the following options:
   1. Add/edit host(s)
   2. Delete host(s)
   Enter the option number or one of the following directives
   (<c>ontinue, <h>elp, <q>uit):
   ```

3. At the components prompt, select the OS Provisioning components to install:

   ```
   Host/Component Layout
   =====================
   1. Satellite [<ip_address>]
   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): 2
   ```

4. Select the IDs of the components you want to install (OS Provisioning Boot Server and OS Provisioning Media Server) and assign each of them to a host:

   ```
   Host/Component Layout
   =====================
   1. Satellite [<ip_address>]
   2. OS Provisioning Boot Server [<ip_address>]
   3. OS Provisioning Media Server [<ip_address>]
   Enter the number of the component or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit): c
   ```

   After all the components have been assigned to a host, press c to continue.

Phase 2: Installing the Satellite components

1. Before starting the installation, SA performs a prerequisites check to validate that the host on which you are installing SA meets the minimum requirements for the installation:
   - the required packages are installed
   - the required environment variables are set
   - sufficient disk space is available, and so on.

   For more information, see "System requirements for installation " on page 8

   If your host fails the prerequisites check, the installation fails with an error message that describes the problem. In this case, correct the problem and retry the installation. If you are unable to resolve the problem, contact HPE support services.

   If the prerequisites check completes successfully, you may still see some messages similar to the following:

   ```
   Prerequisite Checks
   ==============
   Results for <IP_address>:

   WARNING File system ‘/’ has 29447 MBytes available and 154050 is recommended.

   Enter the option number or one of the following directives:
   (<c>ontinue, <p>revious, <h>elp, <q>uit):
   ```

   The prerequisites check identifies WARNINGs and/or FAILUREs. FAILUREs can cause a failed or incomplete installation. Resolve these issues before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them. If your server passes the prerequisite check, enter **c** and press **Enter** to start the installation.
2. In **third-party** certificate mode, SA installs the OCT (Opsware Cert Tool) component on the Satellite server before the Satellite installation begins. The OCT component will generate the Certificate Signing Requests (CSRs) for the certificates required for the current installation configuration. After OCT install, follow the following two additional steps before the SA installation begins:
   a. Enter the location where you want the OCT component to generate the *.csr files.

      ```
      Select path where to generate CSRs

      =============================

      Specify the path on the Model Repository server where SA will generate the
      CSR files

      [/var/tmp/csrFiles]:
      ```

```
CSRs were generated in the /var/tmp/csrFiles directory on the server that
hosts the Model Repository component [192.168.136.39].

Please have them signed by your CA. You can resume the install process after
all CSRs are signed.

Make sure you copy all certificates in the same directory on the core's
Model Repository server.

You will be prompted for the path to this directory in the next step of the
install process.
```

Submit these files to your CA for signing and place the issued certificates in a folder of your choice.
After generating the cryptographic material, SA places the CSRs created for that instance in a subfolder named by date. For example: `csr_2017-05-02.08:21:05 csr_2017-05-02.08:22:10`. Any new CSRs are placed in the dedicated folder that you provide during the installer interview.
When providing the third-party certificates, make sure to follow the certificate format and naming requirements described in the SA certificates format.

b. Provide the location where you have placed the custom certificates signed by your CA. The installer checks that the path is correct and that all required certificates are available.

```
Enter the path to the directory containing the custom certificates.
===================================================================

Path to the directory containing the certificates.
[/var/tmp/certificateFiles]:
```

SA now generates a new cryptographic material containing your signed certificates. The cryptographic material is then copied it on all hosts in the mesh.

When the Satellite installation completes, the installer displays a message indicating that the installation was successful.

Installing SA Provisioning components on a non-Satellite host

If you are installing the SA Provisioning components on a different server than the Satellite, you must follow these instructions:

Copy the database of cryptographic material from the Satellite host to the SA Provisioning components host. These file are found on the Satellite host in the following location:

```
/var/opt/opsware/crypto/cadb/realm/opsware-crypto.db.e
```

The database of cryptographic material must have the same paths and filenames on both servers. The directory and files also need to be readable by the root user.

Copy the CDF created by the interview when you installed the satellite component to the server that will host the SA Provisioning components. You can find the CDF file in the following location:

```
/var/opt/opsware/install_opsware/cdf/cdf_<timestamp>.xml
```

Using the Satellite Base Including OS Provisioning media, invoke the SA Installer again with the -c option and specify the CDF you copied previously:

```
/<distro>/opsware_installer/hpsa_add_satellite.sh -c /var/opt/opsware/install_
opsware/cdf/cdf_<timestamp>.xml
```

At the Specify Satellite hosts prompt, you must add the IP or hostname of the server where you want to install the SA Provisioning components

```
Specify Satellite hosts:
========================
Currently specified hosts:
<ip_address_1>
Please select one of the following options:
1. Add/edit host(s)
2. Delete host(s)
Enter the option number or one of the following directives
(<c>ontinue, <h>elp, <q>uit): 1
```

You are asked to specify the number of hosts that will be involved in the installation. Enter the appropriate number. For this example, we add one host in addition to the default host:

```
Enter number of hosts to add: 1
```

Enter the hostname or IP address of the first server that will host an SA Provisioning Component and press Enter. You see this message:

```
All values are entered. Do you wish to continue? (Y/N) [Y]:
```

Enter **Y** to continue.

A screen similar to the following appears:

```
Specify Satellite hosts:
========================
Currently specified hosts:
```

```
<ip_address_1>
<ip_address_2>
Please select one of the following options:
1. Add/edit host(s)
2. Delete host(s)
Enter the option number or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Press C to continue.

The next step is to provide the OS credentials for the added host

```
Host Passwords
==============
Parameter 1 of 2
<ip_address_2> user [root]:
Parameter 2 of 2
<ip_address_2> password []: *******
```

You are prompted for the password credentials for each specified host. After you provide all required credentials, you see the message:

All values are entered. Do you wish to continue? (Y/N) [Y]:

At the components prompt, select the OS Provisioning components to install and assign them to the newly added server:

```
Host/Component Layout
=====================
1. Satellite [<ip_address1>]
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): 2
```

Select the IDs of the components you want to install (OS Provisioning Boot Server and OS Provisioning Media Server) and assign each of them to a host.

```
Host/Component Layout
=====================
1. Satellite [<ip_address1>]
2. OS Provisioning Boot Server [<ip_address2>]
3. OS Provisioning Media Server [<ip_address2>]
Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

After all the components have been assigned to a host, press `c` to continue.

Before SA begins the installation, it performs prerequisite checks that validate that the host on which you are installing SA meets the minimum requirements for the installation. The check ensures that required packages are installed, required environment variables are set, sufficient disk space is available, and so on.

If your host fails the prerequisite check, the installation will fail with an error message that describes the problem. If your host fails the prerequisite check, correct the problem and retry the installation or, if you are unable to resolve the problem, contact HPE Support Services.

If the prerequisite check completes successfully, you may still see some messages similar to the following:

```
Prerequisite Checks
==============
Results for <IP_address>:
 WARNING File system ‘/’ has 29447 MBytes available and 154050 is recommended.
Enter the option number or one of the following directives: (<c>ontinue,
<p>revious, <h>elp, <q>uit):
```

The Prerequisite check identifies WARNINGs and / or FAILUREs. FAILUREs can cause a failed or incomplete installation and must be resolved before continuing the installation. WARNINGs allow you to continue the installation, however, core performance may be negatively affected if you continue without resolving them. If your server passes the prerequisite check, enter c and press Enter to begin the installation.

When Satellite installation completes, the installer displays a message indicating that the installation was successful.

SA Core post-installation tasks

This section describes system administration tasks that you must perform after installing an SA Core:

- "Running the health check monitor" on the next page
- "The SA Client" on page 287
- "Install the SA-required Flash Player" on page 288
- "Enable the Oracle automatic optimizer statistics collection" on page 288
- "Install the SA Server discovery and agent " on page 289
- "Add or change an SA Client launcher proxy server" on page 295

- "Predefined user groups permissions" on page 296
- "Agent Deployment Tool (ADT) requirements" on page 296
- "DHCP configuration for SA Provisioning" on page 296
- "Enable IPv6 networking post installation" on page 296
- "Additional network requirements for SA Provisioning" on page 304
- "Global File System tasks" on page 304

Running the health check monitor

The Health Check Monitor (HCM) includes a suite of tests to check the status of an SA Core. For a full description of the monitor and its tests, see the SA 10.60 Administration Guide.

Run the following command:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh
```

Usage:

```
run_all_probes.sh run|list [<probe> [<probe>...][hosts="[<user>@]<system>
[:<password>] [[<user>@]<system>[:<password>]]..." [keyfile=<keyfiletype>:<keyfile>
[:<passphrase>]]
```

Where:

Health check monitor arguments

Argument	Description
`<system>`	Name of a reachable SA Core system
`<user>`	Optional user to access the remote system. The user needs to have sudo permission. Default user is `root`.
`<password>`	Optional user password for `<system>`
`<keyfiletype>`	SSH keyfile type (`rsa_key_file` or `dsa_key_file`)
`<keyfile>`	Full path to the SSH keyfile
`<passphrase>`	Optional pass-phrase for `<keyfile>`

For <`probe`> specify `check_opsware_version`.

You should specify all servers hosting core components in the current core (hosts="[<user>@]<system>[:<password>]) . There are a number ways to specify login credentials for those hosts. For example, if you were using just passwords, the full command would be like this:

```
# /opt/opsware/oi_util/bin/run_all_probes.sh \
run check_opsware_version hosts="host1.company.com:s3cr3t \
host2company.com:pAssw0rd"
```

The hostnames and passwords, of course, should be replaced with your actual values.

The SA Client

The SA Client is a Java client for the Server Automation System. If you installed your core on multiple servers, you can access the SA Client from any Core Server hosting a Component Slice bundle.

To access the SA Client for the first time, you must press the **Download Server Automation Client** button from the SA Web Client homepage. Clicking on this link will download the SA Client on your local machine. Once installed, you can invoke the SA Client from the local machine.

> Note: The SA Client is a Java application that installs and runs with its own Java Runtime Environment (JRE). The SA Client will not interfere with any other versions of JRE you may have installed on your system. The JDK will not be used (and is not usable) by any other Java application on the target computer, and it will not set itself as the default JDK on the target computer.

See the SA 10.60 User Guide for more information about the SA Client.

Download and update JRE

The SA Client launcher can updates the JRE version directly from the SA Core.

> **Note:** JRE will be downloaded on SA Client only when you connect to the slice component that contains the previous version of the JRE.
>
> The following options are available for updating the JRE:
>
> - Making the JRE available on all slices in the environment and thus ensuring that all Client connections to the SA deployment are prompted to upgrade the JRE version.

> - Enforcing a connection to the slice that contains the updated JRE so that the latest JRE version can be downloaded from that slice and used in all SA Client connections to the SA deployment, irrespective of the target slice.

To update the JRE used by the SA Client application:

1. From the HPE Customer Support, obtain the **jre_name.zip** package containing the distribution of OpenJRE on 32 bit.
2. Copy the new **jre_name.zip** archive to the **/opt/opsware/occclient** location of SA Core.
3. Delete the **metadata.xml** file within the **/opt/opsware/occclient** location.

When you launch the SA Client after performing the above steps, a warning window is displayed to choose whether to continue with the JRE upgrade or not. This warning window is displayed in the following conditions only:

- JRE from the SA Core is newer than the JRE bundled with the launcher
- JRE newer than a previously cached JRE.

For SA 10.51 and above, by default, SA Clients will use the latest JRE available in the cache or that is bundled with the launcher.

Install the SA-required Flash Player

SA requires that you install Adobe Flash Player. You can download it from: http://get.adobe.com/flashplayer/otherversions

1. Select Windows.
2. Select Flash Player for Internet Explorer.
3. Follow the onscreen instructions to install.

Enable the Oracle automatic optimizer statistics collection

SA relies on Oracle’s Automatic Optimizer statistics collection to collect schema statistics used to avoid database performance degradation. By default, Oracle’s Automatic optimizer statistics collection should be enabled.

To verify that the Oracle Automatic optimizer statistics collection is enabled, perform the following steps:

1. Enter the following commands in SQL*Plus:

   ```
   # su - oracle

   # sqlplus "/ as sysdba"


   set line 200

   col status format a10

   SELECT status FROM dba_autotask_client where client_name='auto optimizer stats
   collection';
   ```

   The output from the above statement should be as follows:

   ```
   STATUS

   ----------

   ENABLED
   ```

2. If the status is not `ENABLED`, execute the following statement to enable Oracle’s Automatic Optimizer statistics collection.

   ```
   EXEC DBMS_AUTO_TASK_ADMIN.ENABLE(client_name => 'auto optimizer stats
   collection',operation => NULL, window_name => NULL);
   ```

Install the SA Server discovery and agent

SA Client Server discovery and Agent installation identifies servers on your network that do not have Server Agents installed and installs (deploys) Agents onto those servers.

- "Enabling server discovery and agent installation for UNIX and Windows servers " on the next page
- Launching the SA Web Client
- Downloading and installing the SA Client launcher installation package
- "Creating a user account with administrator privileges" on page 291
- "Creating an SA user as a member of the Software policy setters and Software deployers user groups" on page 292

- "Granting the software policy setters and software deployers user groups the required facility privileges" on page 292
- "Scanning for unmanaged servers on your network" on page 292
- "Bringing a server under SA management" on page 294

Enabling server discovery and agent installation for UNIX and Windows servers

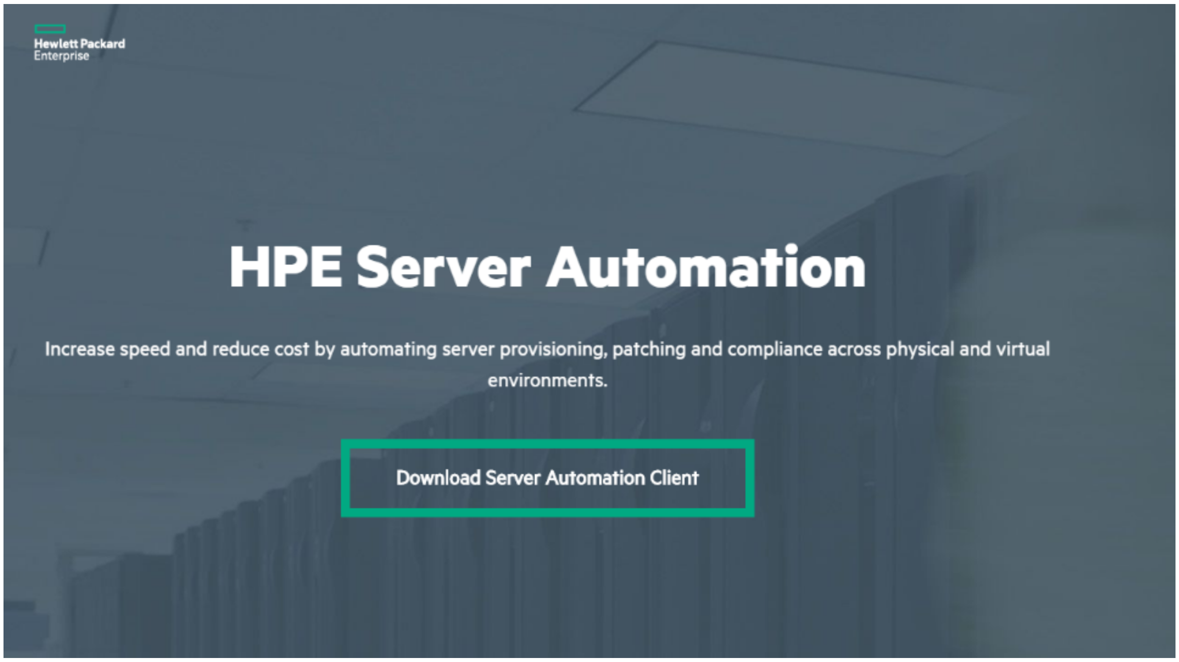
During SA Core installation, the SA Installer automatically installs all required software to perform server discovery and Agent installation from UNIX and Windows hosts . No other configuration is required.

Launching the SA Web Client

To launch the SA Web Client:

1. In a supported web browser, enter the following URL:
   `http://<SA_hostname>`

   where `<SA_hostname>` is the host name or IP address of the server on which you installed SA.
2. The browser displays instructions for installing the required SA security certificate. The SA Web Client homepage appears.


Hewlett Packard Enterprise
HPE Server Automation
Increase speed and reduce cost by automating server provisioning, patching and compliance across physical and virtual environments.
Download Server Automation Client

Downloading and installing the SA Client launcher installation package

> The SA Client requires a Microsoft Windows-based system that is connected to the network on which SA is installed. The SA Client also requires that the Adobe Flash Player be installed for certain functions. See "Install the SA-required Flash Player" on page 288 for more information about installing the Flash Player for use with SA.

You must download and install the SA Client, which is required for most SA features.

1. From the SA Web Client homepage, click on the **Download Server Automation Client** button.
2. Save the file to a directory on your local hard drive.
3. Double-click the file to begin the installation and follow the on screen instructions.

Creating a user account with administrator privileges

Using the SA Client, you must create a new System Administrator user and assign the appropriate SA privileges.

See the "User and User Group Setup and Security" section in the SA 10.60 Administration Guide for instructions on creating new users.

Creating an SA user as a member of the Software policy setters and Software deployers user groups

This user has the privileges to scan your facility’s network for servers not yet managed by SA.

See the "User and User Group Setup and Security" section in the SA 10.60 Administration Guide for instructions on creating new users and adding users to user groups.

Granting the software policy setters and software deployers user groups the required facility privileges

See the "User and User Group Setup and Security" section in the SA 10.60 Administration Guide for instructions on granting privileges to user groups.

Scanning for unmanaged servers on your network

In this phase, you can use SA to scan your network to discover any servers not managed by SA. After SA discovers your unmanaged servers, you are given the choice to bring each server into the SA Managed Server Pool.

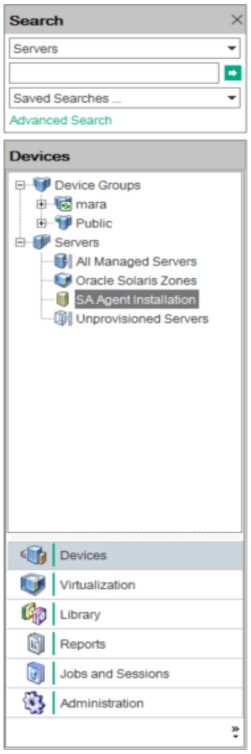
You can scan for unmanaged servers in several ways:

- By specified IP addresses
- By IP address ranges
- Using pre-prepared lists of IP addresses

This section does not attempt to describe all methods, rather it uses a single method for simplicity. For more information about scanning for unmanaged servers (using SA server discovery and Agent installation), see the SA 10.60 User Guide.

Perform the following tasks to scan for an unmanaged server on your network:

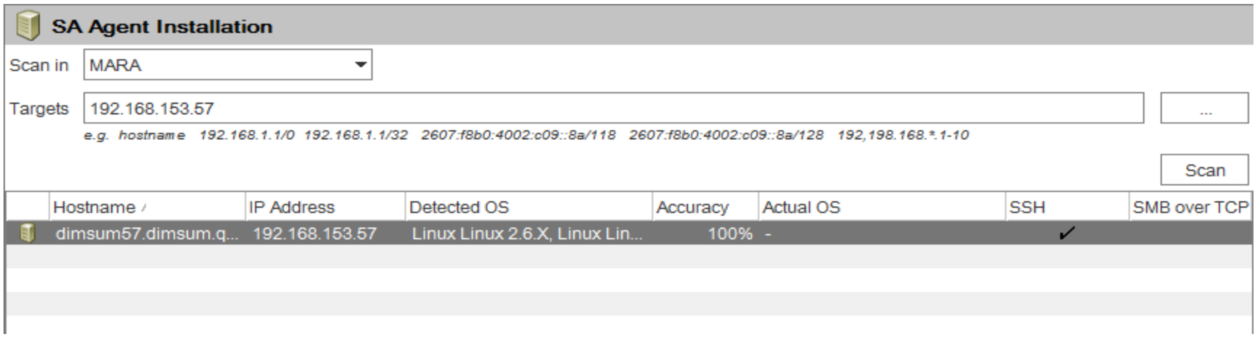
1. Log on to the SA Client as the SA Superuser you created above by double clicking on the SA Client program file or shortcut.
2. On the SA Client main screen, select the **Devices** tab and then select **SA Agent installation** in the navigation pane.



3. In the **Targets** field, specify a list of specific IP addresses to scan, separated by spaces (commas are not supported). Click the ellipsis **(...)** button to display a simple text editor that allows you to enter multiple IP addresses. You can also save the file for future use. Click **OK** to populate the **Targets** field with the IP addresses you entered.

4. Click **Scan** start scanning for unmanaged servers.
   When the scan is complete, a list of discovered unmanaged servers is shown. SA displays each server’s:
   - status
   - IP address
   - host name
   - detected operating system
   - any open ports that can be used to connect to the server

Sample unmanaged server scan results



SA Agent Installation

Scan in: MARA

Targets: 192.168.153.57

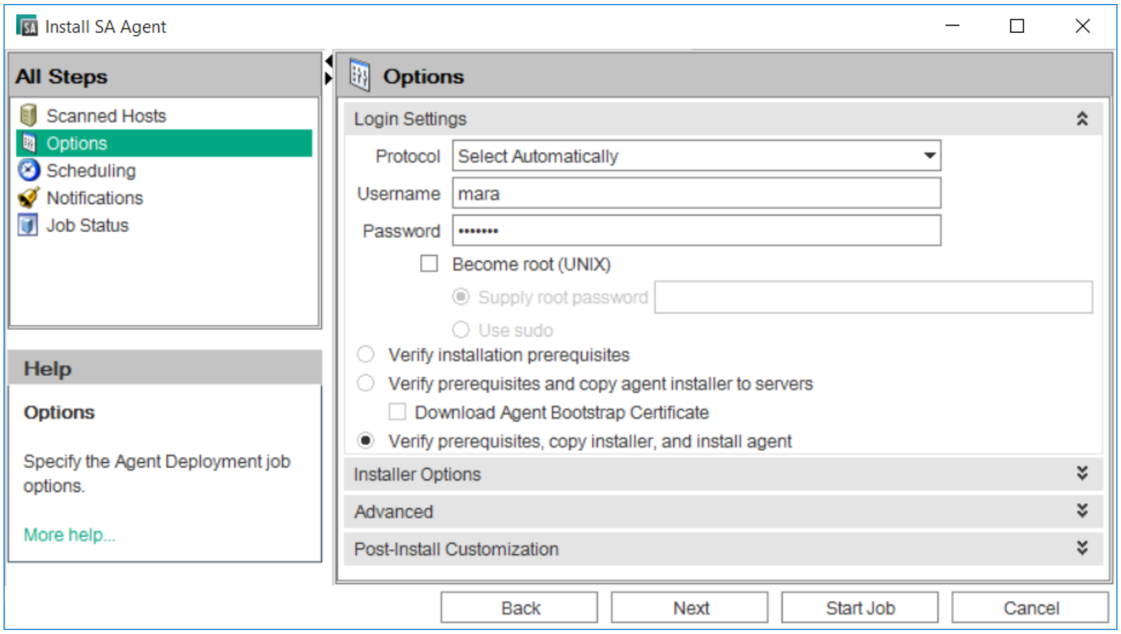
e.g. hostname 192.168.1.1/0 192.168.1.1/32 2607:f8b0:4002:c09::8a/118 2607:f8b0:4002:c09::8a/128 192,198.168..1-10*

Hostname	IP Address	Detected OS	Accuracy	Actual OS	SSH	SMB over TCP
dimsum57.dimsum.q...	192.168.153.57	Linux Linux 2.6.X, Linux Lin...	100%	-	✓	

Bringing a server under SA management

1. Select the servers you want to manage with SA. The SA Client supports hot keys to make multiple selections.

2. From the **Actions** menu, select **Install SA Agent**. This displays the **Install SA Agent** wizard:



Options

Login Settings

Protocol: Select Automatically

Username: mara

Password: •••••••

□ Become root (UNIX)

● Supply root password

○ Use sudo

○ Verify installation prerequisites

○ Verify prerequisites and copy agent installer to servers

□ Download Agent Bootstrap Certificate

● Verify prerequisites, copy installer, and install agent

Help

Options

Specify the Agent Deployment job options.

3. Select a network protocol to use for connecting to the server from the drop-down list.
   In most cases, choosing **Select Automatically** to allow SA to select an appropriate protocol for each server is recommended.

> For VMware ESXi servers where the Linux-based service console (COS) has been removed, you must choose VMware ESX Web Services.

4. Enter a username and password to use for logging into the managed server.
   - Windows-based systems: log in using the Windows administrator username/password.
   - UNIX-based systems: log in as a user with root privileges. If logging in as `root` is not permitted, select the **Become root (UNIX)** checkbox. **Select Supply root password** and enter the password or select **Use sudo** if `sudo` access is enabled for that account.
     If you log in using `sudo`, the sudo user's configuration file (typically `/etc/sudoers`) must allow the account to run any command with root privileges. This is typically accomplished by using the "ALL" alias in the `sudoers` file.

     > **Note:** If you are unable to bring the server under SA management by logging in as root, log in as a non-root user for agent deployment.

5. Select **Verify prerequisites, copy installer, and install agent**.
   See the **Server Discovery and Agent Installation** section in the SA 10.60 User Guide for more information.
6. Make any required changes under the **Installer Options**, **Advanced** and **Post-Install Customization** sections.
7. Click **Next** then **Start Job**. SA performs the required actions on the selected unmanaged servers to bring them into the Managed Server Pool.
8. The SA Client displays the results and updates the status icons for the new managed servers.

You can now use SA to manage these servers.

Add or change an SA Client launcher proxy server

By default, the SA Client uses the proxy server settings configured for the default browser on your local system. For example, if your default browser has no proxy server settings configured, neither will the SA Client.

You can configure SA Client to use a proxy server by editing the Java Web Start `deployment.properties` file.

For details on how to do that, see the SA 10.60 User Guide.

Predefined user groups permissions

SA provides an extended set of role-based, pre-defined user groups. If you plan to use these groups, you must grant read and/or write permissions to the first facility and any other appropriate permissions to the groups. For more information about predefined user groups and permissions, see the Pre-Defined User Groups and Permissions Reference sections in the SA 10.60 Administration Guide.

Agent Deployment Tool (ADT) requirements

If you plan to use the Agent Deployment Tool (ADT) to deploy Server Agents, you must have the OpenSSH client in the root user's path on each server hosting the Slice Component bundle(s) (includes the Gateway) and each Satellite server.

DHCP configuration for SA Provisioning

The Dynamic Host Configuration Protocol (DHCP) specifies how to assign dynamic IPv4 and IPv6 addresses to servers on a network. SA Provisioning uses DHCP to allow network booting and configuration of unprovisioned servers in the Server Pool. DHCP is also used to configure networking on newly provisioned servers that have not been assigned a static network configuration.

For information for setting up DHCP for SA Provisioning, see the "SA Provisioning" section in the SA 10.60 User Guide.

SA also supports Windows and Linux network booting in DHCPless environments (static IP).

Enable IPv6 networking post installation

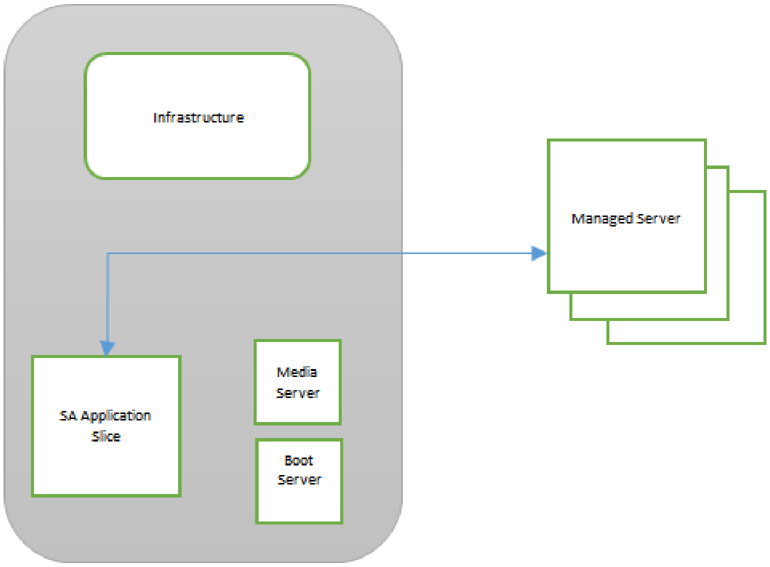
This section describes scenarios to enable IPv6 networking after installation. For details about the `enable_ipv6.sh` script, see the Enable_ipv6.sh Script section in the SA 10.60 Administration Guide.

For the purpose of enabling IPv6 on SA, the following entities are considered to be a single unit:

- A single core with all its slices (excluding the satellites and managed servers behind those satellites)
- A satellite with its associated gateways and OS provisioning components
- Multiple satellite instances in the same realm with their associated gateways and OS provisioning components
- The cores in a multimaster mesh (excluding the satellites and managed servers behind those satellites)

> Note: In all of these scenarios, the phrase “run `enable_ipv6.sh`” means that the script can be run in interactive mode (default) or non-interactive mode (with the `-f` option).

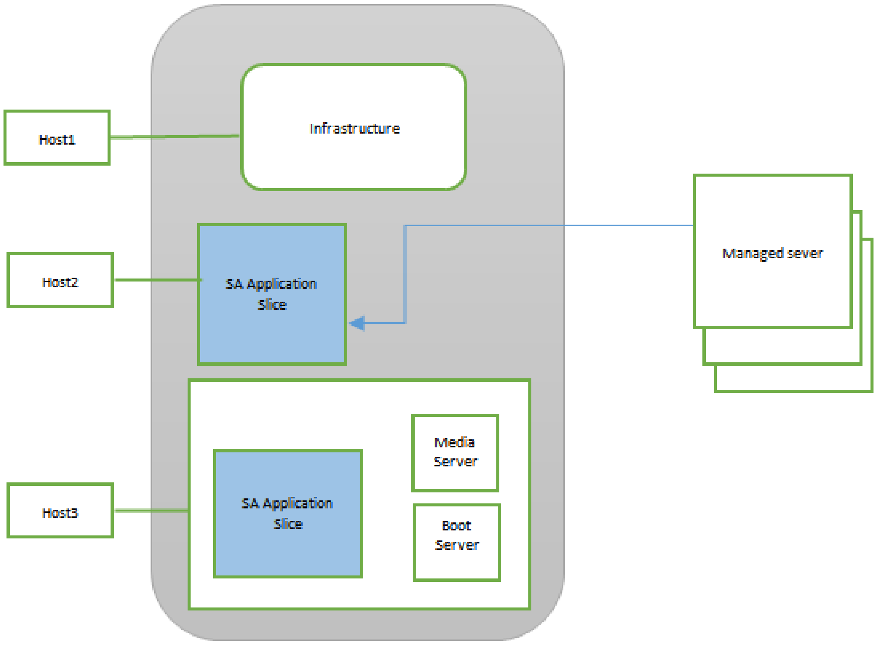
Single core with single slice



The simplest setup is a single core with all SA components installed in the same host. In this case, run the `enable_ipv6.sh` script from the core host. This will enable IPv6 for the gateways (core, agent, and management gateways) and OS provisioning components.

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
```

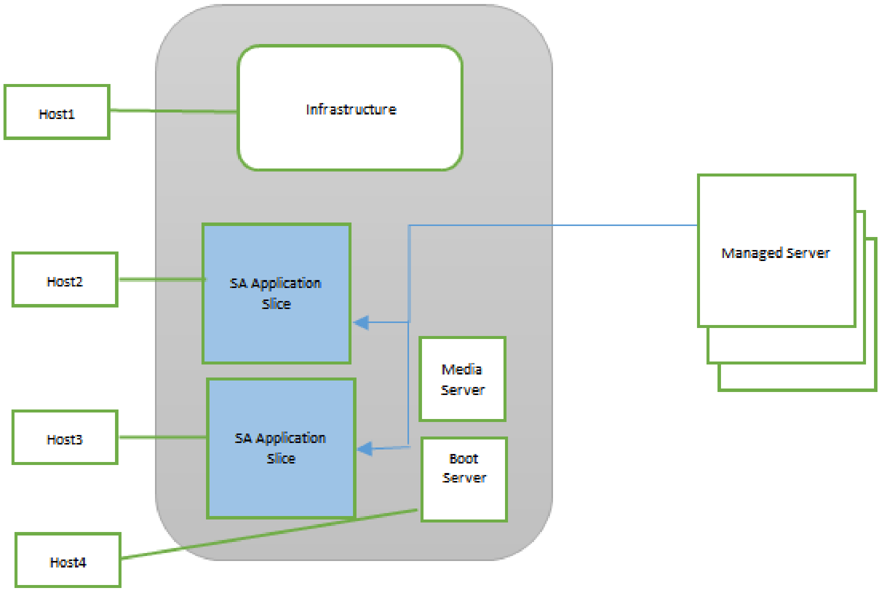
Single core with multiple slices - Boot server and slice running on same host



Run `enable_ipv6.sh` on all infrastructure and slice hosts (Host1, Host2, and Host3 in the previous figure). Note that Host3 is running slice and has Boot and Media Server as well.

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
```

Single core multiple slices - Boot server running on a separate host



The previous figure shows that Host1 runs the infrastructure, and Host2 and Host3 run slices. Run the `enable_ipv6.sh` script in these hosts as:

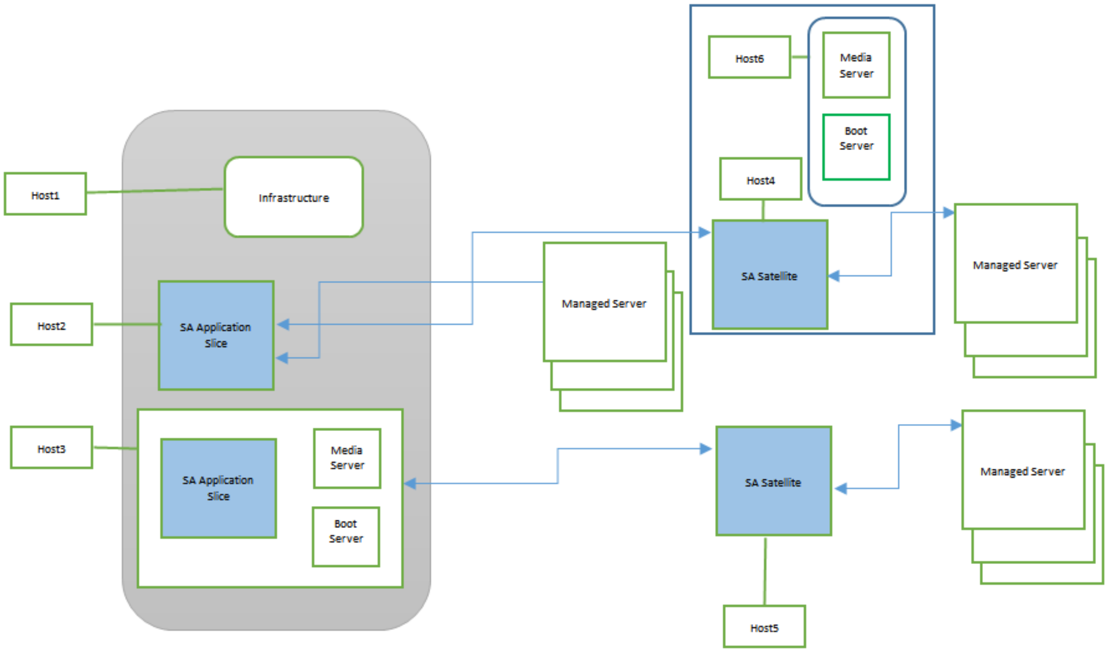
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f

Host4 runs the Boot Server and the Media Server. Host4 does not run any gateway. In this case, the OS provisioning component (Boot Server) is running in a system different from the one in which the gateway is running. Run the `enable_ipv6.sh` script with the `–g` option, where the user has to pass the IPv6 address of the slice running agent gateway.

In the following example, Boot Server (Host4) can be associated with Host2 or Host3 (which run the agent gateway):

```
# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g<IPv6 address of Host2 or Host3>
```

Single core with two satellites and OS provisioning boot server behind the satellite



Host1, Host2, and Host3 run the core components and can be considered as one unit.

Host4 and Host5 run the satellites and can be considered as one unit.

Host6 is running OS provisioning boot server and is associated with the satellite running Host4.

The user can choose to:

- Enable IPv6 on core and satellites:
  In this case, run `enable_ipv6.sh` on all hosts (Host1 through Host6).

  On Host1 to Host5, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f
  ```

  On Host6, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh -f -g <IPv6 Address of
  Satellite>
  ```

- Keep the core as IPv4, and enable IPv6 in satellites:
  In this case, enable IPv6 on host4, host5, and host6.

  On Host4 and Host5, run:

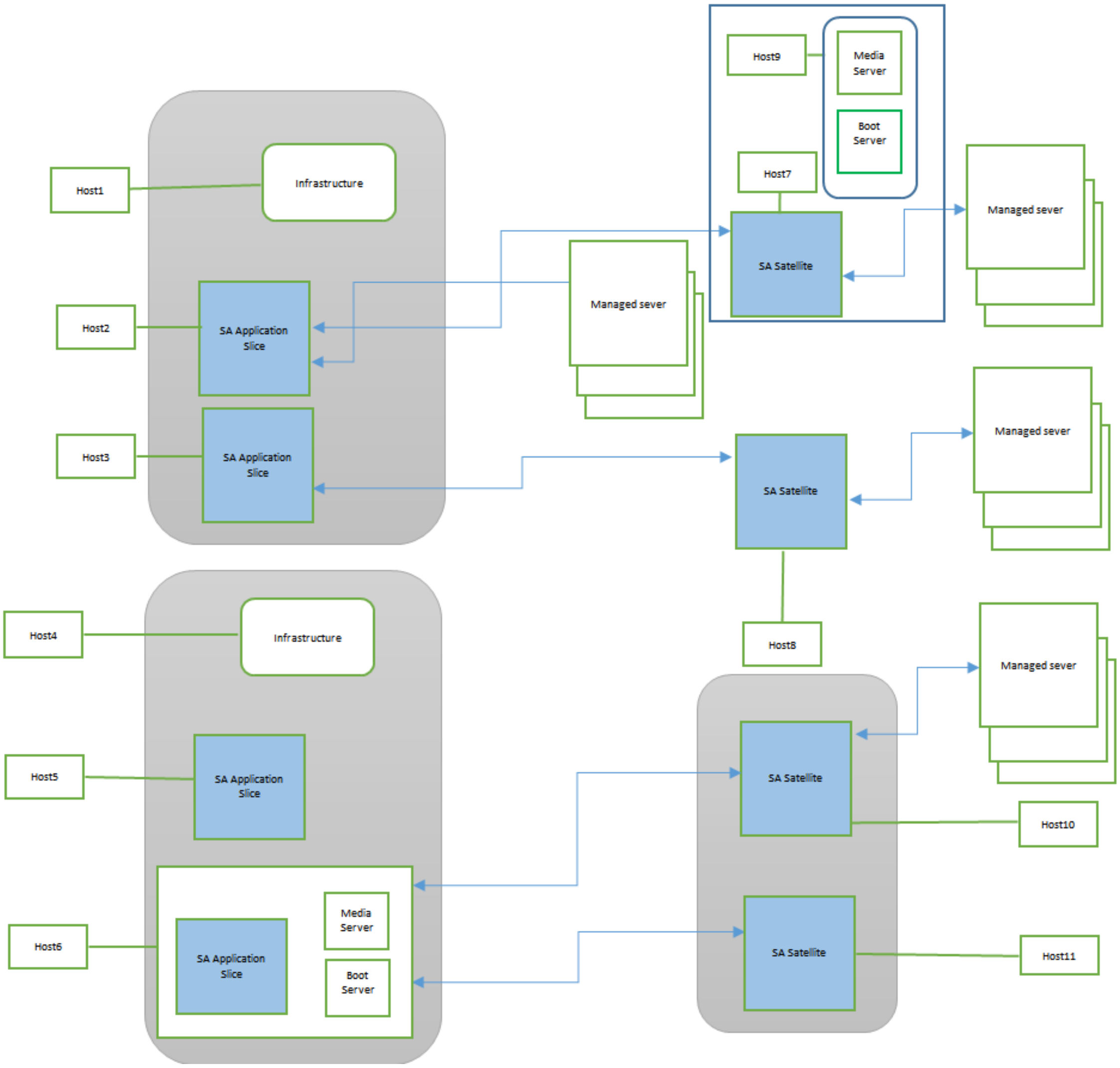
  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host6, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of
  Satellite>
  ```

- Enable IPv6 on the core, and keep the satellites as IPv4:
  On Host1, Host2, and Host3, run: `# /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f`

Multiple cores with single and multiple instances of satellites and the OS provisioning boot server behind a satellite



Host1, Host2, and Host3 constitute the primary core. Host4, Host5, and Host6 makes up the secondary core. For IPv6-enablement purposes, the primary and secondary cores become a single unit.

Satellite Host7 and Host9 (the OS provisioning boot server) are considered a single unit.

Satellite Host8 is considered a single unit.

The satellites on Host10 and Host11 are multiple instances on the same realm, serving to provide high availability. These satellites are considered to be a single unit.

The user can choose to:

- **Enable IPv6 on core and satellites**
  In this case, run `enable_ipv6.sh` on all hosts (Host1 through Host11).

  On all hosts except Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of Host7>
  ```

- **Keep core as IPv4, and enable IPv6 in the satellites**
  In this case, enable IPv6 on Host7, Host8, Host9, Host10, and Host11.

  On Host7, Host8, Host10, and Host11, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

  On Host9, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f –g <IPv6 Address of Host7>
  ```

- **Enable IPv6 on cores, and keep satellites as IPv4**
  On Host1, Host2, Host3, Host4, Host5, and Host6, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

- **Enable IPv6 on some satellites, and keep cores as IPv4**
  For example, the user wants to enable IPv6 on the realm that has multiple satellite instances (e.g., Host10 and Host11).

  On Host10 and Host11, run:

  ```
  # /opt/opsware/oi_util/ipv6_scripts/enable_ipv6.sh –f
  ```

Additional network requirements for SA Provisioning

Open ports

Any server on which an OS is to be provisioned must meet the same requirements for connectivity to the SA Core network as any managed server. For details, see "Required open ports".

Global File System tasks

This section contains optional post-installation tasks for the Global File System (OGFS).

Configuring User ID numbers for the Global File System

When you install a SA Core, you can set values to control the range of UID and GID numbers used by the Global File System. These values are used to provide unique user IDs for all SA users that are logged in to the OGFS. When the Web Services Data Access Engine creates a new user, it will use these values to determine the next available (unique) user ID that is within the range for the local data center.

To set values that control the range of UID and GID numbers, you must specify the following Web Services Data Access Engine parameters in the `params.conf` file:

- **twist.min_uid**: Contains the minimum UID number that can be used. The default value is 80001.
- **twist.default_gid**: Contains the group ID number that a user is assigned to restrict SA users from using certain ports. The default value is 70001.

These parameters are specified as global in the `params.conf` file, which means that they will be written out to the global response file (`oiresponse.global`). This file is generated when the Model Repository export is performed on the Primary Core server. When you follow the installation instructions and provide the global response file (`oiresponse.global`) as the initial response file to the Secondary Core server, SA Installer will use the specified values.

> Requirements: After you make changes to these parameters, you must restart the Web Services Data Access Engine server.

SA configuration

After you have installed the first SA Core, whether as part of a single host or Multimaster Mesh installation, the SA Core Components will be running and you will be able to log in to that core’s SA Client. You can now configure SA so that end users can start managing servers in their operational environment.

The following sections provide a general outline of the SA configuration tasks you will need to do and pointers to the HPE documentation that contains the detailed instructions needed to complete the tasks.

- "Customized SA Core configuration files" below
- "Configuring e-mail alerts" on page 307
- "Setting up SA groups and users" on page 307
- "Creating SA customers" on page 307
- "Defining software management policies" on page 307
- "Deploying Server Agents on unmanaged servers" on page 308
- "Preparing SA for SA Provisioning" on page 308
- "Preparing SA for patch management" on page 308
- "SA monitoring" on page 308

Customized SA Core configuration files

After installing this release, you will be able modify certain SA Core configuration files and preserve those modification during subsequent core upgrades.

SA preserves configuration files for the following components:

- Data Access Engine (`spin`)
- Web Services Data Access Engine (`twist`)
- Component of the Global File System (`spoke`)

- Software Repository (`word`)
- Command Center (`occ`)
- Deployment Automation (`da`)
- Component of the Global File System (`hub`)
- Command Engine (`way`)
- Model Repository Multimaster component (`vault`)
- Gateways (`opswgw`)

To preserve your modifications, SA creates an empty configuration file named with `_custom` appended to the name of the source file, for example:

- `<component_name>_custom.conf`
- `<component_name>_custom.properties`
- `<component_name>_custom.args`

You can modify these files to override default component configuration specifications, for example:

- `twist_custom.conf` is created for `twist.conf`
- `psrvr_custom.properties` is created for `psvr.properties`
- `waybot_custom.args` is created for `waybot.args`

Configuration files created during SA installation

During upgrade, the installer may revert the configuration files to the default values.To preserve your customizations, you should save them in the custom configuration files of the components. You can find the list below:

- `/etc/opt/opsware/spin/spin_custom.args`
- `/etc/opt/opsware/twist/twist_custom.conf`
- `/etc/opt/opsware/spoke/spoke_custom.conf`
- `/etc/opt/opsware/mm_wordbot/mm_wordbot_custom.args`
- `/etc/opt/opsware/occ/psrvr_custom.properties`
- `/etc/opt/opsware/da/da_custom.conf`
- `/etc/opt/opsware/hub/hub_custom.conf`

- `/etc/opt/opsware/waybot/waybot_custom.args`
- `/etc/opt/opsware/vault/vault_custom.conf`
- `/etc/opt/opsware/opswgw-<gateway_name>/opswgw.custom`

Configuring e-mail alerts

You can configure SA to send e-mail alerts to the SA administrator (or other designated users) when certain conditions are met, such as Managed Server error conditions or Multimaster Mesh conflicts. To do so, your e-mail administrator must configure the SA Core and Managed Servers as Sendmail clients. You should configure e-mail alerts in the SA Client when you install Server Agents on your managed servers.

Setting up SA groups and users

You must assign the necessary access rights and permissions to SA administrators, users, and user groups. For example, to log in to the SA Client, you specify a user name and password. Each user belongs to a user group, and each user group has a set of permissions that control access to features (actions), managed servers, and folders.

Creating SA customers

When you installed the First Core, whether Single Core or Multimaster, you specified a single default SA customer.

Defining software management policies

Software policies allow you to install software and configure applications simultaneously. A software policy can contain packages, RPM packages, patches, application configurations, and other software policies. After creating a software policy, you can attach it to servers or groups of servers. When you remediate a server or group of servers, the patches, packages, RPM packages, and application configurations specified in the attached policy are automatically installed and applied.

Deploying Server Agents on unmanaged servers

After you install a Server Agent on an unmanaged server, it can be managed by Server Automation.

Preparing SA for SA Provisioning

SA Provisioning is a feature that allows you to remotely install and uninstall operating systems (and related configurations, packages, and applications) on your servers. During SA Provisioning, a Server Agent is also installed, allowing the server to be immediately managed.

Preparing SA for patch management

The Patch Management for Windows feature enables you to identify, install, and remove Microsoft® Windows patches. With the SA Client user interface, you can identify and install patches for the Windows 2000, Windows 2003, and Windows NT4.0 operating systems. These patches include Service Packs, Update Rollups, and hotfixes. This feature also supports patching on 64 bit for Windows 2003 operating systems and for 32 bit for Windows XP operating systems.

SA monitoring

SA provides several methods that you can use to ensure that your system is performing correctly:

- **Agent reachability tests**: to determine the current reachability of a specific Agent, you can run a Communication Test in the SA Client to find those servers that have unreachable agents.
- **System Diagnostic tests**: several system diagnostics tests are available in the SA Client that can help you determine that your SA installation is operating correctly and help you troubleshoot when there are problems.
- **Core Component logs**: SA components have logs that can help you troubleshoot problems.

SA Core uninstallation

This section describes how to uninstall a Single Core, remove a core from a Multimaster Mesh, and how to uninstall all cores of a Multimaster Mesh.

Uninstall basics

There are several reasons that you might choose to uninstall an SA Core:

- Removing test installations
- Removing demonstration installations
- Merging or modifying a facility’s Multimaster Mesh Cores
- Decommissioning or moving a facility

Make backups of your Model Repository, Software Repository, and your database of cryptographic material unless you are certain that you no longer need that data, because a complete core uninstallation also removes the Model Repository and the cryptographic material database and permanently deletes all the data. You can preserve the SA data in the Model Repository database by doing a database backup before uninstalling. See the Oracle documentation.

> Note: Before you uninstall an SA Core, you should back up the Oracle database running on the server where that core’s Model Repository is installed. See "Oracle database backup methods".

> Note: The core’s cryptographic material must be available during the uninstallation so that SA Core Components can be fully removed from the environment. If the cryptographic material is not available, the uninstallation will fail.

Procedures for uninstalling Cores

You can perform any of the following uninstallation procedures according to your requirements:

- "Uninstall a single Core"
- "Uninstalling a Secondary Core in a Multimaster Mesh"

- "Uninstalling all Cores in a Multimaster Mesh"
- "Decommissioning a facility"

Uninstall a single Core

A single core can have all components installed on one host or may have some core components installed (distributed) on other hosts. To uninstall a single SA Core, perform the following tasks:

1. Before uninstalling a single core, you must deactivate all servers that host components for that Core using the SA Client.
2. On the server hosting the core's Infrastructure Component bundle, log in as root.
3. Change to the root directory:
   ```
   cd /
   ```
4. Run the `uninstall_opsware.sh` script with the `-r` (specify response file) argument. You need to use the response file created when you installed the SA Core you are uninstalling:
   ```
   <distro>/opsware_installer/uninstall_ opsware.sh -r <response-file>
   ```
   where `<distro>` is the full path to the *Product Software* (primary) media. You must specify the full path the response file.
5. A menu similar to the following appears:
   ```
   Welcome to the Opsware Installer.
   Please select the components to uninstall.
   1 ( ) Software Repository - Content (install once per mesh)
   2 ( ) OS Provisioning
   3 ( ) Slice
   4 ( ) Core Infrastructure Components
   5 ( ) Model Repository, First Core
   6 ( ) Oracle RDBMS for SA

   Select one or more or all components to uninstall:
   ```
   Press `a` to select `all` components. If you must uninstall components one-at-a-time, for example due to a custom installation where core components have been distributed among multiple core component hosts, the components must be uninstalled in the order they appear on the menu above. For example, you would first log on to the SA Provisioning component host, run `uninstall_ opsware.sh -r <response-file>` and uninstall that component, then log into the

Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

You will be asked if you want to preserve the database of Cryptographic Material. If you enter `y`, the directory containing the database will not be removed during the uninstall.

You will also see this prompt:

```
Are you absolutely sure you want to remove users' OGFS home and audit
directories? (home and audit directories will only be removed if they are
stored on the Software Repository server) (y/n)?
```

Select `y` if you want to remove the OGFS home and audit directories. If you press `n`, the directories will not be removed. Note that, if you have placed the OGFS home and audit directories on a server other than the server hosting the Software Repository, the uninstall will not remove those directories even if you press `y`.

6. After you have uninstalled all core components, you should remove the `/var/opt/opsware/install_opsware` directory.

> If you specified during the uninstall that you want to preserve the database of cryptographic material, you should not delete the `/var/opt/opsware/crypto` directory. This directory contains the database of your cryptographic material.

Uninstalling a Secondary Core in a Multimaster Mesh

> Note: Do not uninstall the First Core (primary core) unless you plan to uninstall the entire Multimaster Mesh and all its cores. "Uninstalling all Cores in a Multimaster Mesh". This section describes only uninstalling Secondary Cores from a Multimaster Mesh.

To uninstall a single Secondary Core in a Multimaster Mesh:

1. Log in to any SA Client available for that Mesh.
   a. If the Secondary Core to be uninstalled has a Data Access Engine that is currently serving as the Primary Data Access Engine for the core, you must first assign a Data Access Engine in another Core to serve as the Primary Data Access Engine.
   See the Reassigning the Data Access Engine to a Secondary Role section in the SA 10.60 Administration Guide.

   b. Verify that all transactions have propagated to the other facilities in the Multimaster Mesh. For more information about verifying transaction traffic, see "Install SA first (primary) core with a secondary Core (multimaster mesh)".

2. Decommission the facility for the core you will uninstall.
   a. See "Decommissioning a facility".
   b. On the *Infrastructure Component bundle host* in the core you are decommisioning, run the following command:

      ```
      /opt/opsware/bin/python2
      <distro>/opsware_installer/tools/reload_vaults.pyc --certfile
      /var/opt/opsware/crypto/gateway/spin.srv
      ```

      where `<distro>` is the full path to the *Product Software* (primary) media. Successful output will be similar to this:

      ```
      Core ID Peers IDs Known To This Core
      ------- --------------------------------
      <nnn> <nnn>
      ```
3. Stop and start the *Model Repository Multimaster Component* in all cores, except for the core that you will be uninstalling, by entering the following command as root on Infrastructure Component bundle host(s):
   ```
   /etc/init.d/opsware-sas stop vaultdaemon
   /etc/init.d/opsware-sas start vaultdaemon
   ```
4. Stop the Command Center (OCC) component (part of the Slice Component bundle). Log in as root to a Slice Component bundle host and enter the following command:
   ```
   /etc/init.d/opsware-sas stop occ.server
   ```
5. Stop all *Data Access Engines* (part of the Infrastructure Component bundle).
   Log in as root to the Infrastructure Component bundle host and enter the following command:

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

> Note: If the Command Center and the Data Access Engine are installed on different servers, you must also run the `stop spin` command on all Slice Component bundle hosts.

6. Stop the *Model Repository Multimaster Component*.
   Log in as root to the Infrastructure Component bundle host and enter the following command:

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

7. On the Infrastructure Component bundle host, stop and start the *Data Access Engine* that serves as the **Primary** Data Access Engine by entering the following commands as root:

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

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

8. On Infrastructure Component bundle host for the core to be uninstalled, log in as root.

9. Change to the root directory:

   ```
   cd /
   ```

10. Run the `uninstall_opsware.sh` script:

    ```
    <distro</opsware_installer/uninstall_ opsware.sh -r <response-file>
    ```

    where `<distro>` is the full path to the mounted media.

11. At the components prompt, select one or more or all components to uninstall:

    ```
    Welcome to the Opsware Installer.
    Please select the components to uninstall.
    1 ( ) OS Provisioning
    2 ( ) Slice
    3 ( ) Infrastructure
    2 ( ) Model Repository
    1 ( ) Oracle RDBMS for SA
    ```

    Select a for all. If you want to uninstall components separately, they must be uninstalled in the order they appear on the menu above. To do so, enter the number of the component to uninstall. For example, you would first log on to the SA Provisioning component host, run `uninstall_opsware.sh -r <response-file>` and uninstall that component, then log into the Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

12. You will be asked if you want to preserve the database of Cryptographic Material. If you respond y, the directory containing the database will not be removed during the uninstall.
    You will also see this prompt:

    Are you absolutely sure you want to remove users' OGFS home and audit directories? (home and audit directories will only be removed if they are stored on the Software Repository server) (y/n)?

    Enter `y` if you want to remove the OGFS home and audit directories. If you enter `n`, the directories will not be removed. If you chose to place the OGFS home and audit directories on a server other than the server hosting the Software Repository, the uninstall will not remove those directories even if you enter `y`.

> Requirements: If you installed the core using Custom Mode, it is important that you uninstall the components in the reverse order that they were installed.

13. After the uninstall has completed, remove the `/var/opt/opsware/install_opsware` directory.

> Requirements: If you specified during the uninstall that you want to preserve the database of cryptographic material, you should *not* delete the `/var/opt/opsware/crypto` directory. This directory contains the database of cryptographic material.

Uninstalling all Cores in a Multimaster Mesh

To uninstall all cores in a Multimaster Mesh:

1. Stop the Command Engine (OCC) by logging on as root to a Slice Component bundle host and enter the following command:
   ```
   /etc/init.d/opsware-sas stop occ.server
   ```
2. Stop the Data Access Engine (`spin`).
   Log in as root to the Infrastructure Component bundle host and enter the following command:
   ```
   /etc/init.d/opsware-sas stop spin
   ```
   If the Command Engine and the Data Access Engine are installed on different servers, you must also run the `stop spin` command on the Slice Component bundle host(s).
3. Stop the Model Repository Multimaster Component in all cores by logging in to all Infrastructure Component bundle hosts and running the following command as root:
   ```
   /etc/init.d/opsware-sas stop vaultdaemon
   ```
4. In each core, uninstall all SA components on the hosts on which they are installed. On the servers hosting the components to be uninstalled, log in as root.
5. Change to the root directory:
   ```
   cd /
   ```
6. Run the `uninstall_opsware.sh` script:
   ```
   <distro>/opsware_installer/uninstall_ opsware.sh -r <response-file>
   ```
   where `<distro>` is the full path to the mounted media.
7. At the components prompt, select one or more or all components to uninstall:
   ```
   Welcome to the Opsware Installer.
   Please select the components to uninstall.
   1 ( ) OS Provisioning
   ```

```
2 ( ) Slice
3 ( ) Infrastructure
2 ( ) Model Repository
1 ( ) Oracle RDBMS for SA
```

Select a for all. If you want to uninstall components separately, they must be uninstalled in the order they appear on the menu above. To do so, enter the number of the component to uninstall. For example, you would first log on to the SA Provisioning component host, run `uninstall_opsware.sh -r <response-file>` and uninstall that component, then log into the Slice Component bundle host and run the uninstall script to remove that component, and so on down the list.

You will be asked if you want to preserve the database of Cryptographic Material. If you respond `y`, the directory containing the database will not be removed during the uninstall.

You will also see this prompt:

```
Are you absolutely sure you want to remove users' OGFS home and audit
directories? (home and audit directories will only be removed if they are
stored on the Software Repository server) (y/n)?
```

Enter `y` if you want to remove the Global File System (OGFS) home and audit directories. If you enter `n`, these directories will not be removed. If you placed the OGFS home and audit directories on a server other than the server hosting the Software Repository when you installed the core, the uninstall script will not remove those directories even if you enter `y`.

> Requirements: If you installed the core using Custom Mode, it is important that you uninstall the components in the reverse order that they were installed.

8. After the uninstall has completed, remove the `/var/opt/opsware/install_opsware` directory.

> Caution: If you specified during the uninstall that you want to preserve the database of cryptographic material, you should *not* delete the `/var/opt/opsware/crypto` directory. This directory contains the database of cryptographic material.

Decommissioning a facility

> Caution: Performing this procedure does not shut down or uninstall SA in a facility. Decommission facilities with care, because this task cannot be undone.

When you decommission a facility, the facility is still listed in the SA Client; however, it is grayed out. After a short name is used, even if it is decommissioned, that name cannot be reused.

1. To decommission a facility with the SA Client, perform the following steps.
2. From the SA Client navigation pane, select the Devices tab, then select All Managed Servers. This displays all your managed servers.
3. Locate and select the server that is running the core for the facility you want to decommission. You must first deactivate the SA Agent on this server.
4. Select the **Actions** menu or right-click and select **Deactivate Agent**. This deactivates the SA Agent on that server.
5. Select the Administration tab, then select Facilities. This displays all your facilities.
6. Select the facility that you want to decommission.
7. Select the **Actions** menu or right-click and select **Decommission**.
8. Confirm your selection. This decommissions the facility.

> Note: After you have deactivated a facility, you must delete the deactivated core host. This prevents system diagnostic errors.

Removing a decommissioned facility

When you decommission a facility, the facility is still listed in the SA Client; however, it is grayed out. You can remove a facility by performing the following steps:

1. From the SA Client navigation pane, select the Devices tab, then select All Managed Servers. This displays all your managed servers.
2. Remove all the servers which are managed by the facility you want to delete.
3. All customers attached to the facility must be removed before the Facility can be removed.
4. Stop all services on the core servers that are part of the facility which will be deleted.
   ```
   /etc/init.d/opsware-sas stop
   ```
5. Select the Administration tab, then select Facilities. This displays all your facilities.
6. Select the facility you want to remove.
7. Select the Actions menu or right-click and select Delete.
8. Confirm your selection. This deletes the facility.

9. Restart Model Repository Multimaster component on the primary core infrastructure server
   ```
   /etc/init.d/opsware-sas restart vaultdaemon
   ```
10. On the primary core infrastructure server, remove the entry corresponding to the facility you just removed from the following file:
    ```
    /etc/opt/opsware/opswgw-mgw-<primary_facility_name>/opswgw.custom
    ```
    The line will look similar to:
    ```
    opswgw.ForwardTCP=<port>:<removed_facility_name>-mm:<secondary_core_db>:<db_
    port>
    ```
    For example: `opswgw.ForwardTCP=20002:SLAVE-mm:192.168.100.3:1521`

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Install Guide (Server Automation 10.60)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!