



HP

Data Center

Automation

Appliance

Installation and Administration Guide -
Version 1.00
April 2015

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

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

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

Support

Visit the HP Software Support Online website at:

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

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

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online website:

http://h20230.www2.hp.com/sc/support_matrices.jsp

You can also download the *HP DCAA Support and Compatibility Matrix* for this release from the HP Software Support Online Product Manuals website:

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

Documentation Updates

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

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

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details. See Documentation Change Notes for a list of any revisions.

Operations Orchestration Documentation – Reference Table

The following table is a guide to the available documentation for Operations Orchestration. Major OO activities with DCAA will include: Getting started using OO, Installing OO Studio, Authoring new OO content and more.

Please refer to this table to access the OO related topics for DCAA.

Reference Table - Operations Orchestration Documentation

| Tasks | Document Name | Topic | Page | Link to Doc |
|--|--------------------|---|------|--------------------|
| Get started with OO, understand the personas, component and concepts | Concepts Guide | | | go |
| How to install OO Studio | Installation Guide | Installing HP OO Studio Using the Installation Wizard (Windows) | 34 | go |

| Tasks | Document Name | Topic | Page | Link to Doc |
|--|----------------------------|---|----------|--------------------|
| Manage OO Central settings | Central Guide | Setting up the System Configuration | 26 | go |
| Getting started with OO Studio Start authoring new content | Studio Guide | Getting Started with HP OO Studio – Major Steps in the Workflow | 21 | go |
| Installing HP OO Studio | Installation Guide | Installing HP Operations Orchestration | 8 | go |
| Uninstalling HP OO Studio | Installation Guide | Uninstalling HP Operations Orchestration Studio | 43 | go |
| Understanding RAS and Worker Groups | Concepts Guide | Worker Groups | 25 | go |
| Extending execution coverage <ul style="list-style-type: none"> Execute dotNET operation Execute across FW or on remote networks | Architecture Guide | Architecture Guide (RAS section) | 7 | go |
| Handle certificates changing and other security aspects | Hardening Guide | | | go |
| Purge execution data using Purging Flows | OnBoarding Purging Flows | Purging execution data | 3 | go |
| Purge execution data using OO REST API | API Guide | <ul style="list-style-type: none"> PurgeDebuggerExecutionEvents PurgeExecutionStepData,InputsandOutputs | 63 64 | go |
| See the full HP OO Documentation & Videos | Documentation Library List | | | go |

Server Automation Documentation – Reference Table

The following table is a guide to the available documentation for Server Automation (v.10.2). Major SA activities with DCAA will include: application configuration, using the SA client to manage servers, server patching, and more. Please refer to this table to access the SA related topics for DCAA.

Reference Table – Server Automation Documentation

| Tasks | Document Name | Link to Doc |
|--|---|--------------------|
| Contains information about using SA for application configuration and includes a CML primer and reference information as well as tutorials for creating templates and configurations using XML or CML. | User Guide: Application Configuration | go |
| Contains information about setting up audit rules to locate noncompliant servers and how to bring them back into compliance. | User Guide: Audit and Compliance | go |
| Contains information about uploading, viewing and managing native Chef Cookbooks and running Chef Recipes without having to deploy parallel Chef infrastructure. | User Guide: Chef Cookbook Management | go |
| Contains information about using SA to provision operating systems and environment configurations to managed servers. | User Guide: Provisioning | go |
| Contains information about using the SA Client to manage servers, install server agents, execute scripts, and use the SA Global Shell (OGSH). | User Guide: Server Automation | go |
| Contains information about using SA for policy-based software management. Activities include: defining software policies, attaching software policies to servers, installing and uninstalling software, remediating servers against software policies, and running compliance scans. | User Guide: Software Management | go |
| Contains information about using SA to manage Virtualization Services, including VMware vCenter Server and Microsoft SCVMM, create and manage virtual machines, and virtual machine templates. | User Guide: Virtualization Management | go |
| Contains information about downloading and applying patches to Linux, Windows, and Solaris systems. | Users Guide: Server Patching | go |
| See the full HP SA Documentation Set | All Manuals Download - SA 10.20 | go |

Contents

| | |
|--|----|
| Operations Orchestration Documentation – Reference Table | 3 |
| Server Automation Documentation – Reference Table | 4 |
| Installation Procedure Using the DCAA Installer | 8 |
| Best Practices | 8 |
| Downloading and Installing DCAA | 9 |
| Deploy OVF Template | 9 |
| Virtual Snapshot | 12 |
| Starting DCAA..... | 12 |
| Default DCAA login information | 12 |
| Post installation Tasks | 13 |
| Configure and Publish the Offerings..... | 14 |
| Configure DHCP on the Appliance..... | 15 |
| Configure Media Server..... | 16 |
| Update/Create Build Plans..... | 16 |
| Create a New Build Plan | 17 |
| Manipulate OVF Properties | 18 |
| Migrations – Upgrading from SAVA 10.0x to DCAA 1.0 | 19 |
| Overview | 19 |
| Adding vCenters Manually | 22 |
| Offerings | 24 |
| Provision Servers | 24 |
| Server Policy Remediation | 24 |
| Manage Servers..... | 24 |
| Install Server Automation Agent | 24 |
| Provision Servers | 24 |
| Provisioning a Network booted un-provisioned server..... | 24 |
| Server Policy Remediation..... | 30 |
| Manage Servers | 31 |
| Requesting Manage Servers | 31 |
| Install Server Automation Agent..... | 32 |
| Publish Service Offering | 32 |
| Integrations..... | 32 |

| | |
|---|----|
| DCAA Integration with Cloud Service Automation..... | 32 |
| DCAA Integration with Operations Orchestration | 33 |
| Setting up DCAA with an OO Integration..... | 33 |
| OO Purge Flows..... | 36 |
| Appliance Support and Maintenance..... | 37 |
| Custom Attributes..... | 37 |
| Certificate import for V12N..... | 37 |
| Support | 38 |
| Appliance Updates and Patches | 38 |
| Log collection for support | 38 |
| Update mechanism | 38 |
| OO Password Change Policy | 39 |
| DCAA high-availability (HA) and disaster recovery (DR)..... | 40 |

DCAA - Introduction

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

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

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

Installation Procedure Using the DCAA Installer

This is the overall procedure for downloading, preparing, deploying, and starting the HP Data Center Automation Appliance (DCAA).

To install the HP Data Center Automation Appliance (DCAA), you will perform the following steps:

- Install the VMware vSphere client
- Download the installation package including the split OVA files, the MD5 checksum files and the HP-DCAA-Express installer.
- Reassemble the appliance OVA file using the Installer.
- Deploy the template
- Start the appliance so that it completes its first time setup and is ready to use

IMPORTANT: HP recommends that you take a virtual machine snapshot *before* starting the appliance for the first time. Also, before taking a snapshot, then powering on DCAA, verify the date and time are set properly on your VM host system. Be sure to maintain an accurate time on the host system, such as with NTP, because the VM guest will synchronize with that time.

Best Practices

HP recommends following industry-standard high availability and disaster recovery methods and practices, especially when working with mission-critical IT systems. For detailed information, please see the section titled, [“DCAA high-availability \(HA\) and disaster recovery \(DR\)”](#) in this guide.

Downloading and Installing DCAA

This is the step-by-step procedure for downloading, preparing, and deploying the HP Data Center Automation Appliance (DCAA).

1. Download all files that make up the HP DCAA. This set includes the split OVA files, MD5 checksum files, documentation, and the HP DCAA Express Installer.
2. Create a folder that will hold the reassembled OVA file.
3. Launch the HP DCAA Installer by opening the “**hp-dcaa-Express.exe**” file.
4. Select English, Japanese or Simplified Chinese language for the installer user interface. Click **OK**.
5. The Installer will open; Click **Next**.
6. Select the target folder that you created in Step 2 for the complete OVA file, i.e. the target folder.
7. Click **OK** to select.
8. Click **Install** to finish installing the OVA file.
9. The installer verifies all prerequisites necessary for application reassembly of the split OVA file are installed. (Note: the ‘Perform Integrity Check’ box is pre-selected by default.
10. Click Reassemble.
11. The Setup reassembles all files for the appliance and will output a ‘Reassembly completed’ message once finished.
12. The OVA file is now complete. Click **Next**.
13. Please Note the location of the virtual machine files in the target folder. You should see an output file will be name **DCAA-1-0.OVA**.
14. Click **Finish**.
15. Now, navigate to the target folder which contains the OVA file. Note that it now contains a single OVA file called **DCAA-1-0.OVA**. You are ready to deploy the OVF template.

Deploy OVF Template

When the template file is successfully created, it can be deployed on VMware ESXi 5.x. Before you begin, make sure you have the following information available, needed for the appliance:

| REQUIRED | |
|------------|---|
| IP address | A static IPv4 address that will be assigned to the appliance. A DHCP-assigned address for the appliance is not supported. |
| Gateway | Network gateway |
| Netmask | Network mask |
| DNS | One or more DNS servers. Multiple entries can be separated using a comma. |

| | |
|-----------------|--|
| root password | Password for the appliance root account. |
| OPTIONAL | |
| vCenter IP | One or more IPv4 address of (a) Windows vCenter to be managed by the appliance. The vCenter(s) can also be added at a later time through the Server Automation interface. It enables the creation of VMs using this vCenter directly from the appliance interface in your VMware ESXi environment. |
| vCenter user | Username and password for the vCenter admin user. |
| SMTP host | SMTP host for job email notification. |

The next steps are to start the VMware vSphere client and then deploy the OVF template within your ESXi environment.

1. Start the VMware vSphere client.
2. On the menu bar, select **File**, then **Deploy OVF Template**.
3. Click **Next**.

The vSphere Client **Deploy OVF Template** installer will now take you sequentially through the following installation steps, which are visible on the left sidebar of the installer:

- OVF Template Details
 - End User License Agreement
 - Name and Location
 - Host / Cluster
 - Resource Pool
 - Disk Format
 - Properties
 - Ready to Complete.
4. **OVF Template Details:** This screen shows details of the template such as Product, Version, Vendor, Publisher, Download Size, Size on Disk available (based on how the application is provisioned), and the template Description.
 5. Read the End User License Agreement. Click **Accept**, then click **Next**.
 6. On the **Name and Location** screen: Specify the **Name** and **Location** for the deployed template.
 7. Select an **Inventory** location.
 8. Select the text in the **Name** window, which defaults to **HP Data Center Automation appliance**, and re-name the appliance.
 9. Click **Next**.
 10. On the **Host/Cluster** screen: select a cluster in which you want to run the deployed template.
 11. Click **Next**.
 12. On the **Resource Pool** screen, select a Resource Pool within which you want to deploy the template.
 13. Click **Next**.
 14. On the **Storage** screen, select a storage location where you want to store the virtual machine files.

15. Click **Next**.
16. On the **Disk Format** screen, there are three options: **Thick Provision, Lazy Zeroed**; **Thick Provision, Eager Zeroed**; and **Thin Provision**. It is recommended that you select **Thin Provision**, then click **Next**.
NOTE: for maximum performance, you may choose a **Thick Provisioning** option, however this will require more system resources.
17. On the **Network Mapping** screen, select the Network for the deployed template, then click **Next**.
18. The **Properties** screen has several selections to complete:
 - a. Enter the **Host Name**.
 - b. Enter the **IP Address**.
 - c. Enter the **Gateway**.
 - d. Enter the **Subnet Mask**.
 - e. Enter the **DNS Servers**, with multiple server addresses separated by a comma.
 - f. Enter the Root password.
 - g. Scroll down for more properties; **vCenter** and SMTP are *optional* properties.
 - h. Click Next.

NOTE: Regarding the two optional properties:

The '**vCenter**' is used to register one or more **vCenter** servers to enable the use of the SA V12N feature to deploy and manage virtual machines using the OOTB DCAA virtual server provisioning offering.

SMTP server is the IP or hostname of a specific SMTP server to use, in case SA's use of the default value 'smtp' does not work. See the *Server Automation Administration Guide*, section "[Configuring the Mail Server for a Facility](#)". You can find a link to this document in the [SA Documentation](#) section of this guide.

19. On the **Ready to Complete** tab, review your configuration, then click **Finish** to start the deployment.
20. NOTE: the selection box 'Power on after deployment' is un-checked. **Do not** check this box, as you should take a snapshot first **BEFORE** you power on the virtual machine.
21. A status window will appear during deployment showing progress. Please be patient; this process can take several minutes to an hour.
22. You will get a status message, '**Deployment Completed Successfully**' once the deployment is successful.
23. Click **Close**
24. Locate the deployed appliance; (NOTE: vSphere will show it under Home → Inventory → VMs and Templates.)
25. This concludes the deployment phase. You are now ready to run the HP DCAA.

Virtual Snapshot

After you have deployed the appliance, and before turning the appliance on for the first time, it is important to capture a system snapshot. This allows you to go back to an earlier state in the appliance if you encounter any issues.

1. Right click on deployed DCAA appliance to open the context menu.
2. Navigate to **Snapshot**, then click on **Take Virtual Snapshot** before starting the appliance for the first time.
3. In the **Take Virtual Machine Snapshot** window, enter a snapshot name, then click **OK**. You can also enter a short description of the snapshot.
4. Once you click OK, vSphere will create a snapshot. In the vSphere **Recent Tasks** window, click on **Create VM Snapshot** to check that the snapshot has been created successfully.

Starting DCAA

Important: Before powering on DCAA for the first time, verify that the date and time are properly set on the VM host system. Maintain an accurate time on the host system, such as Network Time Protocol (NTP), as the VM will synchronize with that time.

1. Right click again on the deployed DCAA appliance to open the Context menu.
2. Select **Open Console** to open the console window.
3. Click on the green **Play** button to start the appliance. The appliance starts, configures the networking and starts its first time setup configuration.
4. The appliance will now run through a series of checks and self-tests during initialization. This will take between 15 and 30 minutes.
5. Once initialized, the appliance is ready to be used.
6. You will see a login screen appear at the console prompt.

Default DCAA login information

- The Management Console is available at: <https://<appliance>:8444/csa>
- (username: **admin** / password: **cloud**)
- The IT Operations portal is available at: <https://<appliance>:8079>
- (username: **consumer** / password: **cloud**)

The Operations Orchestration portal is available at: <https://<appliance>:8443/oo>

- (username: **admin** / password: **admin**)
- The Server Automation client can be downloaded from <https://<appliance>>.
- Click on the “Download HP launcher” link and install the SA client.
- (username: **admin** / password: **opsware_admin**)

Post installation Tasks

After the First Time Setup completes, the following steps must be performed:

- [Configure and Publish the offerings](#)

In order to provision servers the following steps must be performed:

- [Configure DHCP on the Appliance](#)
- [Configure the Media Server](#)
- [Update/Create Build Plans for the Desired Operating Systems](#)
- [Create a New Build Plan](#)

Once these steps are completed and your servers are provisioned, the appliance is fully ready to be used.

Other Post-Installation tasks that need to be done initially:

- Setting up and defining Server Automation (SA) [Software Policies](#) and [Patch Policies](#)
- You may be a current [SAVA 10.x customer](#) looking to migrate to HP DCAA
- You may need to [add a vCenter manually](#)
- Every user will want to know [how to redeploy DCAA](#) using the initial appliance snapshot

Please see the below sections for more information on these topics.

SA Software Policies

For more information on how to create software policies and manage packages, see the *SA User Guide: Software Management*: Chapter 2 – **Creating and Managing Software Policies**, and Chapter 3 - **Managing Software Packages**. You can find a link to this document in the [SA Documentation](#) section of this guide.

SA Patch Policies

In order to patch the managed servers, the patch metadata database and patches need to be imported and patch policies defined. For more information consult the *SA User Guide: Server Patching*. You can find a link to this document in the [SA Documentation](#) section of this guide.

SAVA Migration Customers

Current SAVA 10.x customers looking to migrate will want to see the topic: [Migrations – Upgrading from SAVA 10.0x to DCAA 1.0](#) in this guide for more information.

Adding vCenters

In case a vCenter was not provided during the appliance deploy or if another vCenter needs to be added under DCAA management, please follow the steps shown in the section: [Adding vCenters Manually](#) in this guide.

Re-deploy DCAA using OVF Properties

After DCAA is setup and deployed, you may want run the re-deploy the appliance from a snapshot using a new configuration. See the topic: [Manipulate OVF Properties](#) in this guide for more information

Configure and Publish the Offerings

To make the offerings available on the **Operations Portal**, they first need to be configured and published. In order to use the Provision Servers offering to create new virtual machines, it must be configured with your vCenter details.

The following steps should be performed to publish an offering:

- Connect to the Management Console (<https://<appliance>:8444/csa>)
- Click on Offerings
- Click on the desired offering
- Review the offering configuration, by accessing the Options tab. For the *Provision Servers* offering it is mandatory to configure the New Virtual Servers section with appropriate values for the vCenter (e.g. Datastore, inventory folder, network name). Save your changes before you continue.
- NOTE: The VMware virtual server provisioning will work only if virtualization is *pre-configured*.
- Access the Publishing tab and click on the Publish button to make the offering available on the Operations Portal. Select the category “Server Management” and then click Publish.

Configure DHCP on the Appliance

The DHCP Network Configuration Tool for IPv4 is installed on the appliance.

Perform the following steps to configure networks for Provisioning:

Log in as root on the appliance.

(Optional) Make a backup copy of the configuration file with the following commands:

```
cd /etc/opt/opsware/dhcpd cp dhcpd.conf dhcpd.conf.orig
```

Run the DHCP Network Configuration Tool with the following command:

```
/opt/opsware/dhcpd/sbin/dhcpdtool
```

The following DHCP Network Configuration Tool main menu appears:

```
Current Configuration: Full DHCP Management
Select New Configuration:
 1) Full DHCP Management
 2) Disable All DHCP Management
 q) Quit Without Configuration Changes
Choice [1-3, q]: █
```

1. To perform full DHCP Management, enter ‘1’ at the selection prompt;
2. To Disable All DHCP Management, enter ‘2’ at the prompt;
3. To Quit without configuration changes, enter ‘q’ at the prompt.

To add a new network, enter ‘a’ at the Opsware DHCP Network Configuration Tool prompt:

```
Opsware DHCP Network Configuration Tool
Editing DHCP information for 192.168.33.0/27 (255.255.255.224)
All values which prompt for an address accept either a IP or a hostname.
Enter the DHCP Range (start address, stop address)
: 192.168.33.3, 192.168.33.23
Enter the DNS server(s) (comma separated)
: 192.168.162.139, 192.168.163.142
Enter the DNS domain: opsware.com
Would you like to add the IPs from DHCP range in /etc/hosts ? (y/n): █
```

- To configure the DHCP service on the local network, enter '1' at the prompt. Local networks are detected automatically and displayed.
- If you are adding a local network, you need to enter the IP addresses or host names of the DHCP range and the DNS servers. Note that the IP addresses are separated by a comma and a space.
- If the displayed information is correct, enter 'k' to keep the network and return to the main menu.
- At the main menu, to save the information you have entered, enter 's' ; Or
- To edit a configured network, enter the corresponding integer and return to step 3.
- To exit the DHCP Network Configuration Tool, enter 'e'. You are prompted to start (or restart) the DHCP server process.
- To start (or restart) the DHCP server process, enter 'y'. The DHCP Network Configuration Tool displays diagnostic output as part of its start-up.

Configure Media Server

To perform OS provisioning tasks, a media server that hosts the installation media for the desired Operating Systems is required.

For more information on setting up the media server, please consult the [Provisioning User Guide, Chapter 2: Performing SA Provisioning in Server Automation Documentation](#).

Update/Create Build Plans

Before server provisioning can be performed, Build Plans for the desired operating system needs to be created. In order to have Build Plans that will be filtered correctly in the Operations Portal, it is recommended to copy the templates available from the SA Library located in `/Opsware/Tools/Build Plans/SAVA`.

NOTE: the supplied build plans have the required custom attributes for filtering on NGUI. User created Build Plans should be placed in `/Home/CommonCustomerBuildPlans` under the corresponding folder (in the ProLiant folder place Build Plans customized for provisioning ProLiant systems, Non-ProLiant/OS family folder for others).

Create a New Build Plan

These are the steps you must follow to create a new Build Plan:

- Start the SA client and access the **Library**
- Select the “**By Folder**” tab and navigate to the corresponding subfolder in:
/Home/CommonCustomerBuildPlans
- Right click and select **New > OS Build Plan**
- Provide a name for the Build Plan; this name will appear in the Operations Portal.
- Click on **Build Plan Items** and click on the **Copy Plan** button
- Select a Build Plan for the desired Operating system from one of the subfolders of:
/Opware/Tools/Build Plans/SAVA
- Configure the “Set Media Source” step in the build plan; then, click on the “Set Media Source” step.
- Set the **Parameters** field to a working network share that contains the media for the Operating System.
- For Windows Operating Systems, a **Product Key** needs to be provided.
- Click on the **Custom Attributes View**, in the left side of the window. The Custom Attributes should be defined as per the previous comment.
- Input a valid key for the desired Windows version in the **Product Key** attribute row. *(Optional, for Windows build plan only)*
- Save changes from **File > Save** or typing **CTRL+S**

Manipulate OVF Properties

How to manipulate OVF properties in conjunction with snapshots

This process shows you how to bring up the appliance in various mode/configuration(s).

If the user has taken a snapshot BEFORE starting the appliance for the 1st time, then it is possible to re-deploy the appliance from a 1st time startup again. It is also possible to bring up the appliance multiple times with different settings. This is why the snapshot is so important, as you can use the snapshot as a fresh starting point for the appliance and change the mode and configurations of the appliance.

The procedure for *deployment* is:

- Import the appliance using Deploy OVF template.
- Follow the wizard and configure the appliance.
- Take a snapshot.
- Run the appliance
- Try it out

Then, to run a *redemption* of the appliance from the snapshot:

- Revert to the snapshot that was taken before the 1st appliance start.
- Open the appliance settings; click on the appliance.
- Click on '**Getting Started**'; click on '**Edit virtual machine settings**'.
- Navigate to the **Options** tab, select **vApp options / Properties** on the left pane.
- Edit the properties.
- Save the new settings.
- Take a **new snapshot** before your 1st start
- Run the appliance
- Try it out with your new configuration.
- If you want to change the configuration again, start the same process over from the beginning to re-deploy again. You can repeat this procedure as many times as necessary.

Migrations – Upgrading from SAVA 10.0x to DCAA 1.0

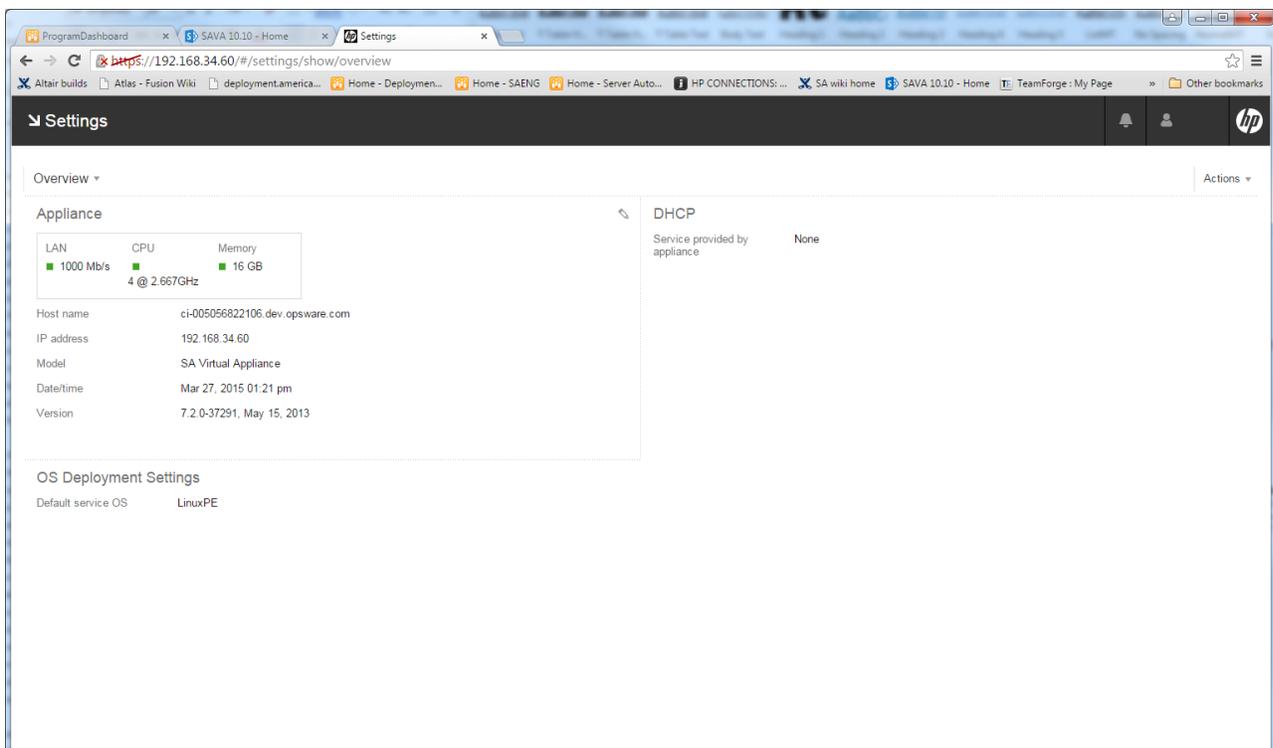
Note: Before starting, make sure you have the network information for the SAVA appliance available. The new DCAA appliance must be deployed with the same IP as that used by SA (not the appliance IP) on the SAVA appliance.

Overview

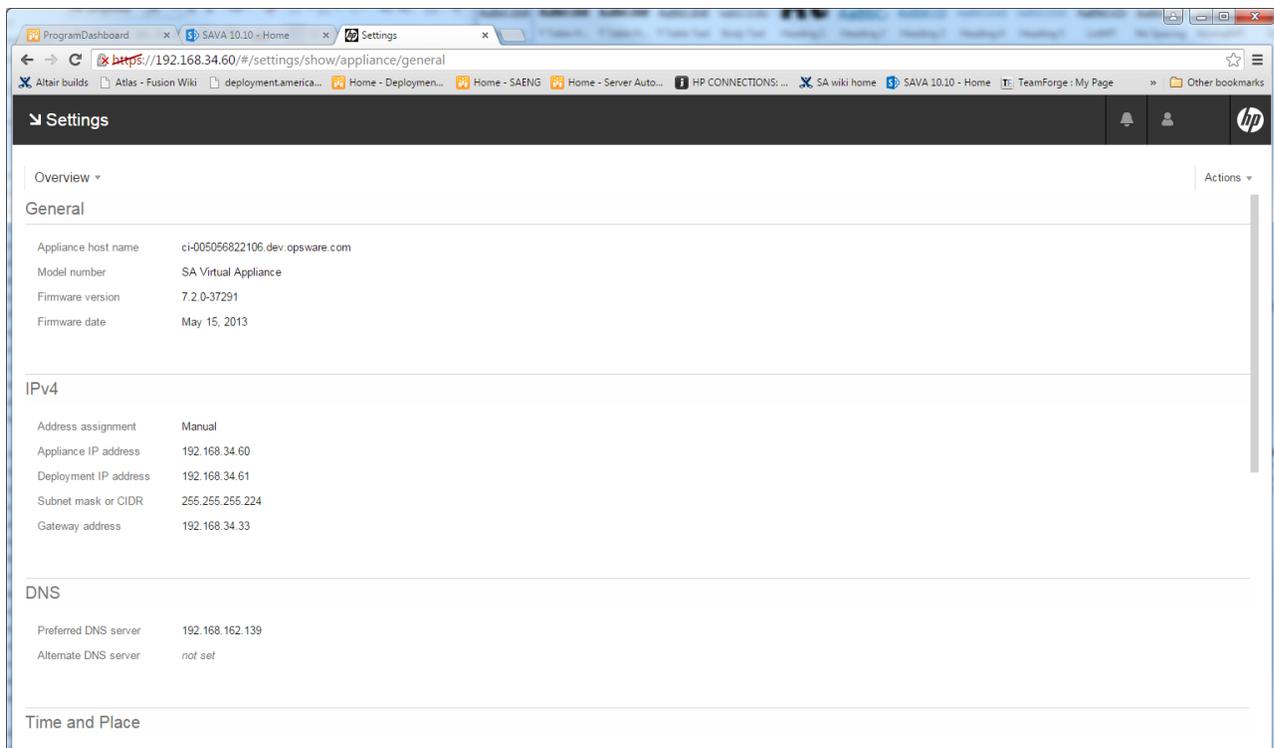
The steps to finding the SA IP address in SAVA are as follows:

1. Navigate to the SAVA appliance address on your system: `http:// <SAVA appliance IP>`.
2. Login using the Administrator user account and password.

Once logged in you will see:



Then, Click the **Overview** and select **Appliance**:



Then, notice that the SA IP address is the **“Deployment IP address”**, i.e. in this example, it is 192.168.34.61.

Migration from a SAVA appliance to DCAA

Migration from a SAVA 10.x appliance to DCAA is done in two steps:

- Export SAVA content
- Import SA content on a deployed DCAA

Important Reminder: Before you start, backup your virtual machine, and then take a snapshot.

The steps are as follows:

1. Export SAVA content

Copy the upgrade media on the `/hpsaxfer` share on the SAVA appliance.

Create an `export.cfg` file in `/hpsaxfer` with the information of a network share, where the export will be placed. The file must contain 2 lines:

- <nfs server> - IP or hostname of an NFS server
- <share path> - a path exported with read/write permissions.

Note: In case the file is created from Windows, make sure to save the `export.cfg` with the End Of Line (EOL) in UNIX format.

The share on the specified NFS server must be exported with read and write permissions, so that the appliance can write the exported files.

Next, you can upgrade SAVA using the upgrade `.bin` file, using this process:

1. In the SAVA user interface **Settings** screen, select **Actions > Update Appliance**.
2. Click **Upload File** and browse to locate the `.bin` file.
3. Double-click the `hpsa_cordpatch_10.20_59710.bin` file to upload it.
4. Once the file upload is complete, click **Install Update** to install the update file.
5. The **End User License Agreement** screen is displayed. After agreeing to the End User License Agreement, the Update appliance dialog is re-displayed.
6. Press **Install Update** a second time to display a notification message with an estimated time for the install update process.
7. Press **Install Update** a third time to display an update progress screen and start the upgrade.

NOTE: The installation will take between 3-5 hours or more if you have a lot of content in the SA database...

When the upgrade and export complete, a message that the upgrade failed is shown and the appliance is reverted back to its original state and reboots.

NOTE: Progress during the export process is written in the `UPGRADE_MSGS` file on the share.

If the export completed successfully, a `DB_EXPORT_SUCCESSFULL` file is created on the provided share.

If the upgrade is reported as failed and there is no file created on the network share, please make sure that the NFS share is exported with write permissions.

2. Import content on a deployed DCAA

- Important Note: bring up the NEW appliance in an isolated VLAN that allows it to have the same IP address!
- Deploy a new DCAA appliance using the OVA file.
- For more information on the Installing OVA files and DCAA Deployment, review the topics [Installation Procedure Using the DCAA Installer](#) and [Downloading and Installing DCAA](#) , and [Deploy OVF Template](#) in this document.

NOTE: Do *not* specify a vCenter to be added during the First Time Setup phase. The information provided will be overwritten when importing the content from the SAVA appliance. Instead, vCenters managed by the appliance need to be added manually. Please see the topic, '[Adding vCenters Manually](#)' in this document regarding how to add vCenters.

- After DCAA is deployed successfully, the content from SAVA can be imported:
- On DCAA, change to the migration tools folder: `cd /var/opt/hp/dcaa/migration/`
- Edit the export.cfg file with the same details used during the export phase.
- Run the import tool: `import_sava1.sh`
- When the import tool completes, DCAA will have the content from SAVA appliance and is ready to be used.

NOTE: Before servers assigned to a Customer imported from SAVA can be used in DCAA, the permissions on that particular customer must be granted to the SuperUsers group.

The upgrade patch/instructions for customers upgrading from SAVA 10.x to DCAA 1.00 will be hosted on your 'My Updates' from the HP Support Organization. Please contact your HP Support Renewal Rep for detailed instructions on how to upgrade from SAVA to DCAA.

Adding vCenters Manually

NOTE: This is the process for bringing vCenter(s) under DCAA management, and is the only way to add vCenter(s) into appliances that have been migrated.

- Install the SA agent on the Windows server where the vCenter runs.
- NOTE: Please make sure you install the agent with full software and hardware registration. Check the “Immediately do full hardware registration” and “Immediately do software registration” options in the Advanced section.
- Add the Virtualization service: go to Virtualization > VMware vCenter > right click on the right pane and select “Add Virtualization Service”.
- Select the server and provide the credentials needed to authenticate with the vCenter.
- After the vCenter is added, in order for operators to use it in the portal, permissions must be granted on the vCenter for the SuperUsers group.

For more information on managing permissions and other virtualization tasks, see the *Server Automation Virtualization Management Guide*: Chapter 2 –**Managing Permissions** and Chapter 5 - **Virtualization Service Tasks**. You can find a link to this document in the [SA Documentation](#) section of this guide.

Offerings

This solution offers the following offerings for server management:

[Provision Servers](#)

[Server Policy Remediation](#)

[Manage Servers](#)

[Install Server Automation Agent](#)

Functionality supported in this solution

Policy remediation and deployment on the managed server involves the following steps:

- Remediate a patch and/or software policy on a server or server group.
- Install software packages on a server
- Attach a patch policy to a managed server hence associating that policy with the server.
- Attach a software policy to a managed server hence associating that policy with the server
- Execute server scripts on a managed server.

Important Note: HP recommends that you make a copy or version of the OOTB base offering or service design (1.0.0) *before* making any modifications. During HP maintenance updates, the 1.0.0 version of any service design or service offering can be updated and overwritten.

Provision Servers

This service offering provisions operating system baselines onto a physical server or multiple virtual servers, allowing you to select from pre-defined options. This is intended to be used by the IT operator to provision servers. The IT operator has the option of choosing to either provision one network booted un-provisioned server at a time or multiple virtual servers on VMware virtualized environments.

Provisioning a Network booted un-provisioned server

This part of provisioning the offering assumes that there is an un-provisioned server in Server Automation (SA) and it can be either a physical server or a virtual server, which can then be provisioned by an IT operator by choosing from available options.

HP Proliant servers offer an advantage in functionality over a third party server. For example, HP Proliant servers have the flexibility of network booting from any service OS in SA and are will still be able to perform any OS

provisioning due to SA's enhanced iLO integration.

Third party or virtualized servers have the limitation of supporting provisioning of only those Oses which are supported by the booted service OS. For example, if a third party or virtual server is booted with a Linux Service OS, then only Linux based OS Build plans are shown on the IT operator portal.

There are seven server options to be chosen by the IT operator: four of them are dynamic, with two among these being optional, and the remaining three are non-dynamic and optional.

The table below details these options:

Dynamic Server Options

| Option | Description |
|------------------------------|---|
| OS Build Plan | <p>A Dynamic List of SA's OS build plans applicable for the selected booted server are shown.</p> <p>For an HP ProLiant server, the OS build plans are listed from 2 folders, "/Opware/Tools/Build Plans/SAVA/ProLiant" and "/Home/CommonCustomerBuildPlans/ProLiant". The first folder has HP supplied build plans and the second one is for customer updated build plans.</p> <p>For a Non-ProLiant or Virtual Server, depending on the service OS, build plans from "Linux" or "Solaris" or "Windows" folder in "/Opware/Tools/Build Plans/SAVA/Non-ProLiant" and "/Home/CommonCustomerBuildPlans/Non-ProLiant" folders are shown. The first folder also has HP supplied build plans and the second one is for customer updated build plans.</p> <p>Non-ProLiant subdirectories:</p> <p>This configuration of entries can be found in the file: \$CSA_HOME/jboss-as/modules/sun/jdk/main/service-loader-resources/sa-provider.properties</p> <pre>hp.sa.osbp.nonproliant.internal.sub.dir.linux=Linux hp.sa.osbp.nonproliant.internal.sub.dir.windows=Windows hp.sa.osbp.nonproliant.internal.sub.dir.solaris=Solaris hp.sa.osbp.nonproliant.customer.sub.dir.linux=linux hp.sa.osbp.nonproliant.customer.sub.dir.windows=windows hp.sa.osbp.nonproliant.customer.sub.dir.solaris=solaris</pre> |
| Un-Provisioned Server | <p>A dynamic list of Un-Provisioned Servers network booted with one of SA's Service OS are shown here. The IT operator has to choose which server to provision.</p> |

Optional Server Options

| <u>Option</u> | <u>Description</u> |
|----------------------------------|---|
| Hostname Prefix | This is optional field can be up to nine characters in length and will appear prefixed to hostname. A hostname is automatically generated if nothing is specified. |
| Attach to a Customer | This is Optional. A Dynamic List of customers defined in SA are shown if chosen and IT operator would then have to choose one. |
| Attach to a Device Group | This is Optional. A Dynamic List of public and static Device Groups defined in SA are shown if chosen and IT would then have to choose one. |
| Send Email Notification | This is Optional. An IT operator can specify an email address to be notified about the status of the provisioning job in SA. Note: This requires that SMTP configuration is setup on the SA side. |
| Attach Ticket ID | This is Optional and when chosen, IT operator can specify a ticket ID of ITIL process for the provisioning job in SA. |
| HP-SA Provider properties | This is Optional. You can provide the name of the SA Provider under: <code>\$CSA_HOME/jboss-as/modules/sun/jdk/main/service-loader-resources/sa-provider.properties</code> |

Provisioning VMware Virtual Servers

This part of the Provisioning Servers offering will allow an IT operator to provision up to 16 servers with the chosen options in one pass, provided at least one VMware vCenter is registered with SA's virtualization service.

This VMware virtual server provisioning part of the service offering has both dynamic and non-dynamic options. The dynamic options for provisioning are listed in the table below:

Dynamic Provisioning Options

| <u>Option</u> | <u>Description</u> |
|----------------------|--|
| Hypervisor | A dynamic list of VMware hypervisors is shown here, from which the IT operator has to choose one where the virtual server(s) would be provisioned. |

| | |
|----------------------------------|---|
| Attach to a Customer | This is Optional. A Dynamic List of customers defined in SA are shown if chosen and IT operator would then have to choose one. |
| Attach to a Device Group | This is Optional. A Dynamic List of public and static Device Groups defined in SA are shown if chosen and IT would then have to choose one. |
| OS Build Plan | A Dynamic List of SA's OS build plans from "Linux", "Solaris" and "Windows" folder resides in the "\Opsware/Tools/Build Plans/SAVA/Non-ProLiant" and "\Home/CommonCustomerBuildPlans/Non-ProLiant" folders. The 2 folders are for HP provided and customer updated build plans. |
| Number of Virtual Servers | The number of virtual servers to be provisioned with the selected options. This can be from 1-16. Note: this number can vary based on a parameter set by the Administrator in vCenter. |
| Number of CPUs | The number of CPUs in the virtual server(s) to be provisioned with the selected options. This can be from 1-32 CPUs. NOTE: This number may also have restrictions in the hypervisor. |
| Memory in MB | The amount of Memory in MB on the virtual server(s) to be provisioned with the selected options. This can be from 512-1000000. NOTE: This number may also have restrictions in the hypervisor. |
| Hostname Prefix | This is an optional field, which can be up to 9 characters in length and will be prefixed to hostname. A hostname is generated if nothing is specified. |
| Datastore | Datastore is where the Virtual Server(s) configuration is stored. This datastore should be accessible by all the hypervisors listed by the hypervisor dynamic option. |
| Inventory Folder | Inventory folder on vCenter where the virtual server(s) will be created. Folder name should be in "/Datacenter/<full path to folder>" format. Example: /<DC1>/Folder1/Folder11, where DC1 is the datacenter name in vCenter. |

| | |
|--|--|
| Attach Custom Server Attributes | If chosen, the IT operator can specify a comma separated list of keys and values. Note: The number of values and keys have to be same. |
| Storage Device Type | The type of storage devices on the virtual server(s) to be created. This is preset to “SCSI, IDE”, which can be changed by the Administrator or an IT operator while subscribing. This can be a single value or a comma separated list, but the number of options selected should match the storage options available; see options listed below. |
| Storage Device Usage Type | The type of storage devices on the virtual server(s) to be created. This is preset to “disk, cdrom”, which can be changed by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |
| Device Capacity | The capacity in GB of storage devices on the virtual server(s) to be created. This is preset to “20, 0”, which can be changed by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |

Apart from the dynamic options listed above, there are some non-dynamic options which can either be preset by the Administrator or selected by the IT operator. The Administrator can control how these non-dynamic options are used, and also whether they are available to the IT operator. The table below lists these options:

Non-Dynamic Provisioning Options

| | |
|---------------------------------|---|
| Storage Device Datastore | The Datastore where the disk(s) of the virtual server(s) to be created will be stored. This can be preset/changed by the Administrator or by IT operator while subscribing. This can be a single value or a comma separated list. This datastore should be accessible by all the hypervisors listed by the hypervisor dynamic option. |
| Storage Device Filepath | This option is needed only when CDROM's are created and is preset to “, /mnt”, specifying that the mount point for the CDROM created. This can be preset/changed by the Administrator or by the IT operator while subscribing. This can be a single value or a comma separated list. |

| | |
|--|---|
| Storage Device Connect at Startup | Boolean values to specify whether the storage devices are connected to the Virtual Server(s) to be created. This is preset to “True, True”, to connect both disk and CDROM at startup and can be changed either by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |
| Storage Device Lazy Allocation | Boolean values to specify whether lazy allocation should be used for the storage devices of the Virtual Server(s) to be created. This is preset to “True, True” and can be changed either by Administrator or by IT operator while subscribing. This can be a single value or a comma separated list. |
| NIC Name | Network Interface Card(s) name(s). This is preset to “eth0”, to add a single NIC on the virtual server(s) to be created and can be changed either by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list, but the number of options should match with the network options, listed below. |
| NIC Key | Network Interface Card(s) key name(s). This is preset to “eth0k”, to add a key for the single NIC on the virtual server(s) to be created and can be changed either by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |
| NIC Network Name | The network name in vCenter to which the NIC(s) on the virtual server(s) to be created, will be attached to and can be changed either by Administrator or by IT operator while subscribing. This can be a single value or a comma separated list. |
| NIC Adapter Type | The type of NIC(s) attached to the virtual server(s) to be created and can be changed either by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |
| NIC Connect at Startup | Boolean values to specify whether the NIC(s) are connected to the Virtual Server(s) to be created. This is preset to “True”, to connect the NIC at startup and can be changed either by the Administrator or by an IT operator while subscribing. This can be a single value or a comma separated list. |

| | |
|--------------------------------|---|
| OS Provisioning Network | The network to be used for provisioning virtual server(s) from SA. This will be one of the key(s) specified in NIC Key Option. |
| Send Email Notification | This is Optional; when chosen, the IT operator can specify an email address to be notified about the status of the provisioning job in SA. Note: This needs SMTP configuration to be setup on SA side. |
| Attach Ticket ID | This is Optional; when chosen, the IT operator can specify a ticket ID of ITIL process for the provisioning job in SA. |

Some of the above non-dynamic options are marked locked and/or invisible by default and can be changed by the Administrator by logging into the **Administrator Portal**, located in the **Options** Tab under the **Provision Servers** Offering by clicking the highlighted icons below. This can be used in scenarios where the Administrator wants to limit certain options for the IT operator.

The screenshot displays the 'Provision Servers' interface with the 'Options' tab selected. Under 'Virtual Server Details', the following options are listed:

| Option | Value | Lock Icon | Eye Icon | Edit Icon |
|------------------------------|--|-----------|----------|-----------|
| 1. Hypervisor | Selectable values will be determined at subscription time. | Locked | Visible | Editable |
| 2. Number of Virtual Servers | 1 | Locked | Visible | Editable |
| 3. Number of CPUs | 2 | Locked | Visible | Editable |
| 4. Memory in MB | 2048 | Locked | Visible | Editable |
| 5. Hostname Prefix | | Locked | Visible | Editable |
| 6. Datastore | CSL-Vdisk003 | Locked | Visible | Editable |
| 7. Inventory folder | /CSL-AO/Test1/Test11 | Locked | Visible | Editable |

For more information about the Provision Servers Offering in DCAA, please reference the “*Provision Servers*” section in the [DCAA Users Guide](#).

Server Policy Remediation

This offering remediates patch and/or software policies on a device group or on an individual server.

Functionality supported in this solution

Server Policy Remediation and deployment on the managed server provides the following features:

- Remediate a patch and/or software policy on a server or server group.
- Install software packages on a server
- Attach a patch policy to a managed server hence associating that policy with the server.
- Attach a software policy to a managed server hence associating that policy with the server
- Execute server scripts on a managed server.

Note: The time taken to remediate a Device Group can vary greatly depending on how many servers the Device Group has and also how much time each of the server remediation will need. Hence the timeout value for waiting for a Device Group remediation to complete is made configurable using a system property called “DCAA_Remediate_DG_Timeout” on OO central.

This property is set by default to 4 hours (expressed as a value in *milliseconds*) and could be changed if needed as per the instructions below. Remember to update the timeout value in *milliseconds*.

1. Login to OO central @ <https://<DCAA-Appliance-IP>:8443/oo>
2. Click on ‘Content Management’, go to “Configuration Items” tab and expand “System Properties”
3. Choose “DCAA_Remediate_DG_Timeout” system property and edit to update the “Override Value” to a desired timeout value in milliseconds

For more information about the Server Policy Remediation Offering in DCAA, please reference the “Server Policy Remediation” section in the [DCAA Users Guide](#).

Manage Servers

This solution is part of the Data Center Automation Appliance that demonstrates how to manage life span of various servers using HP Server Automation. HP Server Automation (SA) provides the ability to manage servers individually or in a device group by *implementing* a well-defined process of remediating and deploying software policies and software packages, bringing HP-SA policy management capabilities into a server environment.

The HP DCAA Manage Servers offering provides support to remediate additional software policies and/or software packages on an individual server. This offering also supports running server scripts on the selected server, and can send email notifications detailing the results of jobs run on the server.

Requesting Manage Servers

As the Administrator, you must complete the following steps to configure **Manage Servers** offering before it can be used for the first time:

- Configure the **Data Center Automation Appliance**
- All servers should have SA agent installed and be recognized as SA managed servers
- Managed servers should be running in SA for this offering to work

For more information about the Manage Servers Offering in DCAA, please reference the “Manage Servers” section in the [DCAA Users Guide](#).

Install Server Automation Agent

Installs the HP Server Automation Agent. This service offering installs the management agent on target servers to be discovered and managed by HP Server Automation for application provisioning and ongoing lifecycle management.

For more information about the *Install Server Automation Agent* in DCAA, please reference the “Install Server Automation (SA) Agent” section in the [DCAA Users Guide](#).

Publish Service Offering

For more information on publishing a Service Offering in DCAA, please reference the “*Publishing*” section in the [DCAA Users Guide](#).

Integrations

DCAA Integration with Cloud Service Automation

This integration allows administrators to use the Server Automation (SA) 10.20 that is part of the DCAA appliance to be configured as the SA provider for a CSA installation. Once configured, the CSA administrator will have access to the provisioning, patching and policy management capability that is already delivered as part of the DCAA bundle.

When configuring the SA provider in the CSA 4.2 instance the hostname of the DCAA appliance must be specified:

- Display Name: HPSA
- User ID: <SA user account> (must be member of SAVA SuperUsers)
- Password: <account password>
- Service Access Point: <https://<DCAA Hostname>:443>

Please see the following guide for information on how to integrate CSA with SA:

HP Cloud Service Automation Integration Pack 4.20 available here:

<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01439648>

DCAA Integration with Operations Orchestration

This integration allows administrators to use the Server Automation (SA) 10.20 that is part of the DCAA appliance to be integrated with flows from an Operations Orchestration (OO) 10.20 installation. Integrating SA and OO makes it possible to use many features available in SA within custom OO flows in order to solve specific customer use cases. The integration would rely on accessing the SA instance using the DCAA hostname and account credentials.

Please see the following guides for information on this Integration:

- HP Server Automation 10.20 Integration Guide available here:
<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01253511>
- HP Operations Orchestration-HP Server Automation Integration Guide available here:
<https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01253511>

Operations Orchestration

Setting up DCAA with an OO Integration

Before you Begin: Make sure the path is set to: `/usr/local/hp/csa/openjre/bin/java`

The following steps needs to be followed for using the HP-SA provider internal to DCAA with an OO environment:

- 1) In the command prompt of the appliance, you can type command: “which java” to discover the path set. If it is not set, then we may need to add the above path to the system variable.
- 2) The following CP jars need to be installed, and can be found in the `HP-DCAA-OOTB.zip` file, which is downloadable directly from the <URL> where the zip file resides. **Note:** The BASE, SA and CSA Integrations CP jars should be installed only if they aren’t already installed on external OO Central. Also for the first three jars, the listed versions are minimum needed and higher versions should also suffice. Make sure you install the content packs (CP) and jars in OO central below in the order listed:
- 3) Install the following Content Packs (CP) and jars in OO:
 - a. Base CP jar (v. 1.3.1)
 - b. HP SA content jar (v. 1.2.0)

- c. CSA CP integrations jar (v.4.50.0)
 - d. DCAA content jar
- 4) Install the jars in OO in the above descending order. All the jars are available in the HP-DCAA-
OOTB.zip file. The zip file can be downloaded from the link <location>.
- 5) Creating an internal user 'admin' for HP OO. In the appliance, run the command below. The internal user
'admin' uses default password as 'admin':

```
curl -X POST -d
'{"password":"admin","roles":[{"name":"PROMOTER"}, {"name":"ADMINI
STRATOR"}, {"name":"SYSTEM_ADMIN"}],"username":"admin","permission
s":"ADMINISTRATOR"}' https://localhost:8443/oo/rest/users --
header "Content-Type: application/json" -k
```

- 6) Configure the CSA_OO internal user Configure the user created in the previous step as a new CSA- OO
user. In order to achieve that, you can run the following command in our appliance from the command
line:

```
curl -X PUT -d 'admin' https://localhost:8443/oo/rest/content-
config/CSA_OO_USER?type=SYSTEM_PROPERTY --header "Content-
Type:application/json" --header "Authorization:Basic
YWRtaW46YWRtaW4=" -k
```

- 7) If you need to configure the user from the OO side, log into OO and configure the user from Content
Management -> configuration items. In configuration items, click on System Properties. We get
CSA_OO_USER with the default value as OoInboundUser. We need to add the value as “admin” in the field
override value. Click save. Now you have setup admin as the override value for the user.
- 8) Configure CSA_REST_CREDENTIALS: In order for CSA to make rest calls to OO, we need to configure CSA
REST credentials. In order to achieve this, we can run the below command in the DCAA appliance
machine:

```
curl -X PUT -d '{"username":"admin","password":"cloud"}'
https://localhost:8443/oo/rest/content-
config/CSA_REST_CREDENTIALS?type=SYSTEM_ACCOUNT --header
"Content-Type:application/json" --header
"Authorization:Basic YWRtaW46YWRtaW4=" -k
```

9) Ideally, you can log into OO and configure the credential from within OO. You need to go into Content Management → Configuration Items. In configuration items, click on System Account. Find `CSA_REST_CREDENTIALS`, and then edit the user name and password to match the DCAA credentials, then click Save.

10) Next, you need to export and import the OO certificate into CSA the certificate store so that SSL Handshake happens between CSA and OO:

11) Export the OO certificate:

```
keytool -export -alias tomcat -file /home/csouser/oo-  
certificate.crt -keystore  
/usr/local/hp/oo/central/var/security/key.store -storepass  
changeit
```

12) Import the OO certificate into the CSA certificate store:

```
keytool -importcert -alias tomcat -file /home/csouser/oo-  
certificate.crt -keystore $JRE_HOME/lib/security/cacerts -  
storepass changeit -noprompt
```

13) Change the port number for OO in the `central-wrapper.conf` file as port 8081 is used by SA. Since port number 8081 is used by SA, we are now assigning port number 8090 for OO. We need to make the change in the `central-wrapper.conf` file. Use this command below:

```
sed -i 's/8081/8090/' /usr/local/hp/oo/central/conf/central-wrapper.conf
```

14) **Run PDT: Go to:** `/usr/local/hp/csa/Tools/ProcessDefinitionTool`

15) The file "`HPOOInputInfo.xml`" is the xml file that needs to be edited.

16) Include the following entries in the `HPOOInputInfo.xml` if not already setup in the XML file:

```
<ooengine  
name="OO-MACHINE-NAME"  
password="ENC (/Nbkt0aFhhSMWN49QpBHTA==) "  
truststore="/usr/local/hp/csa/openjre/lib/security/cacerts"  
truststorePassword="ENC (q6ctyVrBrqWIp107R00q58CrZh8tzPkP) "  
uri="https://localhost:8443/PAS/services/WSCentralService"  
username="admin">
```

```
<!-- SAVA Provisioning-->
<folder path="/Library/Data Center Automation Appliance/Provision
Servers/Actions" recursive="true" update="true"/>
<folder path="/Library/Data Center Automation Appliance/Server
Management/Actions" recursive="true" update="true"/>
<folder path="/Library/Integrations/Hewlett-Packard/Server
Automation" recursive="true" update="true"/>
</ooengine>
```

17) Run this Command in PDT:

```
java -jar process-defn-tool.jar -d db.properties -i
HPOOInputInfo.xml
DO an OO restart
Do a CSA restart

su - csuser << EOD
service csa restart
service mpp restart
EOD
```

18) Base-CP, SA-CP, CSA-Integrations-CP, DCAA CP are available in the location: <location_url>

Note: Instead of using a local host, the IP of the OO engine (the System where we have OO) can be replaced to make it work for an external OO.

OO Purge Flows

Refer to the [Operations Orchestration Reference Table](#). See the topic *Purge execution data using Purging Flows*. In the table, click 'go' to download a PDF regarding running OO Purge Flows.

Appliance Support and Maintenance

HP DCAA releases regularly scheduled updates, documentation releases and maintenance releases. You can find out more information about new Documentation content, Add-Ins, upcoming HP DCAA software releases, and product announcements via the [HP Live Network](#). If you need information about your Support and Maintenance contract, please contact your HP Support Representative.

Custom Attributes

Your build plan must configure custom attributes so they can get picked up by the offerings.

Build plans can be put into the following locations:

- Home/CommonCustomerBuildPlans/ProLiant for HP ProLiant-specific build plans (any platform)

These build plans must carry the following custom attributes:

For the ApplicableServerType with the following value: `physicalproliant`

- Home/CommonCustomerBuildPlans/Non-ProLiant/Linux (for non-HP ProLiant-specific build plans for Linux)
- Home/CommonCustomerBuildPlans/Non-ProLiant/Windows (for non-HP ProLiant-specific build plans for Windows)
- Home/CommonCustomerBuildPlans/Non-ProLiant/Solaris (for non-HP ProLiant-specific build plans for Solaris)

These build plans must carry the following custom attributes:

For the ApplicableServerType with a value of `"physicalnonhp,virtual"` or

`"physicalnonhp,physicalproliant"` (ESXi only):

- VMwareGuestOsName with a value of one of the following: `centos64Guest`, `oracleLinux64Guest`, `rhel5_64Guest`, `rhel6_64Guest`, `rhel7_64Guest`, `sles11_64Guest`, `sles12_64Guest`, `ubuntu64Guest`, `solaris10_64Guest`, `solaris11_64Guest`, `windows7Server64Guest`, `winLonghorn64Guest`, `windows7Server64Guest`

Certificate import for V12N

In order to enable secure communication between the vCenter and the appliance, the secure mode has to be enabled and the vCenter certificate imported onto the appliance. For more details, please consult the *SA User*

Guide: *Virtualization Management*, Appendix B: Virtualization Security - Editing Secure Mode and Importing the CA Certificate. See the [SA Documentation Resource Table](#) at the beginning of this guide.

Support

Appliance Updates and Patches

Please note that patches or updates to the HP Data Center Automation Appliance (DCAA) must *only* be applied at the HP DCAA appliance level. Applying any product specific patches or updates directly to the sub- component products (*HP Server Automation, HP Operations Orchestration*) and *not* at the HP Data Center Automation Appliance level is **not supported** and could render the appliance inoperable.

Log collection for support

- Run `/opt/opsware/oi_util/support_tools/sa_scenesnap.sh` to collect is a good starting set of logs for support.
- The logs are gathered in the following location: `/var/opt/opsware/tmp/`
- The file will be named: `sa_scenesnap.<hostname>.<date>.<time>.zip`
- Log collection for support for CSA and OO
- (ADD)

Update mechanism

Product fixes, OS updates/patches/fixes, or any other update will be packaged as a single GZIPPed TAR file. To install the appliance update, copy the update file to a temporary location such as `/tmp`.

Then run the `appliance update` script, putting in the location and name of the update:

```
cd /var/opt/sava_update
sh updateAppliance.sh /tmp/<name of update file>
```

OO Password Change Policy

You will need to perform this policy procedure **AFTER** changing the password in HP Operations Orchestration (OO). This needs to be done in order for your offerings to function properly after changing the OO admin user password.

These are the steps for the Operations Orchestration password change policy:

1. Go to the folder: `/usr/local/hp/csa/Tools/ProcessDefinitionToolFolder`
2. The file "HPOOInputInfo.xml" is the xml file that needs to be edited.
3. There are 3 tag locations in HPOOInputInfo.xml where the update is required.
4. Find the following 3 tags:
 - a. `<ooengine name="OO-MACHINE-NAME"`
 - b. `<ooengine accessPointType="EXTERNAL_APPROVAL" name="OO-EXTERNAL-APPROVAL"`
 - c. `<ooengine accessPointType="RESOURCE_POOL_SYNC" name="OO-RESOURCE-POOL-SYNC"`

Image - Operations Orchestration password change

```
<ooengine name="OO-MACHINE-NAME" password="ENC(48sP1vpH16c2ostujFa+nbf3t/djc4Rq)" truststore="/usr/local/hp/csa/ope
PkP)" update="true" uri="https://localhost:8443/PAS/services/WSCentralService" username="admin">

  <!-- To import all the flows under a single folder, use the syntax
  <folder path="/path/to/folder">, as shown below
  -->

  <!-- SAVA Provisioning-->
<folder path="/Library/Data Center Automation Appliance/Provision Servers/Actions" recursive="true" update="true"/>
<folder path="/Library/Data Center Automation Appliance/Server Management/Actions" recursive="true" update="true"/>
<folder path="/Library/Integrations/Hewlett-Packard/Server Automation" recursive="true" update="true"/>

  <!-- To import all the flows under a folder and all its subfolders,
  use the syntax
  <folder path="/path/to/parent/folder" recursive="true">
  -->
  <!-- To import a specific flow, use the syntax
  <folder path="/path/to/the/flow" flow="true">
  -->
  <!-- To detect and import changes to previously imported flows, set
  the "update" attribute to "true" on <folder>
  -->
  <!-- To delete previously imported flows that are unreferenced, set
  the "delete" attribute to "true" on <folder>
  -->
</ooengine>

<ooengine accessPointType="EXTERNAL_APPROVAL" name="OO-EXTERNAL-APPROVAL" password="ENC(vjInPq/7/j/ausKhS5qoBst8/c0
ssword="ENC(q6ctyVrBrqWIp107R00q58CrZ8tZPkP)" update="true" uri="https://localhost:8443/PAS/services/WSCentralServic
</ooengine>

<ooengine accessPointType="RESOURCE_POOL_SYNC" name="OO-RESOURCE-POOL-SYNC" password="ENC(mI5m2JD7W56CRVN3cF54LKFcY
Password="ENC(q6ctyVrBrqWIp107R00q58CrZ8tZPkP)" update="true" uri="https://localhost:8443/PAS/services/WSCentralServ
</ooengine>

</ooengines>
```

5. You need to update the password attribute in **all three locations** and make the following changes:

- a) Update the new password: `password="<Password>"`;

Note: The clear text password for 'admin' user on OO Central entered here will be encrypted when the PDT is run in step 8.

- b) Add an attribute `update="true"` before the URI attribute;
6. Close the file by saving it.

7. Go to `/usr/local/hp/csa/Tools/ProcessDefinitionTool`

8. Run this Command in PDT:

```
java -jar process-defn-tool.jar -d db.properties -i HPOOInputInfo.xml
```

For an example, the first ooengine tag will look similar to the one below after the change:

```
<ooengine name="OO-MACHINE-NAME" password="ENC(48sP1vpH16c2ostujFa+nbF3t/djc4Rq)"  
truststore="/usr/local/hp/csa/openjre/lib/security/cacerts"  
truststorePassword="ENC(q6ctyVrBrqWIp1O7R00q58CrZh8tzPkP)" update="true"  
uri="https://localhost:8443/PAS/services/WSCentralService" username="admin">  
...  
</ooengine>
```

DCAA high-availability (HA) and disaster recovery (DR)

- [Overview](#)
- [Disaster recovery](#)
- [High-availability](#)
 - [High-availability in SA](#)
 - [High-availability with VMware vSphere HA](#)
 - [Case 1 ESXi host failure](#)
 - [Case 2 Guest OS failure in the virtual machine](#)
 - [Case 3 Application failure in the virtual machine](#)
- [Links](#)

Overview

Is DCAA mission-critical software?

If not, then customers may elect to not spend time in a High-Availability setup.

In any Case, customers should spend time in creating and following rigorous disaster recovery procedures for their environment.

Disaster recovery

Disaster recovery on appliance upgrade can be done by taking a snapshot before running the upgrade and reverting to this snapshot if the upgrade fails. Either way, the snapshot should be deleted when it is established that everything runs fine, to prevent any performance degradation from the use of snapshots. (Check the VMware documentation on snapshots, referenced at the end of this section.)

Disaster recovery on catastrophic failure resulting in virtual machine loss can be achieved by regular backups of the DCAA virtual machine. Check the VMware backup guide and/or backup best practices documents.

Disaster recovery procedures will protect the customer's investment in case of catastrophic failure.

Recovering from such a disaster will depend on the type of failure: network, hypervisor, underlying bare metal, disk array, etc.

Good, rigorously followed disaster recovery procedures are key to any customer DCAA setup.

High-availability

High availability is maximizing the uptime in case of failure of the hypervisor and/or the underlying server which can be recovered nearly instantaneous and in an automated way.

This is a lot more difficult to achieve and is typically only implemented for mission-critical applications. It can be implemented inside the application (in the) VMs, outside or both. If DCAA is to be used as part of a mission-critical application, customer may elect to invest in high-availability setups that cover the DCAA appliance.

The DCAA appliance itself does not have any internal pre-enablement for an in-product high-availability setup. With this, we mean the ability to run DCAA appliances in a two- or three-node cluster whereby the appliance file system is clustered, the system is being monitored by heartbeat software and failover from one node to any other node is handled automatically. Let's be clear: that is NOT possible in any way, shape or form today in DCAA.

Hypervisor vendors like VMware or Microsoft have their own HA implementation, which after reading is largely independent from the actual application that is provided by the virtual machines being protected.

Since DCAA right now (March 2015) only supports VMware ESXi, we will limit to that hypervisor, we will look at VMware vSphere HA.

High-availability in SA

In SA Ultimate, high-availability is typically achieved by adding whole cores, slices and satellites with the SA gateways on the satellites configured with crossed fail-over routes.

DCAA however, is a single core setup with satellite support so the options are more limited here, because a satellite does not run (besides Word repo and possibly OS provisioning boot server components) any actual core functionality. If the DCAA appliance goes down or becomes unresponsive that's it. Game over.

High-availability with VMware vSphere HA

VMware vSphere HA protects virtual machines from three types of failures. It will protect if the ESX host the VM's running on fails, if the guest OS inside the VM fails, or if an application inside the VM fails. The Basic requirement is for the DCAA appliance to run in a vSphere cluster with more than one ESXi host in that cluster.

Case 1 ESXi host failure

Heartbeats are being sent between the ESXi hosts in the cluster, and VMs can be restarted on other hosts within the cluster if one (or more) hosts go down. Crash and restart of a virtual machine containing CSA, OO and SA is not without risk, so it is entirely possible that one or more of these products fail to recover from a crash. For SA, at the time of the 1st Altair release tests have been performed where the VM was hard-stopped at various moments in the lifecycle and then restarted and any side-effects observed. No tickets were raised at this time and no showstopper unrecoverable behavior was identified at that time. Of course, any running jobs will be marked as failed and will have to be restarted.

Case 2 Guest OS failure in the virtual machine

Heartbeats are being sent between VMware Tools inside the DCAA appliance and the vCenter server.

If the heartbeats are no longer received from the virtual machine (guest OS hang and subsequent VMware Tools hang) then the vCenter server will restart that virtual machine.

Case 3 Application failure in the virtual machine

 Heartbeat support has to be implemented in the application to be monitored. VMware has an application monitoring SDK for this. Since this support has not been added into CSA, OO or SA inside DCAA, this feature cannot be used.

Heartbeats are being sent between VMware Tools inside the DCAA appliance and the vCenter server (as before).

Heartbeats are also being sent between an application inside the virtual machine and the vCenter server.

If the heartbeats are no longer received from the virtual machine (the application inside the VM is no longer working) then the vCenter server will restart that virtual machine.

Links

VMware video content from VMware training department: <https://youtu.be/EPm8Fmhxasc>

