Data Center Automation Suite

Software Version: 2016.10

Installation and Administration Guide

Document Release Date: October 2016
Software Release Date: October 2016

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.

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

Documentation Updates

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/.

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/km/KM01702731.

Contents

Introduction

This section describes the overall procedure for downloading and preparing, deploying, and starting DCA.

The installation of DCA involves:

1. Installing the VMware vSphere client. For more information, see the VMware vSphere documentation.
2. Downloading the installation package from the HPE Software Support site.
3. Reassembling the appliance OVA file using the installer
4. Deploying the template
5. Starting the appliance
   This completes the first time setup so that the appliance is ready to use.

   Follow the post-installation tasks after the installation is complete.

Prerequisites

Before you start installing DCA on your facility, HPE recommends that you:

- Follow the industry-standard high availability and disaster recovery methods and practices, especially when working with mission-critical IT systems. See DCA high-availability (HA) and disaster recovery (DR).
- Verify that 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. This is because the VM guest will synchronize with that time.
- Take a virtual machine snapshot before starting DCA for the first time.

Install DCA

This is the systematic procedure for downloading and preparing the OVA file for DCA.

1. Download all files that make up the DCA. This set includes the split OVA files, a configuration file, documentation, and the DCA installer.

2. Create a folder that will hold the reassembled OVA file.
3. Run the executable to reassemble the OVA file.
4. Select English, Japanese, or Simplified Chinese language for the installer user interface and click **OK**.
5. Click **Next** when the installer opens.
6. Select the target folder that you created in Step 2 and click **OK**.
7. Click **Install** to finish installing the OVA file. The installer verifies that all the prerequisites for application reassembly of the split OVA file are installed.

   > The **Perform Integrity Check** box is selected by default.

8. Click **Reassemble**.The setup reassembles all files for the appliance and shows a **Reassembly completed** message once finished.
   The OVA file is now complete.
9. Click **Next**.
10. Note down the location of the virtual machine files in the target folder.
11. Click **Finish**.
12. Navigate to the target folder that now contains the OVA file. Use this to deploy the OVA template.

Prerequisites for deploying the OVF template

Before you deploy the DCA appliance, ensure that you have the following information:

REQUIRED	
Hostname	A fully qualified hostname for the appliance. **Note:** This hostname is used by the portals for redirects, therefore it should be resolvable on the hosts that are used to connect to the appliance portals.
Deployment IP address	A static IPv4 address for the deployment network that will be assigned to the appliance. A DHCP-assigned address for the appliance is not supported.
Subnet Mask	Network mask
Gateway	Network gateway
DNS	One or more DNS servers. Multiple entries can be separated using a comma.

root password	Password for the appliance root account.
Admin account password	Password for all the admin accounts for the embedded products SA, OO, ITOC, and IT Operator UI.
OPTIONAL	
Management IP address	A static IPv4 address for the optional management network that will be assigned to the appliance. A DHCP-assigned address for the appliance is not supported.
Subnet Mask	Network mask
vCenter IP	One or more IPv4 address of a Windows vCenter to be managed by the appliance. 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 DCA virtual server provisioning offering. **Note** The vCenters can also be added later 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. SMTP server is the IP or hostname of a specific SMTP server to be used in case default 'smtp' does not work through SA. For more information, see "Configuring the Mail Server for a Facility" section in the Server Automation Administration Guide.

Deploy the OVF template

When the template file is successfully created, it can be deployed using VMware vCenter 5.x or 6.x. If you want to deploy the appliance in multiple networks, see Deploying in a multiple network 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 takes you sequentially through eight installation steps, visible on the left sidebar of the installer.

4. On the **OVF Template Details**, review the details of the template such as Product, Version, Vendor, Publisher, Download Size, Size on Disk available (depending on how the application is provisioned), and the template description.
5. Read the End User License Agreement and click **Accept**.
6. Click **Next**.
7. On the **Name** and **Location** screen, specify the name and location for the deployed template.
8. Select an inventory location.
9. Select the default text in the **Name** window and rename the appliance.
10. Click **Next**.
11. On the **Host/Cluster** screen, select a cluster in which you want to run the deployed template.
12. Click **Next**.
13. On the **Resource Pool** screen, select a **Resource Pool** within which you want to deploy the template.
14. Click **Next**.
15. On the **Storage** screen, select a storage location where you want to store the virtual machine files.
16. Click **Next**.
17. On the **Disk Format** screen, select your provisioning type. HPE recommends that you choose thin provisioning as this requires less system resources.
18. Click **Next**.
19. On the **Network Mapping** screen, select the network for the deployed template, and then click **Next**. You must always enable the deployment network. Optionally, you can select to attach the application to a management network.

    > **Note: Secure and insecure networks**
    > Deployment networks are typically considered insecure as they may have DHCP and PXE enabled. Provisioning and management of target servers happens in this network. Generally, these do not have Intranet/Internet access. Management networks are typically considered secure. Generally, these have access to the Intranet/Internet.

20. Complete the **Properties** screen. For information on the available options, see the table in the Prerequisites for deploying the OVF template topic.
21. On the **Ready to Complete** tab, review your configuration, then click **Finish** to start the deployment.
    A status window shows the deployment progress. This process can take several minutes to an

hour.

> **Note:** Ensure that the **Power on after deployment**checkbox is not selected. You should take a snapshot BEFORE you power on the virtual machine.

22. Click **Close**.
23. Locate the deployed appliance and run DCA. vSphere shows the appliance under **Home** > **Inventory** > **VMs and Templates**.

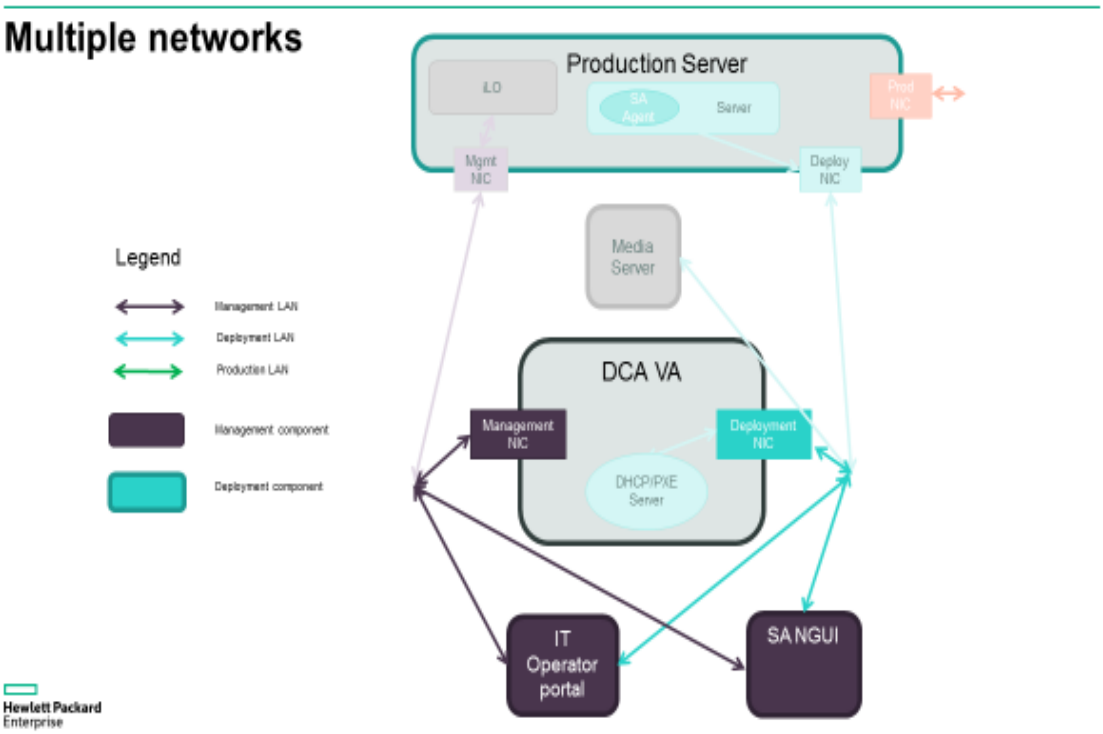
Deployment in multiple-network environments

You can deploy DCA in an environment with multiple networks that handle different types of traffic and can be isolated from one another.

The multiple-network environments defined in DCA are Deployment network and Management network. These are explained in detail below:

Deployment network

This is the network used to provision and manage servers. It is considered the 'insecure' network with PXE, DHCP, media servers, build servers. Typically, a deployment network does not have access to Intranet/Internet.



Management network

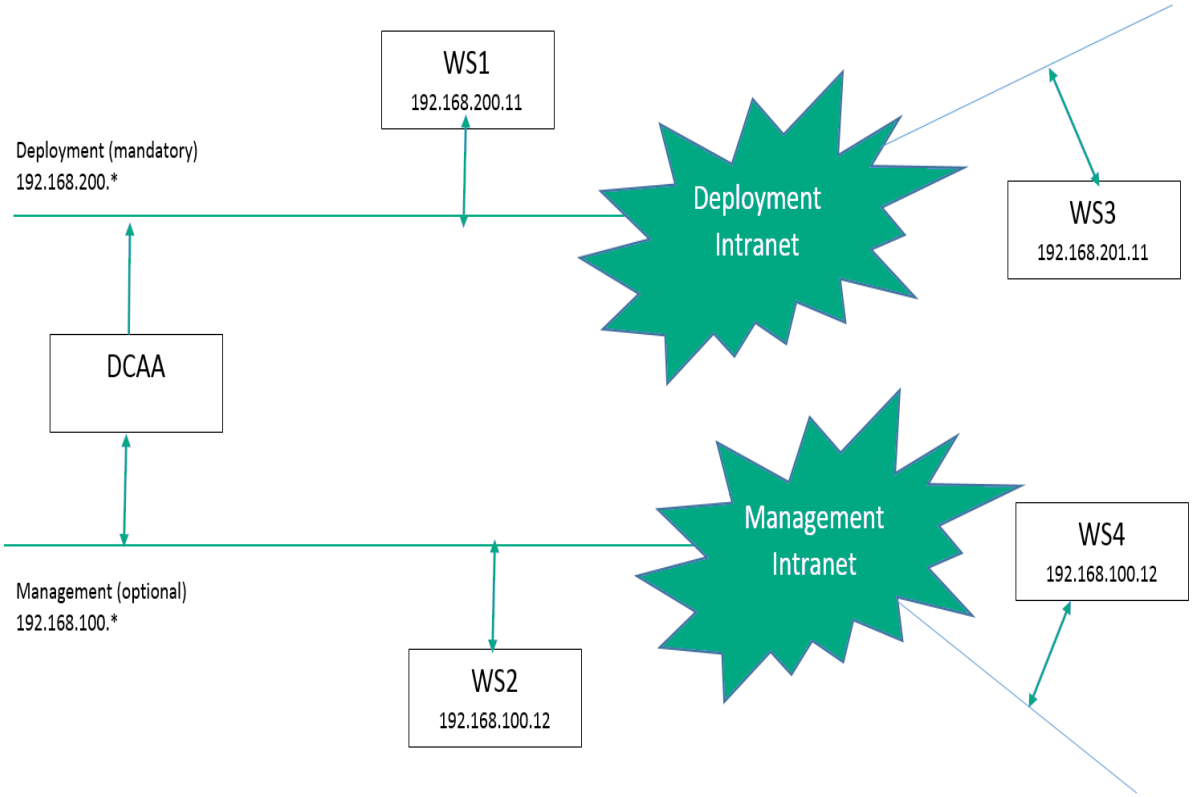
This is the network used for configuration and administration tasks.

The appliance has two network interfaces that can be connected to the corresponding network. The required configuration parameters will have to be provided during the OVF deployment for each of the two networks.

If there is no use case-based separation in the environment and only one network is used, then only the options for the deployment network need to be provided during OVF deployment and the management network will be ignored.

By default, the embedded products are configured to listen on both interfaces, therefore the portals and the SA Client will be available in both networks. If the two networks are isolated (traffic from one network is not routed to the other), consider that:

- The Operations Portal performs redirects that use the hostname provided during OVF deploy. Therefore, the hostname should be resolvable to a valid IP on the host from which the connection is made.
  This means that for a browser connecting from the management network, the hostname needs to resolve to the appliance management IP and for one connecting from the deployment network, to the IP of the deployment interface.
- There is only one default gateway defined for the appliance (usually set in the management network). If the appliance is connected to isolated intranets (management and deployment), connections to and from hosts that are not on the same subnet as the appliance will only be possible if the default gateway is set in that intranet.
  For example, in the following diagram, connections from WS3 workstation will not be possible because the default route uses the management interface.



Capture a 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 the deployed DCA appliance to open the context menu.
2. Navigate to **Snapshot** and then click **Take Virtual Snapshot**.
3. In the **Take Virtual Machine Snapshot** window, enter a snapshot name and description.
4. Click **OK** to create a snapshot.
5. In the vSphere **Recent Tasks** window, click on **Create VM Snapshot** to check that the snapshot has been created successfully.

For better performance, you can remove the snapshot once the initialization phase competed successfully.

Starting DCA

Before powering on DCA for the first time, check that the date and time are set correctly on the VM host system. The VM synchronizes with the Network Time Protocol (NTP).

1. Right-click the deployed DCA appliance and select **Open Console**.
2. In the **Console** window, click the green **Play** button to start the appliance.
   The appliance starts, configures the network, and starts the initialization phase. This process takes between 15 and 40 minutes.

   Once initialized, you can start using the appliance. Check the */var/log/dca/first_time_setup.out* log file to make sure that the initialization phase is completed successfully. The log should end with a *BUILD SUCCESSFUL* message.

   Note: The initial configuration also sets up the firewall and opens only the ports that are required by the components.
3. You will see a login screen appear at the console prompt.
   The default login information:
   - The Management Console is available at: `https://<appliance>:8444/csa`
     (username: admin / password: <configured admin account password>)
   - The DCA Operations Portal is available at: `https://<appliance>:8079`
     (username: consumer / password: <configured admin account password>)
   - The Operations Orchestration portal is available at: `https://<appliance>:8443/oo`
     (username: admin / password: <configured admin account password>)
   - The Server Automation client can be downloaded from `https://<appliance>`
     Click on the “Download HPE Launcher” link and install the SA client. (username: admin / password: <configured admin account password>)
   - The IT Operations Compliance portal is available at: `https://<appliance>:9100`

Post-installation tasks

Initialization phase tasks

- Configure and publish the offerings

Server provisioning tasks

Once your servers are provisioned, the appliance is ready to be used.

- Configure DHCP on the Appliance
- Configure the Media server
- Update/create build plans for the desired Operating Systems
- Create a new build plan

Other post-installation tasks

- Set up and define Server Automation (SA) software and patch policies
- Configure IT Operations Compliance business services, policies, and maintenance windows
- Add one or more vCenter manually
- Redeploy DCA using the initial appliance snapshot
- Configure and publish the offerings

Configure and publish the offerings

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

To publish an offering:

1. Go to `https://<appliance>:8444/csa` to connect to the Management Console.
2. Click **Offerings**.
3. Click the desired offering and select the desired version.
4. Review the offering configuration, by accessing the **Options** tab. For the Provision Servers offering to be able to create new virtual machines, configure the **New Virtual Servers** section with appropriate values for the appliance-managed vCenter. For example: Datastore, inventory folder, network name.
5. Save your changes.
6. Access the **Publishing** tab and click **Publish** to make the offering available on the Operations Portal.
7. Select the category **Server Management**, then click **Publish**.
8. Check the **Offerings** section for more information on each available offering.

Configure DHCP on the appliance

The DHCP Network Configuration Tool for IPv4 is installed on the appliance. To configure networks for provisioning:

1. Log in as root on the appliance.

   > **Note:** (Optional) Make a backup copy of the configuration file with the following commands:
   >
   > - `cd /etc/opt/opsware/dhcpd`
   > - `cp dhcpd.conf dhcpd.conf.orig`

2. 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]:
```

- 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 'c' at the prompt. Local networks are detected automatically and displayed.
- If you are adding a local network, enter the IP addresses or host names of the DHCP range and the DNS servers. A comma and a space separate the IP addresses.
- If the displayed information is correct, enter 'k' to keep the network and return to the main menu.
- At the main menu, enter 's' to save the information you have entered.
- To edit a configured network, enter the corresponding integer and go to step 2.
- 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 the 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, see the Server Automation Administration Guide.

Create build plans for the OS

To perform server provisioning, DCA requires build plans for each desired operating system.

Build plan templates

Copy the templates available from the SA library to create build plans filtered correctly in the Operations Portal. These supplied templates are available under */Opsware/Tools/build plans/SAVA* and their have the required custom attributes for filtering in the Operations Portal.

Custom build plans

Create your custom build plans in the corresponding SA library folder under */Home/CommonCustomerBuildPlans*. For example, in the ProLiant folder, place build plans customized for provisioning ProLiant systems, Non-ProLiant/<OS family> folder for others.

Create a new build plan

To create a build plan:

1. Start the SA client and access the **Library**.
2. Select the **By Folder** tab and navigate to the corresponding subfolder in: `/Home/CommonCustomerBuildPlans`
3. Right-click and select **New > OS Build Plan**.
4. Provide a name for the build plan. This name will appear in the Operations Portal.
5. Click on **Build Plan Items** and click **Copy Plan**.
6. Select a build plan for the desired OS from one of the subfolders of `/Opsware/Tools/build plans/SAVA`
7. Configure the **Set Media Source** step in the build plan then click on the **Set Media Source** step.
8. Set the **Parameters** field to a working network share that contains the media for the Operating System.
9. Click on the **Custom Attributes View**and add custom fields so that the build plan can be filtered correctly in the Operations Portal.

10. Enter a valid key for your Windows version in the **Product Key** attribute row.
11. Click **File > Save** or type **CTRL+S** to save your changes.

Add custom attributes

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

HPE ProLiant-specific build plans (any platform)

1. Add build plans under `Home/CommonCustomerBuildPlans/ProLiant`
2. Add the following custom attributes: `ApplicableServerType - physicalproliant`

Non-HPE ProLiant-specific build plans

1. Add build plans in the following locations according to their target platforms
   - Linux - `Home/CommonCustomerBuildPlans/Non-ProLiant/Linux`
   - Windows - `Home/CommonCustomerBuildPlans/Non-ProLiant/Windows`
   - Solaris - `Home/CommonCustomerBuildPlans/Non-ProLiant/Solaris`
2. Add the following custom attributes:
   - ESXi only - `ApplicableServerType` with a value of `physicalnonhp,virtual` or `physicalnonhp,physicalproliant`
   - `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`.

Add a vCenter manually

This is the process for bringing vCenters under DCA management, and is the only way to add vCenters into migrated appliances.

1. Install the SA Agent on the Windows server where the vCenter runs.
   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.

2. Go to **Virtualization** > **VMware vCenter**.
3. Right-click on the right pane and select **Add Virtualization Service**.
4. Select the server and provide the credentials needed to authenticate with the vCenter.
5. Grant permissions on the vCenter for the **SuperUsers** group. This enables operators to use vCenter in the portal.

The virtualization framework only supports managing vCenters running on Windows operating system.

Enable secure communication

To enable secure communication between the vCenter and the appliance, activate the secure mode and import the vCenter certificate into the appliance.

Redeploy DCA using OVF properties

After DCA is set up and deployed, you can redeploy the appliance from a snapshot using a new configuration.

If you took a snapshot of the DCA appliance before starting it for the first time, you can redeploy the appliance from a first time startup again. You can also bring up the appliance multiple times with different settings. This means that you can use the snapshot as a fresh starting point for the appliance then change its mode and configurations.

To deploy a DCA appliance from a snapshot:

1. Import the appliance using **Deploy OVF template**.
2. Follow the wizard and configure the appliance.
3. Take a snapshot.
4. Run the appliance.

To redeploy the appliance from a snapshot:

1. Revert to the snapshot that was taken before the first appliance start.
2. Open the appliance settings and click on the appliance.
3. Click on **Getting Started**; click on **Edit virtual machine settings**.
4. Navigate to the **Options** tab, select **vApp options/Properties** on the left pane.

5. Edit the properties.
6. Save the new settings.
7. Take a **new snapshot** before your first start.
8. Run the appliance.

SA software policies

For more information on how to create software policies and manage packages, see the Server Automation User Guide.

You can use the product documentation library to find the latest version of this guide on the HPE Software Support site (HPE Passport required).

SA patch policies

To patch the managed servers, the patch metadata database and patches need to be imported, and the patch policies should be defined.

For more information, see the Server Automation User Guide.

You can use the product documentation library to find the latest version of this guide on the HPE Software Support site (HPE Passport required).

IT Operations Compliance business services, policies, and maintenance windows

To enable ITOC integration from the IT Operations Portal offerings, business services, policies and maintenance windows will need to be setup in ITOC so they can be selected from the Operations Portal offerings.

For more information, consult the IT Operations Compliance User Guide.

You can use the product documentation library to find the latest version of this guide on the HPE Software Support site (HPE Passport required).

Offerings

This solution offers the following offerings for server management:

- Provision servers
- Remediate server policies
- Manage servers
- Install Server Automation Agents

Functionality supported in this solution

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

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

Set up DCA default offerings

Server provisioning

This service offering provisions operating system baselines onto a physical server or multiple virtual servers. The IT operator has the option to either provision one network-booted unprovisioned server at a time or multiple virtual servers on VMware virtualized environments.

In addition to provisioning options, the IT operator can optionally select to link the new server into a new or existing ITOC business server and optionally link the business service to ITOC policies and maintenance windows.

Options for provisioning a network-booted 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.

HPE ProLiant servers offer an advantage in functionality over a third-party server. For example, HPE 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 operating systems that 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 Operations Portal.

There are seven server options to be chosen by the Operations Portal:

- four of them are dynamic
- two are optional
- three are non-dynamic and optional

The table below details these options:

Dynamic server options

Option	Description
OS Build Plan	A dynamic list of the SA's OS build plans that are applicable for the selected booted server are displayed. For an HPE ProLiant server, the OS build plans are listed from two folders, `œ/Opsware/Tools/Build Plans/SAVA/ProLiant` and `œ/Home/CommonCustomerBuildPlans/ProLiant`. The first folder has HPE-supplied build plans and the second one is for customer updated build plans. For a non-ProLiant or Virtual Server, depending on the service OS, build plans from Linux or Solaris or Windows folder in `œ/Opsware/Tools/Build Plans/SAVA/Non-ProLiant and œ/Home/CommonCustomerBuildPlans/Non-ProLiant` folders are shown. The first folder also has HPE supplied build plans and the second one is for customer updated build plans. Non-ProLiant subdirectories:

	This configuration of entries can be found in the file: `$CSA_HOME/jboss-as/modules/sun/jdk/main/service-loader-resources/sa-provider.properties`
	
	`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`

Un-provisioned Server	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.
Hostname Prefix	Optional. 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	Optional. A dynamic list of customers defined in SA are listed. The IT operator can choose one.
Attach to a Device Group	Optional. A dynamic list of public and static Device Groups defined in SA are listed. The IT operator can choose one.
Operations Portal	Optional. A dynamic list of ITOC business services, compliance policies, and maintenance windows are listed. You can also select to create a new business service from the drop-down list, then provide a name for the business service in the edit field below the drop-down.
Send Email Notification	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	Optional and when chosen, the IT operator can specify a ticket ID of ITIL process for the provisioning job in SA.
HPE-SA Provider properties	Optional. You can provide the name of the SA provider under `$CSA_HOME/jboss-as/modules/sun/jdk/main/service-loader-resources/sa-provider.properties`

Options for 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 be registered with SA's virtualization service.

> **Note:** To provision new VMware virtual servers, the vCenter needs to be managed by the appliance. If the vCenter was not specified when the appliance was deployed, you can follow the steps described in the "'Add a vCenter manually" on page 18" section to add your vCenter under appliance management.

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

Option	Description
Hypervisor	A dynamic list of VMware hypervisors is shown here, from which the IT operator has to choose one where the virtual servers would be provisioned.
Attach to a Customer	Optional. A dynamic list of customers defined in SA are listed. The IT operator can choose one.
Attach to a Device Group	Optional. A dynamic list of public and static Device Groups defined in SA are listed. The IT operator can choose one.
OS Build Plan	A dynamic list of the 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. These folders are for HPE-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 servers to be provisioned with the selected options. This can be from 1-32 CPUs. **Note:** This number may also have restriction in the hypervisor.
Memory in MB	The memory in MB on the virtual servers to be provisioned with the selected options. This can be from 512-1000000.

Option	Description
	Note: This number can vary based on a parameter set by the administrator in vCenter.
Hostname Prefix	Optional. Can be up to 9 characters in length and will prefixed to hostname. A hostname is generated if nothing is specified.
Datastore	Datastore is where the Virtual Servers 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 servers 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 servers 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 servers 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 servers 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.

Non-dynamic provisioning options

Apart from the dynamic options, some non-dynamic options 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 whether they are available to the IT operator. The table below lists these options:

Option	Description
Storage Device Datastore	The Datastore where the disks of the virtual servers 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 CD-ROMs are created and is preset to ,`/mnt`, specifying that the mount point for the CD-ROM 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 Servers to be created. This is preset to `True`, `True`, to connect both disk and CD-ROM 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 Cards names. This is preset to `eth0`, to add a single NIC on the virtual servers 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 Cards key names. This is preset to `eth0`, to add a key for the single NIC on the virtual servers 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 NICs on the virtual servers 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 NICs attached to the virtual servers 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 NICs are connected to the Virtual Servers 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 servers from SA. This will be one of the keys specified in NIC Key Option.
IT Operations Compliance	Optional. A dynamic list of ITOC business services, compliance policies, and maintenance windows. You can also select to create a new business service from the drop-down list and then provide a name for the business service in the edit field below the drop-down list.
Send Email Notification	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.

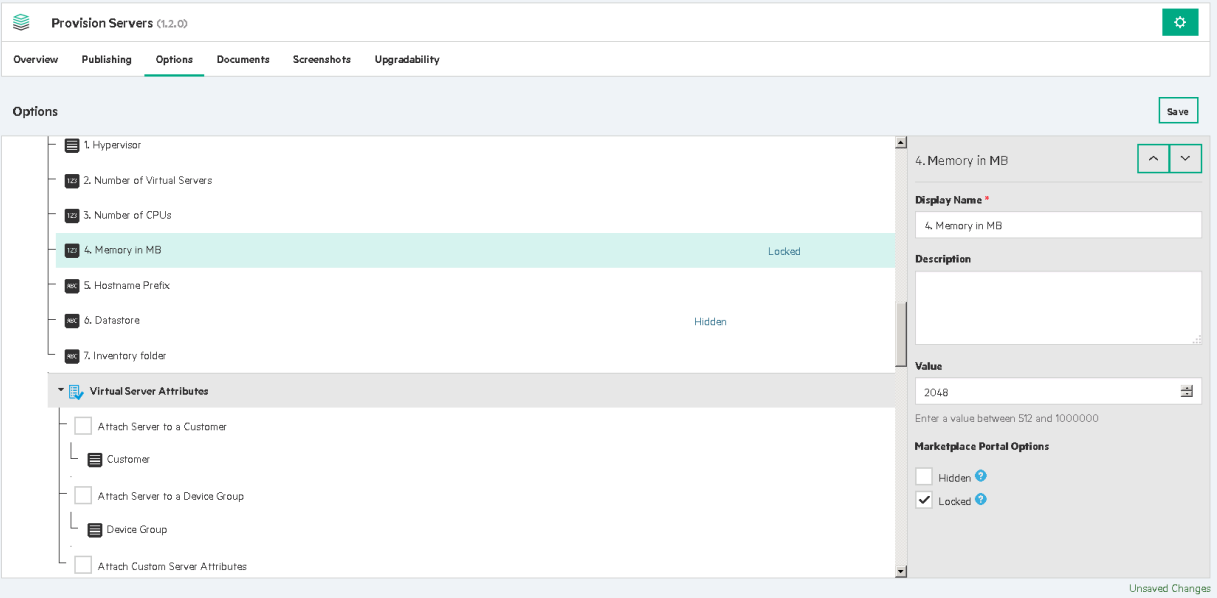
Attach Ticket ID	Optional. When chosen, the IT operator can specify a ticket ID of ITIL process for the provisioning job in SA.

Locking non-dynamic provisioning options

Some of the above non-dynamic options are marked locked and/or **invisible** by default. This can be used in scenarios where the Administrator wants to limit certain options for the IT operator.

To change the visibility of these options:

1. Log into the Administrator Portal as an Administrator.
2. Under the **Provision Servers** offering, click the **Options** tab.
3. Select the corresponding option as shown below:



Server provisioning options for ITOC

> **Note:** These options are supported only in the Premium version of the product.

The following options are available for configuring Server Provisioning offering with Operations Portal.

Newly provisioned servers can be attached to policies and business services defined in ITOC. The options are available for both provisioning network-booted servers and virtual servers.

Option	Description
Attach Policies	The following set of options allow attaching the newly provisioned server to existing ITOC policies. After the server is provisioned, it will be added to the specified Business Service and new Statement of Applicability (SOA) will be created using the selected policies, maintenance windows and the business service.
Select Policies	A dynamic list of production policies defined in ITOC.
Select Maintenance Windows	A dynamic list of maintenance windows defined in ITOC.
Select Business Service Name	The name of a new Business Service that will be created. If `--NONE--` is specified, a name will be automatically generated.
Attach Business Services	The following set of options allow attaching the newly provisioned server to existing Business services.
Select Business Service	A dynamic list of Business Services defined in ITOC.
Default Business Service	The name of a Business Service. The DCA administrator may use this option to specify a Business Service to which the newly provisioned servers are added by default.

For more information about the Provision Servers offering in DCA, see **Provision Servers**.

Remediate attached patch and software policies

The Server Policy Remediation offering remediates already attached patch and/or software policies on a device group or on an individual server.

Change the timeout for a device group

The time taken to remediate a Device Group can vary greatly depending on how many servers the Device Group has and 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.

By default, this property is set to 4 hours (in milliseconds). To change it:

1. Go to `https://<DCA-Appliance-IP>:8443/oo` to log in to OO Central.
2. Click on **Content Management**.
3. In the **Configuration Items** tab, expand **System Properties**.
4. Choose **DCAA_Remediate_DG_Timeout** system property and update the **Override value** to a desired timeout value in milliseconds.

For more information about the Server Policy Remediation Offering in DCA, see Server Policy Remediation.

Manage Servers offering

This solution is part of the Data Center Automation Suite that demonstrates how to manage life span of various servers using HPE SA. 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.

The 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. In addition to the manage server options, the IT operator can optionally select to link the server into a new or existing ITOC business server and optionally link the business service to ITOC policies and maintenance windows.

Options for Manage Servers offering

The **Manage Servers** offering has the following options:

Option	Description
Server Name	A dynamic list of servers managed by the SA instance embedded in the appliance
Install Software Packages	A dynamic list of software packages imported in SA
Run Additional Patch Policies	A dynamic list of patch policies defined in SA
Run Additional Software Policies	A dynamic list of software policies defined in SA
Run Server Scripts	A dynamic list of servers scripts defined in SA

Manage servers with ITOC

> **Note:** These options are supported only in the Premium version of the product.

Option	Description
Select Business Service	A dynamic list of business services defined in the ITOC instance embedded in the appliance
New Business Service name	The name of a new business service that will be created if the operator selects to create a new business service in the list above.
Select Policies	A dynamic list of policies defined in ITOC. Only policies in production state are loaded.
Select Maintenance windows	A dynamic list of maintenance windows defined in ITOC.

Request the Manage servers offering

Before operators can use the **Manage Servers** offering, the administrator using the SA Client should define the content required by it.

- Import software packages
- Define software policies
- Define patch policies
- Create scripts

For detailed steps, see Server Automation Administration Guide.

For more information about the **Manage Servers** offering in DCA, see Manage servers.

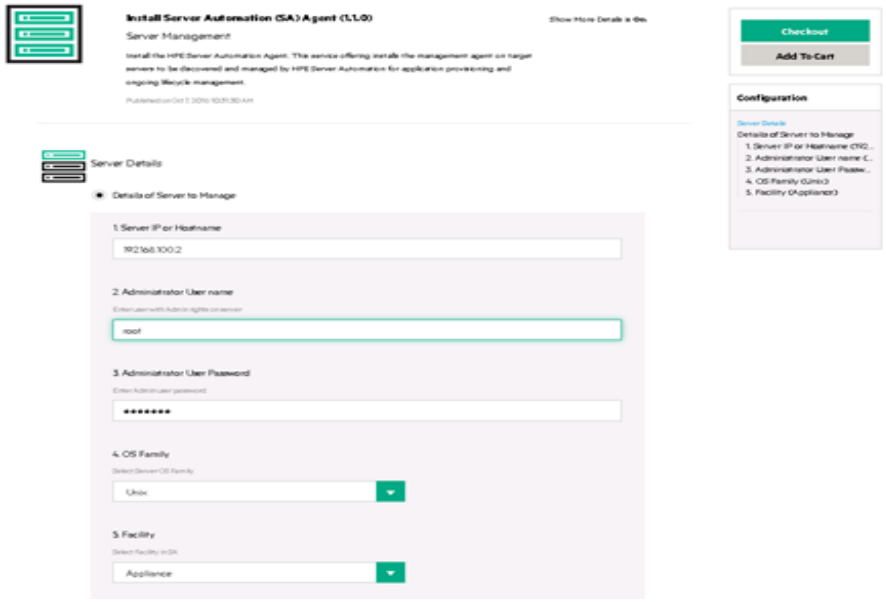
Server Automation (SA) Agent installation

> **Note:** DCA supports installing the SA agent one server at a time.

This service offering installs the management agent on a target server to be discovered and managed by Server Automation for application provisioning and ongoing lifecycle management.

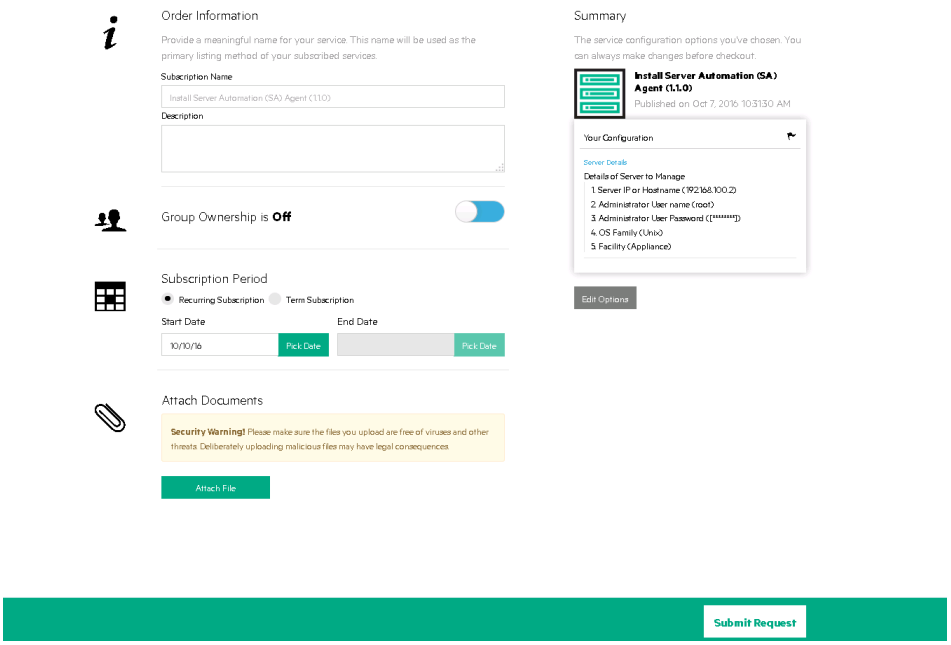
Subscribe to the Install Server Automation (SA) Agent offering

1. Log onto the Operations Portal at **`https://<ipaddress>:8079`**
2. Click **All Services**.
3. Select the **Install Server Automation (SA) Agent** offering.
4. Create a Server IP or hostname.
5. Enter the administrator username for the user with Admin rights on the server.
6. Enter the administrator password.
7. Select the Server OS family for the server from the list of options.
8. Select one of the facilities listed, where the server is hosted.



9. Perform a checkout operation. Include the Subscription Name and Service Description, Subscribing Period (the time period your subscription will operate). Optionally, you can attach documents to the service that are relevant to the user subscribing to the service.

10. Select **Submit Request** to subscribe to the service.



Integrate and configure DCA components

Integrate with Cloud Service Automation (CSA)

This integration allows administrators to use the SA component as the provider for a CSA installation.

Once configured, the CSA administrator has access to the provisioning, patching and policy management capabilities delivered as part of the DCA bundle.

Specify the hostname of the DCA appliance when configuring the SA provider in the CSA 4.7 instance:

- **Display Name**: SA
- **User ID**: <SA user account>. Must be member of **SuperUsers** group.
- **Password**: <account password>
- **Service Access Point**: `https://`<DCA Hostname>`:443`

For detailed information on integrating CSA with DCA, see the CSA documentation on the HPE Software Support site.

Integrate with NA

The Premium version of the appliance supports integration with Network Automation (NA).

NA is not embedded in the appliance and is only supported as an external product.

To allow communication with NA, open the following ports:

- **Port 1099** JNDI
- **Port 1098** RMI Method
- **Port 4446** RMI Object

For more details and information on configuring the NA integration, see the Server Automation Integration Guide.

Integrate with OO

This integration allows administrators to integrate the Server Automation (SA) component with flows from an Operations Orchestration (OO) 10.60 installation.

Integrating SA and OO makes it possible to use many features available in SA within custom OO flows to solve specific use cases. The integration would rely on accessing the SA instance using the DCA hostname and account credentials.

Set up DCA to use an external OO instance

Prerequisites

- Make sure the path is set to: `/usr/local/hp/csa/openjre/bin/java`.
- If the OO Central hosts permits connections on port 8443, you can invoke all the cURL commands below from the appliance.
- The examples use the following credentials: admin/admin. To connect to your OO Central, change the `Authorization:Basic YWRtaW46YWRtaW4=` header to use the password that you set for the OO admin user. To do that, replace `YWRtaW46YWRtaW4= string` with the `base64` encoding of `admin:<your_admin_password>`.

To use the HPE SA provider with an OO environment:

1. In the command prompt of the appliance, type the 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 content packs (CP) need to be available in the external OO central (the listed versions are the minimal requirements):
   - `oo10-base-cp-1.8.0.jar`
   - `oo10-hpe-solutions-cp-1.8.2.jar`
   - `oo10-cloud-cp-1.8.2.jar`
   - `oo10-sa-cp-1.3.0.002.jar`
   - `oo10.50-csa-integrations-cp-4.70.0000.jar`
   - `Data Center Automation Appliance-cp-1.2.1.jar`

   All the content packs are available in the `DCA_VA_1610_OOTB.zip` that is part of the appliance installation package.
3. The appliance requires OO user ‘admin’ to exist on the OO central instance and to have the **Promoter**, **Administrator**, and **System_admin** roles. For example, for a freshly installed OO instance, you can invoke the following command:
   ```
   curl -X POST -d '{"password":"admin","roles":[{"name":"PROMOTER"},
   {"name":"ADMINISTRATOR"},{"name":"SYSTEM_
   ADMIN"}],"username":"admin","permissions":"ADMINISTRATOR"}' --header "Content-
   Type: application/json" -k https://<ooCentral>:8443/oo/rest/users
   ```
4. Configure the CSA_OO internal user on the OO Central. To achieve this, perform one of the following actions:
   - Log into OO central and configure the user from **Content Management** > **Configuration Items**. In **Configuration Items**, expand **System Properties** and edit `CSA_OO_USER`. Its default value is `ooInboundUser`. Input the value `admin` in the field **Override value** and click **Save**.
   - Invoke the following command:

     ```
     curl -k -X PUT -d 'admin' --header "Content-Type:application/json" --header
     "Authorization:Basic YWRtaW46YWRtaW4="
     https://<ooCentral>:8443/oo/rest/content-config/CSA_OO_USER?type=SYSTEM_
     PROPERTY.
     ```
5. Configure CSA_REST_CREDENTIALS. For CSA to make REST calls to OO , we need to configure CSA REST credentials on the external OO Central. To achieve this, perform one of the following actions:
   - Log into OO Central and configure the credential from **Content Management** > **Configuration Items**. In configuration items, expand **System Account** and edit CSA_REST_

CREDENTIALS. Input the credentials of the **admin** user that you use to connect to the appliance Administration Console and then click **Save**.

- Invoke the following command:

```
curl -k -X PUT -d '
{"username":"admin","password":"<applianceAdminUserPassword>"}' --header
"Content-Type:application/json" --header "Authorization:Basic
YWRtaW46YWRtaW4=" https://<ooCentral>:8443/oo/rest/content-config/CSA_REST_
CREDENTIALS?type=SYSTEM_ACCOUNT
```

6. Update CSA_REST_URI. OO Central needs to communicate with the appliance to receive the job details and to submit the results. This is specified through the CSA_REST_URI parameter. Set it by performing one of the following actions:
   - Log into OO Central and configure the credential from **Content Management** > **Configuration Items**. In configuration items, expand **System Properties** and edit `CSA_REST_URI`. Type the URI (`https://`<applianceIP>`:8444/csa/rest`) in the **Override value** field and then click **Save**.
   - Invoke the following command:

```
curl -k -X PUT -d 'https://<appliance>:8444/csa/rest' --header "Content-
Type:application/json" --header "Authorization:Basic YWRtaW46YWRtaW4="
https://<ooCentralIP>:8443/oo/rest/content-config/CSA_REST_URI?type=SYSTEM_
PROPERTY
```

> **Note:** The following 3 steps (7, 8, and 9) apply only to DCAPremium, for running operations on the embedded ITOC.

7. Configure `ITOC_REST_CREDENTIALS`. For OO to make calls to ITOC, configure ITOC credentials on the external OO Central. Perform one of the following actions:
   - Log into OO Central and navigate to **Content Management** > **Configuration Items**. In configuration items, expand **System Account** and edit `ITOC_REST_CREDENTIALS`, input the credentials of the ITOC**csauser** user and then click **Save**.
   - Invoke the following command:

```
curl -k -X PUT -d '{"username":"csauser","password":"<ITOC_csauser_pass>"}' -
-header "Content-Type:application/json" --header "Authorization:Basic
YWRtaW46YWRtaW4=" https://<ooCentral>:8443/oo/rest/content-config/ITOC_REST_
CREDENTIALS?type=SYSTEM_ACCOUNT
```

8. Update ITOC_REST_URI. OO Central needs to communicate with the appliance to run actions on ITOC. Configure this by performing one of the following actions:

- Log into OO Central and configure the credential from **Content Management** > **Configuration Items**. In configuration items, expand **System Properties** and edit ITOC_REST_URI. Input the URI (`https://<appliance>:7771`) in the **Override Value** field and then click **Save**.
- Invoke the following command:

```
curl -k -X PUT -d 'https://<appliance>:7771' --header "Content-
Type:application/json" --header "Authorization:Basic YWRtaW46YWRtaW4="
https://<ooCentral>:8443/oo/rest/content-config/ITOC_REST_URI?type=SYSTEM_
PROPERTY
```

9. Update SA_ITOC_PLATFORMMAP_CSV_PATH. The platform mapping file needs to be available on the OO Central host to run actions on ITOC:
   - Copy the file from the appliance (`/usr/local/hp/oo/sa-itoc-platformMap.csv`) to your OO Central host.
   - Update the SA_ITOC_PLATFORMMAP_CSV_PATH configuration item. Log into OO Central and navigate to **Content Management** –> **Configuration Items**. In configuration items, expand System Properties and edit `SA_ITOC_PLATFORMMAP_CSV_PATH`. Type the path on the OO Central host where you copied the file in the **Override Value** field and click **Save**. Alternatively, you can run the following command:

```
curl -k -X PUT -d '<path>' --header "Content-Type:application/json" --header
"Authorization:Basic YWRtaW46YWRtaW4=" https://
<ooCentral>:8443/oo/rest/content-config/SA_ITOC_PLATFORMMAP_CSV_
PATH?type=SYSTEM_PROPERTY
```

10. Export the OO certificate on the OO Central host.
    - For Linux, run `keytool -export -alias tomcat -file <path>/oo-certificate.crt -keystore /usr/local/hp/oo/central/var/security/key.store`
    - For Windows, run <OO_Intall_Dir>`\java\bin\keytool.exe -exportcert -alias tomcat - file C:\oocentral.crt - keystore` <OO_ Install_ Dir>`\central\var\security\key.store`
    - Copy the certificate to the appliance.
    - Import the OO certificate into the CSA certificate store on the appliance: `keytool - importcert - alias externalOO - file <path>/oo- certificate.crt - keystore $CSA_HOME/openjre/lib/security/cacerts -storepass changeit –noprompt`
11. Update the OO engine used by the appliance.
    - In the updateOOEngine.py file update the access point URI (*https://127.0.0.1:8443/PAS/services/WSCentralService*) line to match your OO host details. For example you can run the following command:

```
sed -i 's/127.0.0.1:8443/<OOCentralHost>:<OOCentralPort>/' updateOOEngine.py
```

- Run the updateOOEngine script to perform the update:
  `/opt/opsware/bin/python2 /var/opt/sava_firstboot/updateOOEngine.py --CSAUSER admin --CSAPASS <password> --OOUSER admin --OOPASS <password>`

12. Restart the CSA service on the appliance using the following command:
    `service csa restart`
13. Update the HPSA provider:
    a. Connect to the Administration console: **`http://`***`<appliance>`***`:8444/csa`**.
    b. Access **Providers** > **HPSA** and click **Edit**.
    c. Update the **Service Access Point** field to use the appliance hostname or IP instead of localhost.

Integrate with OBR

This section describes the process of integrating OBR with DCA Suite Premium. This integration will help you use the reporting capabilities in OBR for the embedded Server Automation component of DCA Suite Premium.

> **Note:** The OBR SA Reports Content Pack provides reporting capabilities to only Server Automation within DCA Suite Premium.
>
> The post-installation configuration of OBR must be done right after installing OBR 10.00. If it is configured after installing any patch versions, such as OBR 10.01, 10.02 and so on, installation of the OBR-SA Reports Content Pack may fail.

The integration involves the following steps:

1. Install the OBR 10.02 patch
   Download and install the patch from https://softwaresupport.hpe.com/group/softwaresupport/search-result/-/facetsearch/document/LID/OBR1002LIN_00001.
2. Configure the OBR SA Reports Content Pack
   To configure the Content Pack, see the **Configuring the HPE OBR SA reports content pack** section of the *HPE OBR-SA Reports Content Pack Configuration Guide*. This guide is located at https://hpln.hpe.com/contentoffering/obr-sa-reporting-content (on this page, navigate to Resources > File Repository > Documentation).
3. Configure the DCA data sources
   To configure the DCA data source, first enable SA in the OBR Administration Console. To do this,

see the **Configuring HPE SA data sources** section of the *HPE OBR-SA Reports Content Pack Configuration Guide*. This guide is located at https://hpln.hpe.com/contentoffering/obr-sa-reporting-content (on this page, navigate to Resources > File Repository > Documentation).
Pre-register a data miner for DCA as a data source.
Perform the following steps to pre-register a data miner for DCA from the OBR Web Administration Console:

a. Log in to **OBR Administration Console**: `https://<obr-core-ip>:21412/BSMRApp`
b. Select **Data Source Configuration > HPSA**.
c. Click **Create New**.
d. In the **Connection Parameters** area, enter the required values.
e. Click **OK**.
f. Click **Save**.
The Saved successfully message is displayed.

4. Set up and install data miners
To set up and install data miners, see the **Setting up and installing data miners on the SA server** section of the *HPE OBR-SA Reports Content Pack Configuration Guide*. This guide is located at https://hpln.hpe.com/contentoffering/obr-sa-reporting-content (on this page, navigate to Resources > File Repository > Documentation).

DCA updates and patches

Data Center Automation (DCA) releases regularly scheduled updates, documentation releases, and maintenance releases.

You can find out more information about new documentation, add-ins, upcoming software releases via the HPE Live Network.

Apply DCA patches

Patches or updates to DCA must only be applied at the DCA appliance level. Do not apply product specific patches or updates directly to the sub-component products (Server Automation, Operations Orchestration) and not at the DCA level as this is not supported and DCA might stop working.

Install appliance updates

To find the latest patches, go to the HPE Software Support site, select **Dashboards** > **Patches** and then search for your product and version.

Product fixes, OS updates/patches/fixes, or any other update will be packaged as a single `GZIP TAR` file.

To install the appliance update:

1. Copy the update file to a temporary location, such as `/tmp`.
2. Run the following appliance update script, using the location and name of the update:
   - `cd /var/opt/sava_update`
   - `sh updateAppliance.sh/tmp/<`name of update file`>`

DCA licensing

This section describes the steps that have to be performed to import licenses into each of the products embedded in the DCA Suite.

Trial license

DCA Suite ships with a 90-day trial license, during which time the full functionality is available. To continue using the appliance after the trial expires, import a full license.

Based on the version of DCA Suite that you have acquired, several license files will be generated.

Import a DCA license

By default, the license filename for the DCA Suite will begin with `DCA-VAPP`.

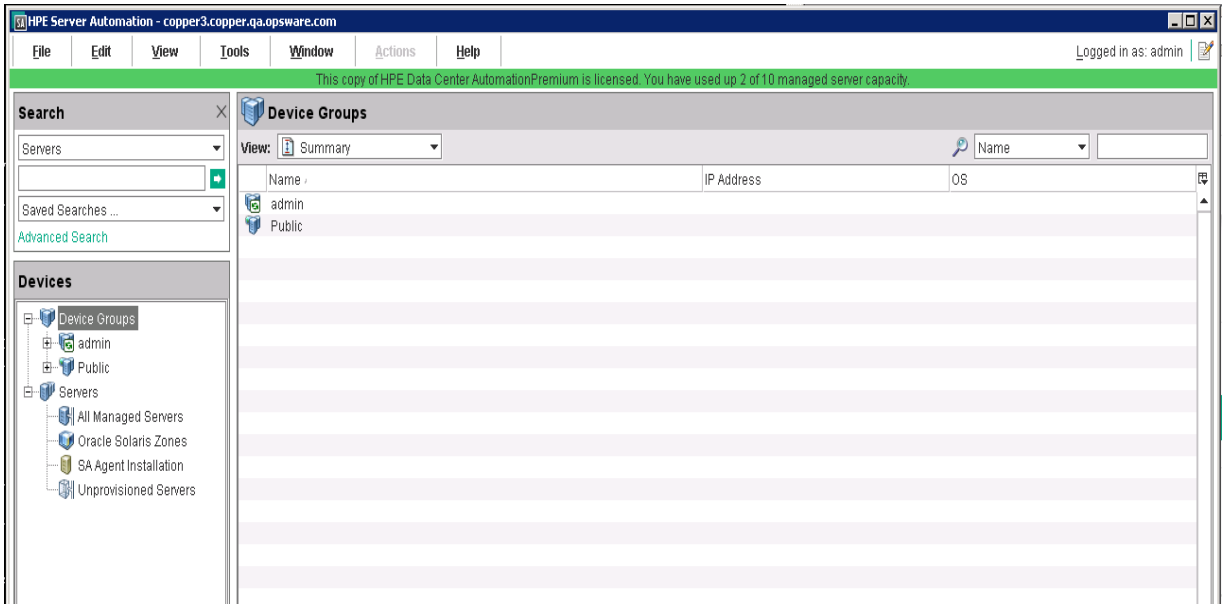
1. Copy the license file on the appliance, for example in the `/root` folder.
2. Run the following command: `/opt/opsware/license/license_import.sh` *`<path_to_license_file>`*.

When the license is imported, the OO-central and Twist services restart.

Example

```
/opt/opsware/license/license_import.sh ./DCA-VAPP-PREM^1.10_5240275.dat

License file path: ./DCA-VAPP-PREM^1.10_5240275.dat

Successfully installed license.
```

The status of the license is reported in SA.

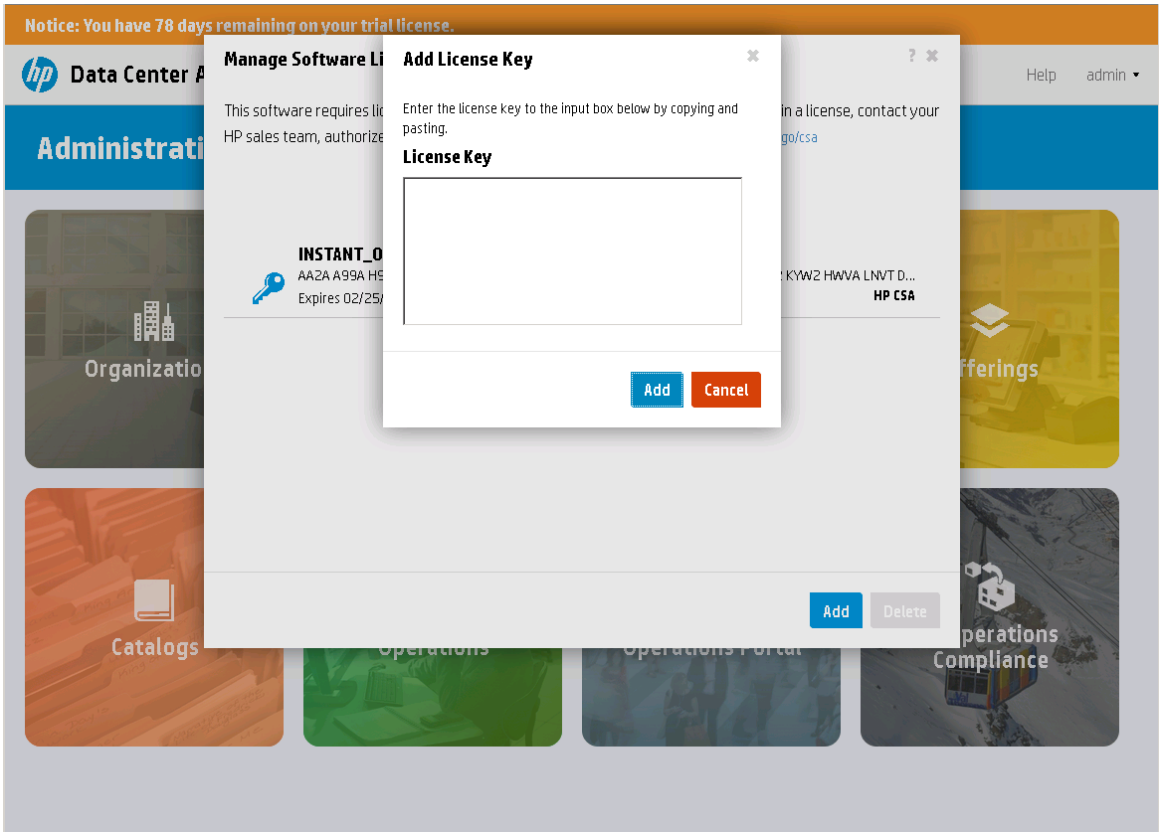


Import an Operations Portal license

The license filename for Operations Portal starts with `DCA-ITOP`.

1. Open the file with a text editor and copy its content.
2. Go to `http://<appliance>:8444/csa` to connect to the Administration console as admin.
3. In the top-right corner, click **admin**.
4. Access **Licensing** and click **Add**.
5. In the **Add License Key** dialog box, paste the content of the license file in the textbox and click

Add.



Import an IT Operations Compliance license

> **Note:** ITOC licenses are generated only for the Premium edition.

The license filename for IT Operations Compliance (ITOC) starts with `DCA-ITOC`.

1. Copy the license file on the appliance in the following location: `/opt/hp/itoc/license/`
2. Rename the file so that it begins with `ITOC`. The filename must be in the format `ITOC*.xml`.
3. Restart the ITOC service in order to import the license.

Example

```
cp DCA-ITOCPREM^1.10_5240283.xml /opt/hp/itoc/license/ITOCPREM^1.10_5240283.xml
/etc/init.d/itoc restart
```

Import an Network Automation license

Network Automation (NA) licenses are generated only for the Premium edition.

NA is not embedded into DCA. Activate the license for the host where NA is running. The license filename for NA will begin with `DCAS`.

1. Copy the license file on host running NA in the following location: `/opt/NA/license.dat`
2. Restart the Truecontrol service.

Example

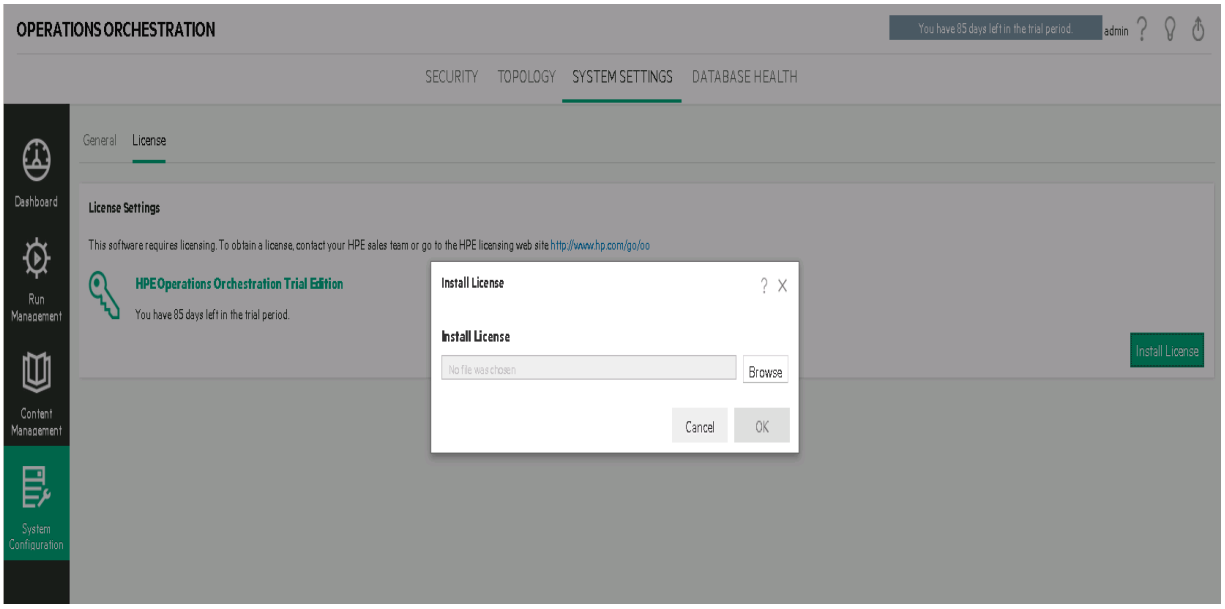
```
cp DCAS_5240277.dat /opt/NA/license.dat

/etc/init.d/truecontrol restart
```

Import an Operations Orchestration license

The license filename for Operations Orchestration starts with `DCA-OO`.

1. Connect to the OO portal.
2. Go to `http://<appliance>:8443/oo` as admin.
3. In the top-right corner, click on the license banner.
4. Click **Install license**.

5. Click **Browse**, select the license file and click **OK**.



DCA accounts and passwords

On a newly deployed appliance, the passwords for the built-in user accounts are set to the value specified in the OVF properties.

These users are:

- Administration Console – **admin** user
- IT Operations Compliance – all built-in users (**itocadmin**, **compliancearchitect**, etc)
- Operations Portal – **consumer** user
- Operations Orchestration – **admin** user
- Server Automation – **admin** user

To change the passwords for these accounts, use the following tool:

```
/opt/opsware/bin/python2 /var/opt/hp/dcaa/utils/changeDCAAadminPassword.pyc --help
```

The tool will set the new password and will make the necessary configurations to keep the appliance working. The tool can be used to set a new password for all accounts at the same time, or one account at a time.

For example, to change the password of Administration Console **admin** user:

```
/opt/opsware/bin/python2 /var/opt/hp/dcaa/utils/changeDCAAadminPassword.pyc -p
'newpassword' -c -a 'ooadminpassword'
```

> **Note:** The password of the OO admin user needs to be supplied, for making necessary configurations on the appliance OO engine, to keep the appliance functional.

DCA high availability (HA) and disaster recovery

You may not want to spend time in a High-Availability setup, but in any case, you should spend time in creating and following rigorous disaster recovery procedures for their environment.

Disaster recovery

Disaster recovery procedures will protect the DCA environment in case of catastrophic failure. Recovering from such a disaster will depend on the type of failure: network, hypervisor, underlying bare metal, disk array, and so on.

Disaster recovery on appliance upgrade can be performed in the following ways:

- Taking a snapshot before running the upgrade and revert to this snapshot if the upgrade fails. Delete this snapshot when it is established that the appliance is running satisfactorily, to prevent any performance degradation from the use of snapshots. Using VMware vSphere HA to protect virtual machines provides detailed information.
- Ensure that you perform regular backups of the DCA virtual machine.
- Read the VMware documentation about backup best practices.

High availability

High availability is maximizing the uptime in case of failure of the hypervisor and/or the underlying server that can be recovered nearly instantaneously 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 DCA is to be used as part of a mission-critical application, you may elect to invest in high-availability setups that cover the DCA appliance.

The DCA appliance is not enabled for an in-product high-availability setup (the ability to run DCA 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).

Hypervisor vendors like VMware or Microsoft have their own high availability implementation, which is largely independent of the actual application that is provided by the virtual machines being protected. Currently, DCA only supports VMware ESXi.

High availability with VMware vSphere HA

VMware vSphere HA protects virtual machines from the following types of failures:

- If the ESX host the VMs running on fails
- If the guest OS inside the VM fails
- If an application inside the VM fails

The basic requirement is for the DCA appliance to run in a vSphere cluster with more than one ESXi host in that cluster.

Case 1 ESXi host failure

Heartbeats are 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 OO, ITOC, and SA is not without risk. It is possible that one or more of these products fail to recover from a crash. 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 DCA appliance and the vCenter server.

If the heartbeats are no longer received from the virtual machine (the guest OS and subsequently, the VMware Tools stops responding) then the vCenter server restarts that virtual machine.

Case 3 Application failure in the virtual machine

Heartbeat support has to be implemented in the application to be monitored, for which VMware has an application monitoring SDK. This feature is not supported in DCA as it has not been added into OO or SA inside DCA. Heartbeats are sent between VMware Tools inside the DCA 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 restarts that virtual machine.

High availability in SA

In SA, 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.

However, DCA is a single core setup with satellite support, so the options are limited because a satellite does not run (other than the Word repository and OS provisioning boot server components) any core functionality. If the DCA appliance goes down or becomes unresponsive, service is interrupted.

Get support

Contact your HPE Support Representative for any information on DCA or on your Support and Maintenance contract.

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`
- The log collection for support for Operations Portal and OO.

Additional support for DCA Suite Premium

The DCA Suite Premium edition provides the following additional support:

- **More Content**: Additional supported content packs available for download
- **Audit and Remediation**: Additional audit and remediation capabilities
- **Larger supported environment**: A single installation of the Premium edition can support up to 3000 licensed servers on a network
- **Provisioning and managed platform**: Solaris x86 support including support for Solaris zones

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 Installation and Administration Guide (Data Center Automation Suite 2016.10)

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 hpedca-docs@hpe.com.

We appreciate your feedback!