Release notes

Data Center Automation Premium 2017.05

Document Release Date: May 2017

Software Release Date: May 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

AMD is a trademark of Advanced Micro Devices, Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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

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

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

UNIX® is a registered trademark of The Open Group.

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/. 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 web site at: https://softwaresupport.hpe.com/. Most of the support areas require that you register as an HPE Passport user to sign in. Many also require a support contract. To register for an HPE Passport ID, click Register on HPE Support site or click Create an Account on the HPE Passport login page.

Table of Contents

Release notes

The DCA suite comprises of containerized applications that are installed and integrated automatically using Docker and Kubernetes technologies. It helps in significantly improving daily operational efficiency in a data center to deliver measurable cost savings.

DCA aims to deliver a unified infrastructure automation suite that provides compliance and remediation as a microservice by leveraging the industry's benchmark and policy standards.

This release of DCA introduces the following features:

- Quick and easy container-based deployment
- Intuitive user interface for simplified database preparation and configuration
- Centralized user authentication
- Suite-level licensing
- Benchmark and policy driven compliance and remediation

The What's new section provides a deeper understanding about the capabilities of the DCA 2017.05 offering.

What's new

This release of DCA includes the following features:

Container-based deployment

DCA is deployed in a container-based mode by leveraging Docker and Kubernetes technologies. In this mode, components are bundled as a suite, installed as containerized applications, and integrated automatically. The components work seamlessly as integral modules within DCA to provide a seamless user experience.

Single pane user interface

The DCA console provides a single pane view of the essential operational metrics of your data center. It graphically represents the compliance states of various resources within your infrastructure.

Centralized user authentication

DCA includes the HPE Identify Manager (IdM) for user authentication. The suite components and IdM are integrated with the same LDAP server (internal or external) to achieve centralized user authentication and single sign-on. Instead of logging in to each individual product, users can now log in to a centralized DCA console. Once logged in to this portal, users can access all suite modules and access one module from another without the need to enter a user name and password again.

Suite-level licensing

Unlike Classic suites that require a separate license file for each suite component, DCA requires only one suite license. However, for this release of DCA, you will require separate licenses of the following products:

- Server Automation (SA)

- Operations Bridge Reporter (OBR)
- Cloud Optimizer (CO)

Compliance and remediation

DCA introduces compliance and remediation as a microservice. It reduces time to audit by automating enforcement, real-time reporting, integrated remediation, and auditing. It also provides up-to-date compliance information to help you control sprawl and compliance drift using a well-defined process of end-to-end lifecycle and policy management.

Using DCA, you can author (create and customize) benchmarks and policies that are available out-of-the-box. The compliance scan and remediation process for policies and benchmarks associated to resources and resource groups can be scheduled to run according to your time of convenience, as well as on demand.

Compliance dashboards allow DCA users to view the compliance scan status of policies and benchmarks that are run against infrastructure resources in that instance of DCA. In addition, it provides an extensive analysis of the resource compliance trends.

Provisioning and configuration

DCA leverages Server Automation to provide the OS and database provisioning on resources, so that users can configure resources tailored to their needs, even in multi-vendor environments. In addition, DCA also provides database and middleware patching on resources. It helps in identifying and remediating vulnerable systems based on defined policies to maintain compliance.

Enhancements

DCA 2017.05 is the first release of the product and does not have enhancements to report.

Fixed defects

DCA 2017.05 is the first release of the product and does not have fixed defects to report.

Known issues, limitations, and workarounds

Known issues

Component	Issue ID	Issue description
ChatOps	QCCR1D232081	If the command syntax is not correct, no response will be returned
	QCCR1D235671	A part of the resource name in the response for 'get resource' command appears as a link.

Compliance		The scan and remediation functionality for **Docker host** only works with the following workaround: **Workaround:** 1. Add the Docker Host resource using the discover_resources.sh script. 2. Deploy the resource from CIS-Compliant Docker Host template. This will create a docker daemon resource linked to the previously added platform resource. 3. Create a resource group. 4. Add the platform resource and the docker_daemon resource group to the newly created resource group. 5. Associate the CIS policy to resource group. 6. Create a maintenance schedule. 7. During the maintenance window, a compliance scan and remediation should run. The compliance functionality for **Docker images** does not work in this release.
	QCCR1D238975	When running a large number of parallel ad hoc compliance scans (approx. 200 jobs) on SA synced resources, some jobs will fail as the OO flow fails to trigger the SA server script.
	QCCR1D239225	When more than 25 concurrent ad hoc compliance scan jobs are run on agentless resources, many of the jobs fail to return valid compliance results. **Workaround:** Run an ad hoc compliance scan on 15 resources for the first run before increasing the number of ad hoc compliance scan jobs to 25.
	QCCR1D239301	In case of ad hoc compliance scan jobs, the reasons for non-compliance is not complete for some of the controls. Hence, they display only the actual values and not the expected ones.
		When you run remediation on a failed ad hoc scan, the OO logs display only the failed rules, without providing the reason for failure.
	QCCR1D239276	When you run a remediation job for agentless resources, all rules for the PCI policy may fail without displaying a reason. This is due to the "RHEL Compatibles:Set Maximux Password Age For Active Accounts" rule, which is not compliant when you run scan compliance job.

	QCCR1D239116	Few rules fail to get imported from a benchmark and display an invalid Control Lifecycle state error.
Patching		For the MSSQL patching template '*MSSQL 2014 with latest patch on existing Windows 2012R2*', the database created ("*MSSQL2012R2DB*") displays target as *'MSSQLINST'* instead of the target system name. However, the software resource created displays the appropriate target name.
Provisioning	QCCR1D236129	Subsequent deployments are skipped due to existing resource types in UCMDB.
Search	QCCR1D235534	The search operation on some of the pages are case sensitive.

Limitations

Component	Issues ID	Limitation
ITOM CDF		In a multiple-master node environment, the master nodes defined as **HA_NGINX_ NODES** in the **install. properties** file should be installed first.
		The ITOM CDF supports English, French, German, and Spanish. However, the License (AutoPass License Manager) user interface only supports the English interface.
		In a multiple-master node environment, when the node where the Ingress container is located runs into error or hangs, you may have problems accessing the Management Portal of the ITOM CDF. This happens because the Ingress and Egress service do not support High Availability (HA) in a multiple-master node environment.
		When the vault token expires during the ITOM CDF installation, the installation may fail. **Workaround:** Manually run the command: `update_kubeVaultToken` in folder /opt/kubernetes/bin of the master node.
		When you uninstall the ITOM CDF on a virtual machine, the virtual machine may hang. **Workaround:** Manually restart the virtual machine.

		The following issues exist when working in Internet Explorer 11: • After you click **ADMINISTRATION > User Management**>**ADD** to add a new user and then click **SAVE**, if you refresh the browser, the newly added user is not in the user list. • After you click **ADMINISTRATION > User Management**> ⋮ > **DELETE**, and then click **DELETE**, if you refresh the browser, the newly deleted user is still in the user list. • After you click **ADMINISTRATION > Nodes**>**Predefined Labels**, enter a new label and then click **[+]** , if you refresh the browser, the newly added label is not in the label list. • After you click **ADMINISTRATION > Nodes**>**Predefined Labels** and then click **[-]** to delete a label, if you refresh the browser, the newly deleted label is still in the label list. **Workaround 1:** Open developer tools (press F12) and then refresh after you have added a record. **Workaround 2:** Use other browsers.
		If you use %, " , \ and space in the User Name field in **ADMINISTRATION** > **User Management** > **ADD**, **SAVE** does not work, and it does not display an error message as well. **Workaround:** Do not use the following characters for **User Name**: % , ", \, <blank>.
		Sometimes a pod may run into errors or display a `CrashLoopBackOff` status when migrating from one node to another node. This issue may occur because the vault token is not generated. **Workaround:** If the failed pod is created by the Replication Controller of deployment (containing a random string at the end of the pod name, such as `idm-848511036-5ev30` or `idm-t56ui`), delete the pod and generate a new pod. Instead, you can also run `kube-restart.sh` in folder $K8S_HOME/bin of the node where the pod is located.

DCA console	QCCR1D239191	The following discrepancies are seen in the **Resource Management** > **Resources** page: • When all resources are selected, instead of displaying the number of resources selected, the option **Multiple Selected** is displayed. • Every time you select or clear the selection for a resource, "1" gets appended to the **Multiple Selected** string. • Each time the resource selection is cleared, the selected resource count decreases by 1, but when the resource is selected again, the resource count does not increase. As a result, the view can show a negative number for the resource count selected.
	QCCR1D239315	While specifying the Maintenance Schedule details, the **Maintenance Window Type** displays the following options: **Read** and **Write**. The Write mode does not work for this release of DCA.

Related topics

Troubleshoot

Deprecations

DCA 2017.05 is the first release of the product and there are no deprecations to report.

Patch releases

DCA 2017.05 is the first release of the product and there are no patch releases to report.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email.

Add the following information in the subject line: Feedback on Data Center Automation 2017.05 - Premium

Just add your feedback to the email and send your feedback to docs.feedback@hpe.com.

We appreciate your feedback.