HP Continuous Delivery Automation

Release Notes

Software version: 1.10, December, 2012

This document provides an overview of HP Continuous Delivery Automation (HP CDA) for Release 1.10. It contains important information not included in the manuals or in online help.

In This Version

HP Continuous Delivery Automation (HP CDA) provides a model-driven approach to DevOps collaboration, automation of application deployment, and monitoring. HP CDA enables customers to focus on their core applications and to drive business values while reducing costs, risks, and time to perform provisioning and deployment tasks. Core HP CDA features include:

- Modeling the application and infrastructure configuration to deliver infrastructure-as-code for deployment and provisioning
- Full artifact version control, role-based access, application lifecycle management, and Definitive Software Library (DSL)
- Application deployment management using configurable tool options
- Infrastructure provisioning management across hybrid environments
- Embedded monitoring deployment in conjunction with application deployment

For more information about supported hardware and software, refer to the *HP Continuous Delivery Automation Platform and Software Support Matrix*, available at: **http://h20230.www2.hp.com/selfsolve/manuals**

Documentation Updates

The first page of this document contains the following identifying information:

- Version number, which indicates the software version
- Publish date, which changes each time the document is updated

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

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

Installation Notes

Installation requirements, as well as instructions for installing HP Continuous Delivery Automation, are documented in the *HP Continuous Delivery Automation Installation and Configuration Guide* provided in Adobe Acrobat (`.pdf`) format. The document file is included on the product's electronic media under the following folder:

cda-iso-1.10\CDA 1.10\Documentation

Contents

Known Problems, Limitations and Workarounds

General

HP recommends following Microsoft security best practices.

QCCR1M6497 HP recommends following Microsoft security best practices.

Description	HP recommends that you configure the Microsoft Windows Server system running HP CDA 1.10 as per Microsoft security best practices, as well as your organization's security policies and processes.
Workaround	Please refer to the link below. **Secure Windows Server** http://technet.microsoft.com/en-us/library/dd548350%28v=ws.10%29.aspx

HP CDA does not time out after waiting for a response from a command that stops responding.

QCCR1M2749 Provision operation does not timeout if knife bootstrap command is hung.

Description	HP CDA does not time out and waits for an indefinite period of time for a response from a command that stops responding. For example, a provision operation does not time out if the `knife bootstrap` command stops responding during the provisioning operation.
Workaround	Use job Timeout values that can be specified when launching an operation.

Limited scripting tool support by HP CDA.

QCCR1M2347 Executed Script common component does not specify interpreter to run script.

Description	HP CDA currently supports only the shell on Linux platforms and the PowerShell on Microsoft Windows platforms as the scripting tools.
Workaround	Not applicable.

For Events, the Task Reports and Lifecycle tabs may not display information.

QCCR1M3291 Task Reports and Lifecycle tabs in Events page do not show any information.

Description	The Task Reports and the Lifecycle tabs in the Events section may not display sufficient information.
Workaround	No known workarounds at present.

HP Server Automation deployer always replaces existing file content.

QCCR1M 2303 SA Deployer replaces the file content even if "Replace" checkbox is unchecked.

Description	The HP Server Automation deployer replaces existing placed file components. HP SA does not use the “Replace” checkbox. Even if the checkbox is **not** selected, HP SA will over-write existing files.
Workaround	No workaround at this time.

License activation delay.

QCCR1M6468 License activation delay.

Description	After you apply for a license, there may be a delay for the license to be activated. This happens when a license is generated in one time zone and applied in a different time zone. The license will be activated after a few hours. For example, a license is generated in the PST and is applied on a system set to follow the EST. In this case, the license should be generated as per the EST time zone. This scenario may be applicable to HP internal customers, who will be generating licenses.
Workaround	Check the time zones where the license will be applied and get the appropriate license from HP.

Email alert for expired HP CDA license contains incorrect information.

QCCR1M3489 License information email alert has incorrect information.

Description	When HP CDA sends a license alert regarding an expired license, the email contains incorrect information. “License Conditions Valid for” are incorrectly listed as “0.” “Product Features” is incorrectly listed as “No.”
Workaround	As a workaround, you can view licensed product features and the actual number of instances provisioned from the HP CDA Administration tab. Administration > Configuration > License.

Applications

Software with custom tags creates a null pointer exception.

QCCR1M2637 Exported software with custom tag has issues.

Description	After an export and import operation of a software application with custom tags, HP CDA displays a null pointer exception when you try to access the software. HP CDA imports the application, but does not import the custom tags associated with the application.
Workaround	You must export or import the tags before exporting or importing the software application with which the tags are associated. You can use HP CDA's Tag Management feature to import or export custom tags associated with a software application.

Application deployment fails while using HTTPS to download software artifacts from external links.

QCCR1M6522 Document that when using https as external source, you must store the password with full URL string or use wildcard *.

Description	When you use HTTPS as the protocol to download software artifacts from external URLs during application deployment, the deployment fails.
Workaround	Store the password with a full URL string or use the wildcard character (*).

Platforms

CLI `get` option cannot return details for server groups with non-English names.

QCCR1M6109 CLI - I18N: Not able to get the details of server group, named with Unicode characters though the servergroup is added successfully.

Description	The command line integration (CLI) `get` option does not list `servergroup` details for server groups that have Unicode character names.
Workaround	Use the CLI `list` option to get sever group details.

Monitors

Cannot add or modify monitoring policies for deployed applications.

QCCR1M2128 Not able to apply monitoring tools for the deployed application.

Description	HP CDA does not support addition or modification of monitoring tools for an application that is already deployed.
Workaround	You can un-deploy the application, assign the required monitoring policies, and then deploy the application.

Deploying multiple HP SiteScope policies can generate the “non-unique” exception.

QCCR1M2299 Multiple SiteScopes can create non-unique exceptions when processing events.

Description	Deployment of the same HP SiteScope policy to the same target directory from two or more HP SiteScope systems generates an exception.
Workaround	You can avoid this problem if you deploy the monitors of each HP SiteScope installation to different target directories.

Cannot add a monitor definition multiple times using different parameters.

QCCR1M3219 Can't have two monitors with the same definition in a policy multiple times with different parameters (e.g., two URL monitors).

Description	You cannot add a monitor definition to the same policy with multiple parameter definitions. For example, the URL latency monitor that takes the URL as the parameter cannot be defined in the same policy with multiple URL parameters.
Workaround	You must create separate policies for specific monitor definitions.

"Deploying Monitoring Application" with HP OM policy fails although server test connection passed.

QCCR1M 6610 OM Monitor server test connection passes even when the credentials are incorrect.

Description	When you deploy an application that is configured with an HP CDA Operations Manager policy, "Deploying Monitoring Application" fails. Failure is unexpected, because the server test connection passed successfully. This could happen because the HP OM server test connection passes, even when the credentials are incorrect.
Workaround	Make sure that correct credentials are provided so that the application can deploy successfully along with the HP CDA policy for Operations Manager. You can view the credentials in the HP CDA user interface on Monitoring > Monitor Administration > Monitor Servers.

NPE when re-monitoring to an HP Cloud System Diagnostics deployment.

QCCR1M6616 NPE when re-monitoring to an HPCS Diagnostics deployment.

Description	In case when a diagnostic server, as well the target nodes being monitored, is hosted on HP Cloud Services, a re-monitoring job fails with exception.
Workaround	Undeploy the application, modify monitoring policies as per requirement and re-deploy the application.

Cloud Administration Dashboard, Cloud Installation Dashboard, and Cloud Connector

No support for importing an operating system image from the internet if there is a firewall in between.

QCCR1M6330 Creating an image failed with QCOW2 format.

Description	Cloud Administration Dashboard does not support importing operating system images from the internet if there is a firewall in between.
Workaround	Provide a URL to the image which is in a local intranet or in a network where there is no firewall between the node hosting the image and the node running Glance. Copy image(s) to a local disk on the node and run Glance to load the image using the following steps (customer environment determines information in < >). 1. Set up the Glance environment before running Glance: export OS_REGION_NAME=<RegionOne> export OS_PASSWORD=<password> export OS_AUTH_URL=http://<IP address of the node> export OS_USERNAME=<Admin> export OS_TENANT_NAME=<AdminProject> 2. Go to the image location on the node. 3. Run. Example: `# glance add name= <"Fedora 16 x86_64"> is_public=true container_format=bare disk_format=qcow2 <precise-server-cloudimg-amd64-disk1.img>`

Creating a volume that appears to be within size limits fails.

QCCR1M6128 Create a volume of a size that appears to be acceptable; it fails, but is still listed in the Volume table.

Description	When a user creates a volume of a size that appears to be within the Volume Quotas, the system displays a message that the volume was created, but the volume was not created successfully.
Workaround	1. If you are logged in as an Administrator, Nova returns all volumes. When you attempt to create a new volume through the dashboard, you may see in **Volume Quotas** there are no volumes available to create. In this case, log out and log back in as a User rather than an Administrator. 2. System admin needs to create a pool for volumes that is larger than what is specified in the limit; OR 3. Reduce the size of the volume limit to match or be smaller than what is actually available on the disk.

Keystone authorization errors when users (instead of Admins) create projects.

QCCR1M6430 Keystone invalidates user's authorization token when user's role within a project is changed by the user.

Description	When a user creates a project, the user will not automatically be added as a member of that project and cannot add himself as a user in the project. A user cannot delete a project in which he or she is a member. This happens because when a user's role within a project changes, the Keystone service invalidates his or her login authorization token. The user then sees unrelated error messages that do not explain this issue.
Workaround	Have the **Admin** user perform the following tasks: • Create other Admin Users with the domain-specific roles Domain Administrator and Domain Architect • Create Projects Other Admin Users tasks: • create non-admin users • add users to projects when they are not logged in • create images

After deleting and recreating a Fixed IP Network, launching a VM results in an error and fails.

QCCR1M6373 Provisioning fails if an Instance randomly selects a deleted network ID.

Description	When a user deletes a Fixed IP Network through the dashboard, the system is not updating the table value. Therefore, provisioning fails if a new instance randomly selects this 'deleted' Network ID.
Workaround	Manually delete the entries in the `fixed_ips` table for the deleted network: 1. Delete the network from the Cloud Administration Dashboard. 2. Connect to the nova database: #: sudo –u postgres psql <provide password at prompt> #: \c nova 3. Run this query to check for the deleted network ID: #: select * from fixed_ips; 4. Delete the network ID: #: delete from fixed_ips where network_id=<deleted network id> 5. Recreate the network within the Cloud Administration Dashboard.

The Infrastructure Topology and Design Documents are interdependent; document deletion errors.

QCCR1M6340 UI binding document can be deleted from under the associated infrastructure topology document.

Description	There are 3 types of topology documents: 1. Infrastructure Design - This document represents the configuration to be used when provisioning the referenced topology. 2. Infrastructure Topology - This document represents the Infrastructure topology that will be created on provision. 3. Infrastructure Metadata - This document contains metadata used by the Topology Designer for correct display of graphical entities. The Infrastructure Topology and Design Documents are interdependent; and Topology and Metadata documents have a 1:1 relationship.
Workaround	The binding document associated to a topology document needs to be deleted if the referenced topology document is deleted from the system. Since topology and metadata documents have a 1:1 relationship, if one is deleted the other will be impacted and require updating.

Operating Systems not listed on server group Properties in HP CDA platform Designer.

QCCR1M6134 HP CDA - Platform >Designer tab, OS list not listed in the Assigned Capabilities in HW&OS tab.

Description	Operating systems are not shown for server group components in an infrastructure. When you display the platform Designer and access server group properties, operating systems are not listed.
Workaround	Create an infrastructure based on a specific HP Cloud Connector resource binding document. Then set the operating system. To set the operating system, follow the process (documented in online help) to use platform Designer to update an infrastructure template's hardware and operating systems.

Logging into Cloud Administration Dashboard fails if user has not been added to any projects.

QCCR1M6024 Login fails if user has no project/role specified.

Description	If a user is created in the Cloud Administration Dashboard but is not added to any projects, user will not be able to log into the dashboard.
Workaround	The Administrator should add the user to a project either through the Create User process or during project setup.

Integrations with HP CDA

Chef 0.10.6 does not set error return codes.

QCCR1M3318 Chef Issue: Deployment succeeds and the application start failed with Deployment Exception: Unable to complete deployment.

Description	Chef does not set error return codes. When an application deployment fails, the status is reported as" success." However, when you attempt to start the application, it leads to an exception. Application deployment should report as a "fail" instead of giving the exception during start.
Workaround	All executed scripts run with Chef must explicitly return non-zero return codes on failure.

HP ALM-CDA integration does not allow certain special characters in the host name.

QCCR1M2865 CDA-ALM: Launching ALM Report page giving error.

Description	When using the HP ALM-CDA integration, the HP ALM server host name cannot contain the hyphen or underscore characters.
Workaround	Use the IP address instead of using host name.

Enabling ICMP in an HP Cloudsystem Matrix template firewall fails with HP Cloud Service.

QCCR1M 6495 Enabling ICMP in MOE template firewall does not work with HPCS due to port being 0 (-1 expected in HPCS).

Description	Adding ICMP in an HP Cloudsystem Matrix template firewall opens the ICMP for only non-negative ports. Nagios monitoring needs the ICMP ping to work, and HP Cloud Service needs ICMP to be opened for port from -1 to -1 for the ping.
Workaround	Edit the security group of the provisioned host to add ICMP from port -1 to -1.

Port configured in platform software connections is not enabled in HP Cloud System security group.

QCCR1M 6493 Port configured in platform software connections is not enabled in HPCS provisioned security group.

Description	Any ports configured in platform endpoints and connections are not opened in the security group of provisioned HP Cloud Service hosts.
Workaround	Manually open the ports in the security group after provisioning.

Diagnostic probe name mismatch in HP Cloud Service deployments.

QCCR1M 6597 Parameter {server.hostname} returns different values at provisioning and deployment times leading to Diagnostic probe name mismatch for HPCS deployments.

Description	When deploying platform software (e.g., the Diagnostic Probe) the hostname provided by HP CDA (i.e. "`${server.hostname}`") during provisioning is different than the hostname by HP CDA when deploying application software to these provisioned hosts. In the case of Diagnostics, this can cause problems deploying thresholds for monitoring the application software because the probe names are derived from hostnames.
Workaround	The workaround, if any, will depend on the platform software (i.e., whether hostnames are used to configure it when applications are deployed). In the case of Diagnostics, the Platform Software Deploy workflow can be changed to simply use `${server.ipaddress}` instead of `${server.hostname}`. From the Platform tab, Browse Software, select the Diagnostics probe software and go to the Workflows tab. With the Deploy workflow you will see several steps. One of the last steps will have this "`application.server.hostname`" as an input component parameter. Edit this parameter to refer to `${server.ipaddress}`.

All HP Cloud System provisioned hosts have the same host name.

QCCR1M 6617 All HPCS provisioned hosts have the same host name.

Description	All HPCS provisioned hosts have the same hostname. This can cause problems for applications or platform software that use hostnames. In the case of Diagnostics, the system metric collectors cannot be used with HP Cloud Services because these non-unique hostnames prevent Diagnostics from distinguishing between system metrics reported from different hosts. The Diagnostics UI will only present on Infrastructure Host and it's not clear which host the measurements represent.
Workaround	There is currently no resolution to this problem other than using a different tool (e.g., SiteScope, Operations Manager, or Nagios) to monitor operating system metrics.

HP CDA - CSA Integration: Platform subscription fails due to invalid Boolean value.

QCCR1M 6590 CDA - CSA Integration: platform subscription failed due to the supplied value (true) is not set to a valid Boolean response of either Yes or No.

Description	Subscriptions for platform software and applications fail in HP CSA when HP CDA publishes Boolean values that are invalid in HP CSA.
Workaround	When creating an application or platform software that will be published to HP CSA, all parameters with Parameter Type set to Boolean must have True Value set to "true" and False Value set to "false." Use all lower case.

HP CSA publishing does not accept predefined Boolean values.

QCCR1M 6518 HP CSA publishing does not accept predefined Boolean values.

Description	Boolean parameters for Platform Software or Applications when used with HP CDA-CSA integration: Publishing of Platform and Application from HP CDA-to-CSA will succeed. However subscription from HP CSA-to-CDA will fail.
Workaround	Boolean parameters for Platform Software or Applications when used with HP CDA-CSA integration: 1. Will work only when the Boolean parameter value = "true" / "false" (lowercase) 2. Doesn't work with the current default Values "True" / "False" 3. Doesn't work with any custom values such as "Value true" / "Value false" or any other.

Security and Passwords

Default for sending Diagnostics credentials is cleartext.

QCCR1M6360 Diagnostics credentials are sent in cleartext.

Description	HP CDA uses basic authentication to communicate with a Diagnostics server. This type of authentication sends the Diagnostics usernames and passwords in cleartext.
Workaround	This situation can be avoided by using HTTPS instead of HTTP. However, the Diagnostics server needs to have a certificate installed for authenticating itself, and HP CDA needs to trust the authority issuing the certificate. Depending on the environment, setting up certificates is burdensome and passing credentials in cleartext may not be a concern. When configuring the monitoring connections for your Diagnostics servers, use the `diag_ssl` parameter to control whether HTTP or HTTPS is used. Please note the default setting (false) will use HTTP, so by default, HP CDA will send monitoring server credentials in cleartext. HP recommends changing this parameter to use HTTPS (true) in all but very isolated testing environments. Change the `diag_ssl` parameter to "true" for your Diagnostics monitoring servers.

Default for sending Nagios credentials is cleartext.

QCCR1M6359 Sending Nagios login credentials in cleartext.

Description	HP CDA uses basic authentication to communicate with a Nagios server. This type of authentication sends the Nagios usernames and passwords in cleartext.
Workaround	This situation can be avoided by using HTTPS instead of HTTP. However, the Nagios server needs to have a certificate installed for authenticating itself and HP CDA needs to trust the authority issuing the certificate. Depending on the environment, setting up certificates is burdensome and passing credentials in cleartext may not be a concern. When configuring the monitoring connections for your Nagios servers, use the `nag_ssl` parameter to control weather HTTP or HTTPS is used. Please note the default setting (false) will use HTTP, so by default, HP CDA will send monitoring server credentials in cleartext. HP recommends changing this parameter to use HTTPS (true) in all but very isolated testing environments.

OM software monitoring contains provision to pass passwords in cleartext.

QCCR1M6377 Operations manager sends passwords in cleartext as part of UI drill down.

Description	In HP CDA, the contextual launch for operations manager contains default password and username which may be different in your case and default contextual launch URL may fail.
Workaround	The user and password should be removed from the URL "&user=username&passwd=password" http://@{om_server}:@{om_port}/OvCgi/ito_op_applet_cgi.ovpl?gui.svcgraph.name=Oracle_@{oracle.instance.name}_@@@{server_hostname}&webstart=true&gui.msgbrw.filter.nodes=@{server_hostname}&gui.msgbrw.brwpane=true This should be done for all the HP Operations Manager related monitors.

Additional Information

How to set up Nagios integration with HP CDA.

CR6475 How to set up Nagios integration with HP CDA.

Copy the files from the HP CDA-installed directory to the tmp folder on the Nagios server. Files are available in the following directory:

1. Linux /opt/hp/cda/1.10/integration/monitoring/nagios.
2. (Windows users) Navigate to the directory:

   C:\CDA\1.10\integration\monitoring\nagios.

Read the Readme.txt file for more information

Legal Notices

Warranty

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

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

- Adobe® is a trademark of Adobe Systems Incorporated.
- Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- UNIX® is a registered trademark of The Open Group.
- RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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

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

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:
http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page. You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: *www.hp.com/go/hpsoftwaresupport* This web site provides contact information and details about the products, services, and support that HP Software offers.

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

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

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