FEDERATION ENTERPRISE HYBRID CLOUD 3.5.0

Release Notes

ABSTRACT

This Release Notes document provides details of new features and resources for the Federation Enterprise Hybrid Cloud v3.5.0.

February 2016

v1.0






Published February 2016

Federation Enterprise Hybrid Cloud v3.5.0 Release Notes

Part Number H14561

Contents

Overview

These EHC v3.5.0 Release Notes cover the following topics:

- What's New in EHC v3.5
- EHC v3.5 Software Table
- Supported FEHC v3.5 Platforms and Configurations
- Upgrades for this release
- Resolved Issues
- Known Issues
- References

What's New

The Federation Hybrid Cloud Solution v3.5 includes the following new platform and feature set updates:

- VMware Platform: vSphere v6.0 support
- VMware Platform: Microsoft SQL Server 2012 SP2 support
- VMware Platform: vRealize Orchestrator support
- VMware Platform: vRealize suite version updates
- VMware Platform: Platform Services Controller (PSC)
- VMware Platform: vCNS support removed
- Storage Platform: EMC ViPR v2.4 support
- Storage Platform: XtremIO DR support
- Storage Platform: VMAX3 DR support
- Encryption Services: CloudLink SecureVM v5.0 support
- Data Protection Backup Platform: Updated EMC Avamar v7.2 support
- Data Protection Backup Feature Set: Add EHC BaaS to existing or imported VMs
- Data Protection DR Platform: Removed VMware NSX dependency for DR
- Data Protection DR Platform: EMC RecoverPoint and vCenter SRM version updates
- Data Protection DR Feature Set: Add EHC DRaaS to existing or imported VMs
- VCE Platform: VxBlock Hybrid Management Pod model
- VCE Platform: RCM Alignment
- Sizing: Updated EHC Sizing Tool
- Documentation: Updated Documentation Suite

VMware Platform

EHC v3.5.0 is based on the VMware vSphere v6.0 platform only.

The database support for VMware vSphere and vRealize components has been updated to Microsoft SQL Server 2012 SP2.

vRealize Orchestrator v6.0.2 is now fully supported in place of vCenter Orchestrator.

Component version updates for VMware NSX and the vRealize Suite, including vRealize Automation, vRealize Operations Manager, vRealize Business Standard. See EHC v3.5 ESSM.

VMware Platform Services Controller (PSC) replaces vCenter SSO in EHC. PSC is a new service in vSphere 6 that handles the infrastructure security functions such as vCenter Single Sign-On, licensing, and server reservation.

EHC has removed support for VMware vCNS as of EHC v3.5

Storage Platform

EHC v3.5.0 is based on EMC ViPR v2.4.1 that provides the following platform support:

- EMC XtremIO v4.0.2-80
- EMC XtremIO with RecoverPoint for EHC DR

DR support for VMAX3 is now available by configuring VMAX3 behind VPLEX Local devices leveraging VPLEX splitter and RecoverPoint

Encryption Services

EHC v3.5 provides Encryption Services with CloudLink SecureVM v5.0

Data Protection Backup

Platform: EHC v3.5 provides updated support for EMC Avamar v7.2

Feature Set: EHC v3.5 provides the ability to assign EHC BaaS services to existing and imported virtual machines. New workflow 'Ingest for DP' called during Bulk Import.

Data Protection Disaster Recovery Platform

Platform: EHC v3.5 removes the dependency on VMware NSX for EHC DR. During the installation of EHC DR Initialization Main, there is option of not choosing NSX.

Note: Without NSX, automation of network re-convergence for EHC Automation and Tenant pods must be configured manually or as part of a professional services engagement. Maintenance of the alternative network convergence strategy is outside the scope of EHC support.

Platform: EMC RecoverPoint and vCenter SRM version updates. See EHC v3.5 ESSM.

Feature Set: EHC v3.5 provides the ability to assign EHC DRaaS services to imported virtual machines. New workflow 'Ingest for DR' called during Bulk Import.

VCE Platform

EHC Hybrid Management model on VCE VxBlock 340, 540 and 740 series now utilizes VCE AMP2-HAP resources for EHC Core Pod components for single-site and DR solutions (no separate Core Pod required)

EHC v3.5 supports VCE RCM v6.0.5 at release

EHC Sizing Tool

The EHC Engineering Sizing Tool as been updated to support EHC v3.5. The sizing process is now platform-driven providing guardrails for EHC hardware configuration across VCE and BYO platforms. Output now also includes sizing considerations for VxBlock AMP components.

Documentation Suite

Replacing the previous EHC Operations Guide, all core EHC use cases are now available in the EHC Administration Guide while all operational management use cases are available in the EHC Infrastructure and Operations Management Guide.

New documents available in the EHC 3.5 release include the VMware Integrated OpenStack Guide and the vRealize Code Stream Guide.

EHC v3.5 Software Table

Please refer to the official EMC Elab ESSM for up to date supported software versions for EHC v3.5 at https://elabnavigator.emc.com

Note: The component versions listed in the EHC ESSM may change over time, therefore for up to date versions, always refer to the official online version of the EHC ESSM.

Supported EHC Platforms and Configurations

The following are high-level guidelines for supported configurations in the Federation Enterprise Hybrid Cloud solution.

Federation EHC Storage Platform Support

The configurations stated in Table 1 are the supported configuration for EHC Tenant/Workload Pod storage managed via EMC ViPR.

Table 1. EHC v3.5 supported Storage Platform support

Storage Array	Single Site	Single Site with VPLEX	Dual Site CA with VPLEX	Dual Site DR with RP
VMAX	Yes	Yes	Yes	Yes
VMAX3	Yes	Yes	Yes	Yes *
VNX	Yes	Yes	Yes	Yes
XtremIO	Yes	Yes	Yes	Yes
ScaleIO	Yes	No	No	No

* VMAX3 is supported for disaster recovery with VPLEX Local, using the VPLEX Splitter with RecoverPoint. Both Source and Target must be VMAX3 arrays.

Note: EMC Isilon is not supported for VMFS and is only to be used for Hadoop File Systems or to manually provide file services within a VM.

EHC Hardware Platform Support

Table 2 displays the supported hardware platforms for EHC deployments.

Table 2. EHC supported Hardware Platforms

	Vblock	VxBlock	VxRack*	VxRail*	BYO
CMP	Yes	Yes	Yes	No	Yes
STaaS	Yes	Yes	Yes	No	Yes
IaaS	Yes	Yes	Yes	Yes	Yes
BaaS	Yes	Yes	Yes	No	Yes
CA	Yes	Yes**	No	No	Yes
DR	Yes	Yes	No	No	Yes

* Support for VCE VxRack and VxRail expected post-EHC v3.5 release.

** For VCE VxBlock in EHC CA deployments a VCE IA (Impact Assessment) is required

Federation EHC Endpoints

The Federation EHC solution can leverage public and private endpoints, as well as remote endpoints, which are referred to as managed endpoints.

Table 3. Supported Endpoints

Endpoint Location	Endpoint Name/Type	Supported Federation EHC Services
Private	VMware vCenter	IaaS, STaaS, BaaS, Continuous Availability, DRaaS, Applications-aaS
Remote	VMware vCenter	IaaS only (Managed Endpoint)
Public	VMware vCloud Air Amazon AWS EMC Powered Service Providers (using vCD)	IaaS (Managed Public Cloud Blueprints)

Note: Microsoft Azure is currently not a supported Endpoint in VMware vRA v6.2.3

Federation EHC Tenant Configurations

The Federation EHC solution can include multiple Tenants. An EHC Tenant includes EHC services, while a native vRA tenant does not include EHC services.

Table 4. Federation EHC Tenants

Configuration	Supported Services	Additional Requirements
Single EHC Tenant	All EHC services	None
Single EHC Tenant + vRA Tenant	All EHC services for EHC Tenant IaaS-only for native vRA Tenant	None
Multiple EHC Tenants	All EHC Services	Per Additional Tenant: vCenter Server, vCO, ViPR Project, Avamar, NSX Manager
Multiple vRA Tenants (native)	IaaS-only	None

Note: Native vRA tenants have no integration with or dependency on the EHC workflows and may exist as a standard vRA construct leveraging Infrastructure services only.

Federation EHC Data Protection Backup

The Federation EHC solution provides backup and restore services for tenant virtual machines. The required components are listed in x.

Table 5. Federation EHC data Protection Backup components

Component	Supported	Comments
EMC Avamar	Yes	Physical Avamar appliance required for EHC BaaS
EMC Avamar VE	No	Virtual Avamar appliance may be used for POC only

Component	Supported	Comments
EMC Data Domain	Yes	(optional) Configured as a backup target behind EMC Avamar
EMC Networker	No	
EMC Data Protection Advisor	Yes	(optional) Required for some virtual machine level reports

Federation EHC Continuous Availability Configurations

The EHC Continuous Availability (CA) solution provides continuous availability and disaster avoidance across a maximum of 2 EHC sites. The EHC CA solution is supported by EMC VPLEX only. MetroPoint is not supported.

Table 6. Federation EHC Continuous Availability

Configuration	Supported Services	Additional Requirements
Cross-Connect	IaaS, STaaS, BaaS, Continuous Availability, Applications-aaS	None
Non Cross-Connect	IaaS, STaaS, BaaS, Continuous Availability, Applications-aaS	None

Supported storage arrays behind VPLEX (cross-connect and non cross-connect):

- EMC VMAX
- EMC VMAX3
- EMC VNX
- EMC XtremIO

Federation EHC Disaster Recovery Configurations

The EHC Disaster Recovery (DR) solution provides disaster recovery services across a maximum of 2 EHC sites. The EHC DR solution is supported by EMC RecoverPoint only. MetroPoint is not supported.

Table 7 highlights the required components for the EHC DR solution.

Table 7. Federation EHC Disaster Recovery

Required Component	Unsupported	Comments
RecoverPoint CL/EX Physical RP Appliances	RecoverPoint SE vRPA, RP4VM	
EMC VNX, VMAX2, VMAX3*, XtremIO**	ScaleIO	* VMAX3 is supported for disaster recovery with VPLEX Local, using the VPLEX Splitter with RecoverPoint. Both Source and Target must be VMAX3 arrays. ** Both source and target storage arrays must be XtremIO

Required Component	Unsupported	Comments
VMware Site Recovery Manager ViPR SRA RecoverPoint SRA vRO plugin for Site Recovery Manager		ViPR SRA for replication of Tenant Pods RecoverPoint SRA for replication of Automation Pod
2-site Configuration	> 2 sites MetroPoint	The DR solution is supported by EMC RecoverPoint only and does not support any mixture of EMC VPLEX and EMC RecoverPoint

Upgrades

The following software upgrade paths are supported for EHC v3.5.0:

- Federation EHC v3.1 to EHC v3.5.0

Note: Pre v3.5 EHC deployments must be upgraded to EHC v3.1 before upgrading to EHC v3.5

Resolved Issues

The following issues have been resolved in the EHC v3.5.0 release:

- Foundation – Stack overflow exception and JSON marshaling errors for ASD packaging
- STaaS – 'AddVMtoDRSGroup' workflow fails to add VM to DRS Group when run multiple times.
- BaaS – When creating the virtual machines from blueprints the workflow logic should select the right service level folder to insert the virtual machine when it is created
- BaaS – Reposition VM Workflow will fail on action "convertVMFolderNametoVMFolderObject" if the datacenter names have a similar name.
- BaaS - On-demand backup gets Avamar default retention instead of assigned data protection policy retention.
- BaaS - MCCLI commands are run continuously on the Avamar server during on-demand restore / backup and final backup. This can create a performance problem if many on-demand backup or restore workflows are running simultaneously.
- BaaS - When the workflow "RepositionVM" is run in CA environment and the "Site Affinity" property is not selected when creating a build profile the workflow fails. The log error message was not descriptive enough to help with analysis and customer remediation.
- BaaS - While restoring a backup (On Demand Restore), it was noticed that the backup list contains local as well as remote backups in CA and DR environments.
- BaaS - "Add Backup Service Level" was failing due to a change in Avamar 7.2 (*Avamar hotfix "hotfix-247126" must be applied to Avamar 7.2 systems, or a build incorporating the hotfix must be used*)
- BaaS – Workflow "Add Avamar Pair" fails due to JSON parsing error in script element "Create Service Levels on New Avamar".
- BaaS - "Deploy Avamar Proxy" workflow was not adding the proxy information to the "AvamarConfigurations" file.
- BaaS - "On Demand Backup" failing because an incorrect retention parameter was getting passed to Avamar.
- BaaS – On Demand Restore failed in CA mode when pairs are toggled.

- BaaS – Toggle Single Avamar Designation Fails in a CA Environment when trying to toggle Avamar's back from secondary to primary.
- BaaS – Duplicate Avamar Grids can be added to the configuration using the catalog item "Add an Avamar Instance or Pair".
- BaaS – During running of catalog item "Prepare for DP failover" the list of clusters contains both "protected" and "unprotected" clusters.
- BaaS - When SRM Mapping fails during Create Service Level WF there was no cleanup of folders.
- DRaaS - Network convergence scripts fail due to special character in vCenter distributed port group name.
- DRaaS - The blueprints and entitlements versions are updated to 3.5
- DRaaS - The DR main will fail if the srm site name matches the vcenter name or fqdn
- DRaaS - Modify the soap request for 'unprotectvm'
- DRaaS - NSX / SRM 5.8 is limited to 19 network mappings – this is fixed in the current EHC 3.1 reference architecture (newer NSX)
- DRaaS - Extend DR vCAC Updater to handle Security Groups
- DRaaS - DR Expired machines 'stick' to the source cluster – Partially Resolved. The existence of 'expired' machines no longer blocks the fail-over process. In DR 3.1.0 they are 'ignored' and the fail-over proceeds. However, this leaves them in a state where the vRA cannot 'manage them' – e.g. change the Lease for example – until fail-back. In addition, SRM will fail the machines over and power them on – even though they are expired.
- DRaaS - DR unprotect fails when NSX security group missing
- DRaaS - DR Initialization Main WF Fails – Have switched to NSX plugin and no longer have REST host to initialize. Provisioning VPLEX DD: ViPR VA and ViPR CG error not prevented.
- DRaaS - DRVMProvision fails with "The object has already been deleted or has not been completely created" – This has been fixed with new DR 3.1 architecture.
- DRaaS - DR workflow never fails – fixed. The overall error handling upgraded and made more robust for this release.
- DRaaS - DR Multi-Machine Request shows Fail even when it runs successfully – The Status Details show success because it actually succeeded – but the machine list is missing from the message.
- DRaaS - SRM-144 ViPR SRA export volume multi-path settings – fixed in SRM SRA 5.0.5.120 or later
- DRaaS - DR Add-on - DRVMProvision failed – fixed
- DRaaS - DR Add-on – DR Post Failover updater blocks on 'missing' machines – The updater now skips over 'missing' machines and no longer blocks or errors. These are machines deleted directly from vSphere instead of going thru vRA.
- DRaaS - DR Add-on - postFailoverUpdaterValidation() logic error blocking DR Remediator – fixed.
- DRaaS - DR Add-on – Local DR ASD WF creating ever expanding list – fixed. The local ASD associations are updated as needed instead of continually re-adding to the end of the list on every initialization.
- DRaaS - DR Add-on – Update DR Catalog items – completed. The DR catalog items are now integrated with overall EHC 3.1 (Foundation) design. Specifically – the DR Cluster Pairing catalog item is renamed to "DR Cluster Onboarding" and integrated with EHC Cluster Onboarding service. The other DR catalog items now appear under the Data Protection Services service instead of appearing as stand-alone services.

- DRaaS - DR Add-on – DR validation WF(s) not throwing error – fixed. The validation WFs were logging an error but not throwing exceptions. This allowed DR Initialization Main to complete successfully – even when the installation reported configuration errors.
- DRaaS - DR Add-on - Recovery Plan length = 0 throwing an error. When all the Recovery Plans are on one Site or the other, an unexpected error was thrown.
- DR Add-on - SRM failover NULLs in vRA blocking Data Collections.
- DRaaS - Network Convergence user/pass removal. The plain text vRO username and password on the SRM Network Convergence script – ArgumentList has now been removed and is now set by a new C:\EHC powershell script "credentials.ps1".
- DRaaS - DR Add-on - DR Post Failover Updater - blocks on 'Finalized' machines. 'Finalized' machines are ignored and the fail-over proceeds.
- DRaaS - DRVMProvision workflow failing. During parallel machine provisions, the workflow was failing with SRM login errors. This is thought to be an SRM login thread-safe issue that only allows 1 login at a time. The DRVMProvision workflow has been enhanced to make up to 10 login attempts on the theory that the random timing will overcome the thread-safe issue and mitigate this issue.
- DRaaS - DRVMUnProvision Failure not calling Retire VM. The DRVMUnprovision WF was throwing an error if it could not (successfully) unprovision a machine, which caused a premature exist from the lifecycle so that the Data Protection RetireVM workflow was not being called. This is now fixed.
- DRaaS - NSX Fail-over Scripts not Triggering VCO Workflow. A space is required between the ' and " at the beginning and end of the powershell –ArgumentList given in the SRM Network Convergence script steps. For Powershell treats '"xx" xx ' as 3 arguments instead of 2. ' "xx" xx ' works as intended – 2 arguments.
- DRaaS - DR Add-on - DR Post Failover Updater - blocks on 'Finalized' machines. In the past the vRA results was always success. vRA now reflects the WF status (success or failure) and show the same error message that is sent in email.

Known Issues

The following issues have been identified in the EHC v3.5.0 release:

- Foundation - Initialization/Main sometimes fails on recreating existing vRA and IAAS hosts. *Workaround – Rerun EHC Main.*
- BaaS – Creating Multiple (Simultaneous) Backup Service Levels on Avamar fails. *Workaround: Let the previous request's operation finalize prior to initiating a subsequent request.*
- BaaS - DR datastores are not being registered on the recovery site proxies during a Disaster Recovery failover. After the SRM Failover completes, the Avamar servers on the Recovery site, must synchronize with the vCenter in order for the proxies to be able to see the datastores which were brought over during the failover process. *Workaround: Avamars must be manually synchronized by using the Avamar client GUI prior to executing the "DR Post Failover Updater". If the Avamars are not synchronized prior to executing the "DR Post Failover Updater", you will need to run the "Associate Datastore to Avamar Proxy" catalog item in vRA on each datastore that has failed over.*
- BaaS - "OnDemandBackup" marked as "success" when it actually failed. *Workaround: Check the Avamar status to determine if there are errors. Monitor reports of backup activity. Email should be sent upon successful completion. If no email is received then investigate logs.*
- BaaS – "RetireVM" workflow fails to take a final backup but still deletes the VM. This is a corner case where the Avamar may be offline and unable to complete a final backup. *Workaround: To insure that a backup is take prior to decommissioning a VM take an On-demand backup before retiring the VM and then retire/destroy the VM. In the*

event of the VM gets deleted without long term backup being performed, contact Avamar Admin to change the last On-demand backup retention to the desired long term retention.

- BaaS – "Associate Datastore to Avamar Proxy" workflow not responding properly to errors while creating a Datastore. *Workaround: Check Avamar to insure correct association after running the workflow.*
- BaaS - When "Deploy Avamar Proxy" workflow is run the directions do not specify to use the full FQDN of the proxy. *Workaround: In the field labeled "Enter The Avamar Proxy Name" the user should enter the FQDN of the proxy and not the short name.*
- DRaaS - DR Post Failover Updater Completes Successfully, but fails to set the StoragePath on the Recovery Site Reservation. When the expected DR Enabled storage does not mount on the fail-over cluster, the DR PostFailover Updater cannot locate the expected storage and throws an error. This situation puts the updater in a state that is not automatically recoverable. *Workaround: This situation can avoided by setting "storageProvider.fixRecoveredDatastoreName" to "true" in the SRM Site -> Manage -> Advanced Settings -> Storage Provider settings. This will remove snap-xxx prefix from the ABR datastore names on failover and avoid the EHC-484 conditions.*
- DRaaS - DR Post Failover Updater Workflow sometimes copies incorrect values for reservations & priority after performing a planned migration. This is because of vRA database corruption but was not reproducible in all cases. *Workaround: This can be solved by manually updating the Storage Reservations with the properties for Priority and Memory.*

Resources

The following are the published documents for the Federation Enterprise Hybrid Cloud v3.5 release:

- *Federation Enterprise Hybrid Cloud 3.5 Reference Architecture*
- *Federation Enterprise Hybrid Cloud 3.5 Concepts and Architecture Solution Guide*
- *Federation Enterprise Hybrid Cloud 3.5 Administration Guide*
- *Federation Enterprise Hybrid Cloud 3.5 Infrastructure and Operations Management Guide*
- *Federation Enterprise Hybrid Cloud 3.5 Security Management Solution Guide*
- *Federation Enterprise Hybrid Cloud 3.5 VMware Integrated OpenStack Guide*
- *Federation Enterprise Hybrid Cloud 3.5 vRealize Code Stream Guide*

Additional Federation Enterprise Hybrid Cloud resources can be found at the following locations:

- Inside EMC @ https://inside.emc.com/community/active/global-solutions/cloud/
- EMC Cloud Sales Playbook @ https://www.emc.com/auth/playbooks/cloud.htm
- EMC Community Network (ECN) @ https://community.emc.com/docs/DOC-26195

Federation Enterprise Hybrid Cloud Software Support Matrix:

- EMC Elab ESSM @ https://elabnavigator.emc.com