



Best Practices for Deployment of your Zerto Solution with VMware-as-a-Service

Rev01

Aug 2020

ZVR-VaaS-8.0 U3

© 2020 Zerto All rights reserved.

Information in this document is confidential and subject to change without notice and does not represent a commitment on the part of Zerto Ltd. Zerto Ltd. does not assume responsibility for any printing errors that may appear in this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the prior written permission of Zerto Ltd. All other marks and names mentioned herein may be trademarks of their respective companies.

The scripts are provided by example only and are not supported under any Zerto support program or service. All examples and scripts are provided "as-is" without warranty of any kind. The author and Zerto further disclaim all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose.

In no event shall Zerto, its authors, or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the sample scripts or documentation, even if the author or Zerto has been advised of the possibility of such damages. The entire risk arising out of the use or performance of the sample scripts and documentation remains with you.

ZVR-VaaS-8.0 U3

Best Practices for Deployment of your Zerto Solution with VMware-as-a-Service Provider

This document covers best practices for using the Zerto IT Resilience Platform with VMware-as-a-Service Providers.

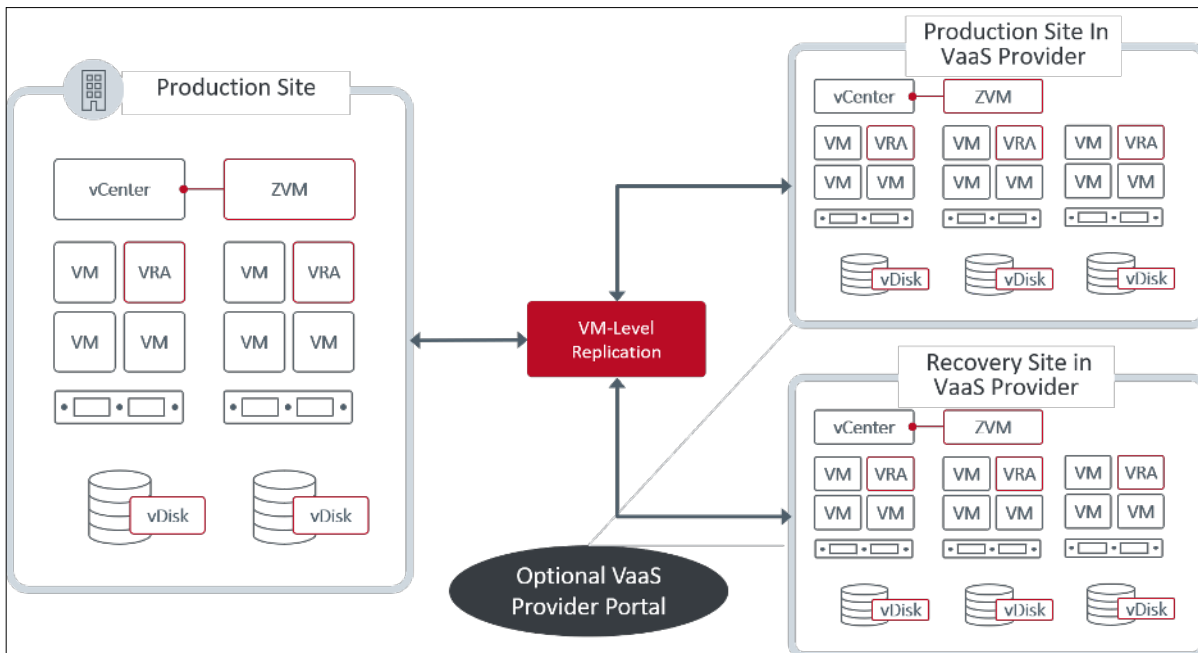
A VMware-as-a-Service (VaaS) Provider offers hardware for compute, storage and networking running VMware Cloud Provider Stack <https://docs.vmware.com/en/VMware-Cloud-Provider-Stack/index.html>. The VMware Cloud Provider Stack consists of vSphere, vSAN and NSX-T.

The VaaS Provider offers cloud style provisioning of the servers and VMware Cloud Provider Stack as a monthly service to their end customers.

The servers and VMware Cloud Provider Stack are delivered as a dedicated, private cloud to each end customer.

The VaaS Provider manages the servers and VMware Cloud Provider Stack across multiple regional data centers for all their customers.

The VaaS Provider's environment is built for scaling to 1000s of customers with each customer having a dedicated private cloud consisting of a vCenter with multiple ESXi hosts.



When you deploy the Zerto IT Resilience Platform in the VaaS environment, your deployment cannot interfere with the operation of the VMware Cloud Provider Stack at scale.

This means you have less control over the vCenter and ESXi hosts at the VaaS provider while significantly reducing your operational costs for each private cloud from the VaaS Provider.

As a customer of the VaaS Provider and Zerto, you can use this document for best practices in using your Zerto Solution in this environment.

Before you begin:

- Please review the [Interoperability Matrix for All Zerto Software Versions](#) for Zerto's compatibility with each VaaS Provider.
- Please ensure the account you are using to connect Zerto Solution with vCenter has all appropriate privileges to deploy Zerto. If the VaaS provider offers the ability to elevate the privileges of the vCenter service account that Zerto uses, then follow the VaaS provider's process to elevate the privileges.
- Prior to installing Zerto, your environment must meet the VaaS Provider's prerequisites.
- You must provide your own DNS and DHCP. Consult the VaaS Provider's documentation for information on configuring DNS and DHCP.
- After installing the Zerto Virtual Manager, the built-in administrator group is entitled to log in and use Zerto. Administrators can allow additional vCenter roles to access Zerto via the installed Zerto permissions accessible in vCenter Roles.

Details on this are available in [Zerto Virtual Manager Administration Guide VMware vSphere Environment](#) > Zerto and VMware Features > Zerto Permissions in vCenter Server.

- Internet access is needed to connect to Zerto CallHome Server, and Zerto Analytics.

Following are links to the key items covered in this document:

- [Connecting to Zerto CallHome Server and Zerto Analytics on page 5](#)
- [Maintenance Mode operation in VMware-as-a-Service on page 6](#)
- [Best Practice for Node additions on page 7](#)
- [Best Practice for Node deletions on page 8](#)
- [Installing your Zerto solution on page 9](#)
- [Upgrading your Zerto solution on page 10](#)


Connecting to Zerto CallHome Server and Zerto Analytics

Zerto recommends enabling Zerto CallHome to monitor the sites deployed in the VaaS Provider. This allows Zerto to contact you about any VaaS Provider events such as vSphere upgrade or new features from the VaaS Provider that affect the Zerto sites.

In the Zerto software > About window, you can do the following:

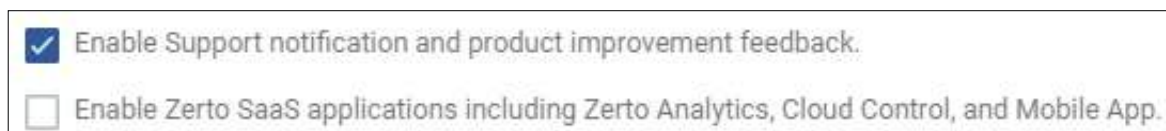
- View the Zerto version being run.
- Enable the **Zerto CALLHOME feature**. The Zerto CALLHOME feature enables support notification and analytics for the following purposes:
 - To improve Zerto.
 - To send notifications to you when a new Zerto version is available, or when new hypervisor versions are supported by Zerto.
- Enable Zerto to send data to the Zerto SaaS platform for monitoring purposes, using the Zerto Analytics and Zerto Mobile App platforms.

> To perform these actions, do the following:

1. In the Zerto User Interface, in the top right of the header, click , and then click **About**.

The version and build of Zerto installed in the site are displayed.

2. To enable the Zerto CALLHOME feature, make sure the following is selected: **Enable Support notification and product improvement feedback** (selected by default).



3. If you want Zerto to send information to our Online Services and Zerto Mobile App, and enable remote upgrade, select **Enable Zerto SaaS applications including Zerto Analytics, Cloud Control and Mobile App**.

This allows licensed Zerto Virtual Manager users to enable data being sent from the Zerto Virtual Manager to the Zerto SaaS platform, thereby enabling site monitoring using the Zerto Analytics and Zerto Mobile App platforms.

Maintenance Mode operation in VMware-as-a-Service

Maintenance Mode on an ESXi host can be used by the VaaS Provider for host failure procedures, maintenance operations, and during software upgrades.

Customers don't enter/exit Maintenance Mode in VaaS Provider environment as the life cycle management of the Software Defined Data Center (SDDC) is handled by the VaaS provider. If this is the case, then the VaaS Provider needs to coordinate host Maintenance Mode with Zerto users. This section covers the best practices for coordinating Zerto recovery site operations with the VaaS Provider.

Short duration Maintenance Mode initiated by the VaaS Provider for routine maintenance operations does not disrupt protection of your VMs. If the VaaS Provider needs Maintenance Mode for over a few hours, then you can take manual steps to prevent a disruption in protection.

The following sections recommend the best practices to support VaaS Provider initiated Maintenance Mode while protecting your VMs.

> **Best practice for entering Maintenance Mode:**

- If this host's VRA is receiving replication, you must use the Zerto Evacuate Host action to move any replication data to another VRA in the host cluster (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Evacuate Host).

> **Best practice for exiting Maintenance Mode:**

- Repopulate the VRA for this host so that some of the replication load is moved to this hosts' VRA (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Populate Host).

Best Practice for Node additions

When you add a node to a cluster in the VaaS environment, you need to install a VRA on the node to enable Zerto protection.

The best practices for handling node additions have slight variations depending on the location of your Zerto solution in VaaS.

The following covers each use case:

[Best Practice: Adding a node to a cluster when VaaS is the Recovery site on page 7](#)

[Best Practice: Adding a node to a cluster when VaaS is the Production site on page 7](#)

Best Practice: Adding a node to a cluster when VaaS is the Recovery site

When adding a node to a cluster, execute these steps on the node that is newly added to the cluster.

> Adding a node to a cluster when VaaS is the Recovery site:

1. Install the VRA on the new host (ZVM UI > Setup > VRAs tab > New VRA).
2. Use the repopulate VRA command to populate the replica Volumes and Journals to the new host (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Populate Host).

Best Practice: Adding a node to a cluster when VaaS is the Production site

When adding a host to a cluster, execute these steps to enable VM protection on the newly added hosts.

Note: It is possible for VMs with Zerto protection to shift to the newly added node with automated DRS. If this happens before the VRA is installed, then there might be a gap in protection for those VMs.

> Adding a node to a cluster when VaaS is the Production site:

- Install the VRA on the new host (ZVM UI > Setup > VRAs tab > New VRA).

Best Practice for Node deletions

Before deleting a node from the VaaS environment, you need to discontinue Zerto protection of any VMs using that node.

The best practices for handling node deletions have slight variations depending on the location of your Zerto solution in VaaS.

The following covers each use case:

[Best Practice: Deleting a node in a cluster when VaaS is the Recovery site on page 8](#)

[Best Practice: Deleting a node in a cluster when VaaS is the Production site on page 8](#)

Best Practice: Deleting a node in a cluster when VaaS is the Recovery site

When you want to remove a node from a cluster, before deleting the host execute these steps .

> Deleting a node in a cluster when VaaS is the Recovery site:

1. Use the evacuate host command to move the protected replica disks to another VRA (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Evacuate Host).
2. Uninstall the VRA from the affected node (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Uninstall).
3. Using the VaaS portal, remove the host from the cluster.

Best Practice: Deleting a node in a cluster when VaaS is the Production site

When you remove a node from a cluster, execute these steps.

> Deleting a node in cluster when VaaS is the Production site:

1. Migrate VMs from this node to another node using the vCenter in the VaaS environment..
2. When the node does not contain any other VMs except the VRA VM, uninstall the VRA (ZVM UI > Setup > VRAs tab > select a VRA > Actions > Uninstall).
3. Remove the node from the cluster with the VaaS portal.

Installing your Zerto solution

To install your Zerto solution, follow the guidelines, considerations and instructions as described in the [Zerto installation guide](#).

When installing Zerto Virtual Replication Appliances (VRA) on your host nodes, the installation is deployed from how the hosts are presented in vCenter. In VaaS, hosts are available via DNS however this name resolution is not available to new VMs in VaaS. Zerto recommends configuring your organization's infrastructure services prior to installing Zerto, for example by forwarding your DNS server to the VaaS DNS server so that name resolution is successful to the hosts from the ZVM.

Note: VMware-as-a-Service Providers expect to deploy recent versions of vSphere.

- As a best practice, Zerto deployments on VMware-as-a-Service environments need to be promptly upgraded to the latest version of Zerto to be compliant to the vSphere version deployed by the VMware-as-a-Service Provider.

Upgrading your Zerto solution

To upgrade your Zerto solution, follow the guidelines, considerations and instructions as described in the [Zerto upgrade guide](#).

Note: VMware-as-a-Service Providers expect to deploy recent versions of vSphere.

- As a best practice, Zerto deployments on VMware-as-a-Service environments need to be promptly upgraded to the latest version of Zerto to be compliant to the vSphere version deployed by the VMware-as-a-Service Provider.

Zerto enhances the Zerto IT Resilience Platform by converging disaster recovery and backup to deliver continuous availability within a simple, scalable platform. Zerto delivers enhanced analytics, platform improvements and cloud performance upgrades required in the future of IT resilience.

Learn more at [Zerto.com](https://zerto.com).

For assistance using Zerto's Solution, contact: [@Zerto Support](https://twitter.com/ZertoSupport).

© 2020 Zerto Ltd. All rights reserved.