Payment Card Industry Data Security Standard (PCI DSS) Compliance

Rev01 U2
Dec 2019
ZVR-PCI-7.5
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-PCI-7.5
Zerto and Payment Card Industry Data Security Standard (PCI DSS)

Review the following:
Executive Summary on page 3
PCI DSS Basics and Zerto on page 3
Then continue with Deployment Considerations for PCI DSS Compliance on page 5.

Executive Summary

Organizations looking to virtualize their mission-critical applications have a number of considerations to take into account:

- How virtualization of these mission-critical applications will impact their security and compliance with the Payment Card Industry Data Security Standard (PCI DSS).
- How to ensure that their business continuity (BC) and disaster recovery (DR) plans are implemented within the virtual environment.

Zerto provides a BC/DR solution in a virtual environment, enabling the replication of mission-critical applications and data as quickly as possible and with minimal data loss. This document describes the considerations required when deploying Zerto for PCI DSS compliance.

This document assumes that readers are familiar with the basics of virtualization and Zerto. Specifically, this paper focuses on solutions and configuration settings that address PCI requirements and will cover Zerto components products such as Zerto Virtual Managers, Virtual Replication Appliances, etc.

PCI DSS Basics and Zerto

The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. The keystone is the PCI Data Security Standard (PCI DSS), which provides guidelines for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

The Payment Card Industry Data Security Standard (PCI DSS) is intended to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. The PCI DSS with Zerto can be summarized by the following:

**Network Security:** Transactions must be conducted in a secure network. This requirement involves not only application network security but also replication network security. Replication must take place within secure networks within well authenticated sites.

**Password Security and Policy:** Authentication credentials such as usernames and passwords must not be the defaults supplied by Zerto and should be changed frequently. All cardholder data, whether production or DR data, must be protected and encrypted at rest and when replicating over the wire. Zerto does not encrypt data so adequate network transport layer encryption must be deployed. Networks must
be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-to-date.

**End-point and Server Security:** Systems should use frequently updated anti-virus software, anti-spyware programs, and other anti-malware solutions. All applications should safeguard against the possibility that cardholder data could be stolen or altered. Patches offered by software and operating system vendors should be regularly installed to ensure the highest possible level of vulnerability management.

**Access Controls:** Access to information and operations should be restricted and controlled whether in production or in DR. While performing DR tests, the same control measures must also be implemented. Every person who uses a computer in the system must be assigned a unique and confidential identification name or number. Cardholder data should be protected physically as well as electronically.

**Security Policy:** A formal data security policy must be defined, maintained, and followed at all times and by all participating entities.
Deployment Considerations for PCI DSS Compliance

Virtual environments can be PCI compliant and are being deployed throughout the payment card industry in a variety of ways. The PCI DSS applies to all organizations that store, process, or transmit cardholder data, regardless of volume. This includes merchants, service providers, payment gateways, data centers, and outsourced service providers, such as the disaster recovery capabilities provided by Zerto.

This chapter describes recommendations to make Zerto deployment PCI DSS compliant within an already compliant virtual environment. It contains the following sections:

- Zerto in Virtualized Environments on page 6
- Questions to Ask to Ensure Compliance With Zerto on page 9
- Managing Access Control on page 10
- Segmenting the CDE on page 11
- Change Control on page 13
- Logging and Monitoring on page 13
- Managing Zerto at Rest and In Transit on page 13
- Conclusion on page 13
Zerto in Virtualized Environments

The following basic environments are the most common implementation of virtualization:

**Local PCI Control Mode:** All systems in the Cardholder Data (CDE) Environment are deployed as virtual machines on dedicated hardware, which is segmented from non-CDE systems, typically through the use of a hardware-based firewall.

**Cloud Multi-tenancy Mode:** Systems in the CDE are outsourced to a cloud provider, whereby multiple tenants reside on the same virtual platforms.

This section describes how to implement a Zerto solution within each of the following architectures:

- Local PCI Control Mode on page 6
- Cloud Multi-tenancy Mode on page 7

**Local PCI Control Mode**

All the virtual machines (VMs) in the CDE are being deployed on a dedicated set of hardware segmented from non-CDE systems. Ensure that the following Zerto components are included on this dedicated hardware and that the relevant PCI controls are implemented:

**Zerto Virtual Manager (ZVM):** The ZVM is a Windows service that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM must be deployed on a VM running on the dedicated hardware. Access to the ZVM requires access to the Windows machine running this service. This access relies on the authentication, authorization, and security mechanisms provided by Microsoft. All communication between Zerto Virtual Managers and hypervisor management tools, such as VMware vCenter Server or Microsoft SCVMM, is secure, either via HTTPS or SSH.

**Zerto Virtual Replication Appliances (VRAs):** VRAs are virtual machines installed on each host with virtual machines to be protected or recovered. They manage the replication of data from protected virtual machines to the recovery site. The VRAs are deployed on hosts running on the dedicated hardware and thus comply with the same PCI controls as the hosts. The VRAs are hardened virtual appliances and must be deployed according to Zerto's hardening and security guidelines.

**Virtual Backup Appliance (VBA):** A Windows service that manages File Level Recovery operations within Zerto Virtual Replication.

**Zerto Diagnostics utility:** The Zerto Diagnostics utility can collect logs from Zerto components as well as hosts and hypervisor management tools, such as VMware vCenter Server or Microsoft SCVMM, where either VRAs or ZVMs run. As such the Zerto Diagnostics utility must be compliant with section 10 of the PCI DSS that defines logging requirements. PCI compliance is fulfilled since the Zerto Diagnostics utility does not collect any data that originated from VMs in the CDE. Zerto recommends that access to the logs produced by the utility is safeguarded by storing the logs safely, for example, on the machine hosting the ZVM.

**Zerto APIs and PowerShell cmdlets:** Both Zerto APIs and PowerShell cmdlets are run by the ZVM and therefore have the same level of protection as the ZVM.
VMs protected by Zerto must be recoverable to hosts on the recovery site that are also deployed on dedicated hardware with the relevant PCI controls implemented. All Zerto components (ZVM, VRAs, etc.) on the recovery site must be deployed with the relevant PCI controls implemented.

Cloud Multi-tenancy Mode

Cloud providers can use virtualized environments and can also support IT operations for more than one organization within a virtual environment. The cloud provider must ensure that the requirements of PCI DSS are met for each organization using the cloud provider services. The cloud provider must ensure the security of cardholder data and PCI compliance for the organization data as well as additional cloud provider requirements, outlined in Appendix A-Additional PCI DSS Requirements for Shared Hosting Providers in the Payment Card Industry (CPI) Data Security Standard Requirements and Security Assessment Procedures from the PCI Security Standards Council, if the cloud provider supplies services to more than one organization in a multi-tenancy environment.

In addition to the considerations outlined above in Local PCI Control Mode on page 6, there is an additional requirement to be aware of: that a breach in one organization might lead to breaches in other organizations using the same cloud provider. Thus, cloud providers supporting multi-tenancy environments must meet PCI DSS Requirement 2.4 which states "shared hosting providers must protect each entity's hosted environment and data."

The following PCI control considerations apply to Zerto components within a cloud provider environment, whether the cloud provider is only used as a recovery site or manages both the protected and recovery sites:

**Zerto Virtual Manager (ZVM):** The ZVM is a Windows service that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM is deployed on a VM running on a secure network (VLAN), preferably the same network where the VMs to be protected, and which are PCI compliant, are running. This applies whether an organization is protecting VMs to a cloud provider, or the cloud provider is protecting VMs from one cloud site to another cloud site. Access to the ZVM requires access to the Windows machine running this service. This access relies on the authentication, authorization and security mechanisms provided by Microsoft. All communication between Zerto Virtual Managers and hypervisor management tools, such as VMware vCenter Server or Microsoft SCVMM, is secure, either via HTTPS or SSH.

**Zerto Virtual Replication Appliances (VRAs):** VRAs are virtual machines installed on each host with virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site. The VRAs are deployed on hosts that comply with the relevant PCI controls. The VRAs are hardened virtual appliances and must be deployed according to Zerto’s hardening and security guidelines.

**Virtual Backup Appliance (VBA):** A Windows service that manages File Level Recovery operations within Zerto Virtual Replication.

**Zerto Cloud Connectors (ZCCs):** A ZCC routes traffic between the customer network and the cloud replication network, in a secure manner without requiring the cloud provider to go through complex network and routing setups, ensuring complete separation between the customer network and the cloud provider network. ZCCs are deployed, one per organization, on hosts that comply with the relevant PCI controls. ZCCs are hardened and must be deployed according to Zerto’s hardening and security guidelines.

**Zerto Diagnostics utility:** The Zerto Diagnostics utility collects logs from Zerto components as well as hosts and hypervisor management tools, such as VMware vCenter Server or Microsoft SCVMM, where
VRAs or ZVMs run. The Zerto Diagnostics utility must be compliant with section 10 of the PCI DSS that defines logging requirements. PCI compliance is fulfilled since the Zerto Diagnostics utility does not collect any data that originated from VMs in the CDE. Zerto recommends that access to the logs produced by the utility be safeguarded by storing the logs safely, for example, on the machine hosting the ZVM.

**Zerto APIs and PowerShell cmdlets:** Both Zerto APIs and PowerShell cmdlets are run by the ZVM and therefore have the same level of protection as the ZVM.
Questions to Ask to Ensure Compliance With Zerto

Incorporating Zerto as the BC/DR solution in a virtualized environment increases the complexity of PCI compliance, by the simple fact that another set of components has been added to the environment. Answering the following questions will help clarify the level of compliance.

What Does Zerto Access?
Zerto replicates the CDE systems. The access to Zerto and the replicated copy of the systems must be clearly defined.

How Does Zerto Manage Changes?
Zerto includes comprehensive auditing, both for the whole system and for specific groups of protected VMs. Further, Zerto provides a set of permissions at the administrator level that control what can and cannot be done within Zerto.

What is Zerto Logging?
Section 10 of the PCI DSS has specific logging and monitoring requirements for all systems in the CDE. Zerto provides full audit trails of all operations done within Zerto as well as the operations Zerto performs in the protected and recovery sites.

How is Encrypted Data at Rest and in Transit Managed?
PCI DSS requires data at rest as well as in transit to be encrypted. Zerto leverages encryption throughout the environment to ensure that information cannot be compromised:

- Access to the Zerto User Interface can be via the vSphere Client console, relying on the security access to this console.
- Communication between the ZVM and the hypervisor management tool, such as VMware vCenter Server or Microsoft SCVMM, is encrypted (HTTPS).
- Communication between the ZVM and the hosts is encrypted (HTTPS).

Communication across networks can be encrypted using network encryption software such as VPN and IPsec. Zerto does not natively encrypt the data across the WAN.
Managing Access Control

Limiting access to the host via the Zerto APIs or PowerShell cmdlets from remote systems on the Internet is not specifically prohibited by a PCI requirement. However if an organization must have remote access, then it must implement PCI DSS 8.2 requirements and ensure processes enforce strong forms of authentication such as signed Digital Certificates from a Certificate Authority combined with strong two factor authentication and monitoring.

Both Zerto APIs and PowerShell cmdlets are run by the ZVM and therefore have the same level of protection as the ZVM. Access to the ZVM itself requires access to the Windows machine running this service. This access relies on the authentication, authorization, and security mechanisms provided by Microsoft.

Control Via Zerto Permissions

Zerto provides a set of permissions at the administrator level that control what can and cannot be done within Zerto. These permissions are assigned to the Administrator role when Zerto is installed. You can define additional roles and assign these roles to all these permissions or to a subset of them as necessary. All the permissions are implemented at the root level, and thus apply to every object in the hypervisor management tool, such as VMware vCenter Server or Microsoft SCVMM.
Segmenting the CDE

Segmenting the CDE requires understanding the network architecture and being able to isolate the CDE from other networks. Segmenting the CDE is achieved either by Port Group Isolation (PGI) or VLAN isolation.

Port Group Isolation

Zerto Virtual Manager requires the following ports to be open in the protected and recovery site firewalls:

<table>
<thead>
<tr>
<th>PORT</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>During Virtual Replication Appliance (VRA) installation on VMware ESXi 5.x hosts and higher for communication between the Zerto Virtual Manager (ZVM) and the hosts IPs and for ongoing communication between the ZVM in the cloud site - but not the customer site - and a Zerto Cloud Connector.</td>
</tr>
<tr>
<td>443</td>
<td>During VRA installation on VMware ESX/ESXi hosts for communication between the ZVM and the hosts IPs. Also, for ongoing communication between the ZVM and VMware vCenter Server.</td>
</tr>
<tr>
<td>4005</td>
<td>Log collection between the ZVM and VRAs on the same site.</td>
</tr>
<tr>
<td>4006</td>
<td>TCP communication between the ZVM and VRAs and the VBA on the same site.</td>
</tr>
<tr>
<td>4007</td>
<td>TCP control communication between protecting and recovering VRAs and between a Zerto Cloud Connector and VRAs.</td>
</tr>
<tr>
<td>4008</td>
<td>TCP communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site and between a Zerto Cloud Connector and VRAs.</td>
</tr>
<tr>
<td>4009</td>
<td>TCP communication between the ZVM and site VRAs to handle checkpoints.</td>
</tr>
<tr>
<td>5672</td>
<td>TCP communication between the ZVM and vCloud Director for access to AMQP messaging.</td>
</tr>
<tr>
<td>8100</td>
<td>Communication between the Zerto Virtual Manager and the Microsoft System Center Virtual Machine Manager (SCVMM).</td>
</tr>
<tr>
<td>9080</td>
<td>HTTP communication between the ZVM and Zerto internal APIs, a Zerto Cloud Manager, and cmdlets</td>
</tr>
</tbody>
</table>

1 If the hosts are given names, make sure that the Zerto Virtual Manager can resolve these names.
<table>
<thead>
<tr>
<th>PORT</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>9081</td>
<td>TCP communication between the ZVMs and between a ZVM and a Zerto Cloud Connector.</td>
</tr>
<tr>
<td>9082 and up</td>
<td><strong>A cloud service provider supplies DRaaS</strong>: Two TCP ports for each VRA (for ports 4007 and 4008) accessed via the Zerto Cloud Connector installed by the cloud service provider. There is directionality to these ports. Zerto recommends using a port range starting with port 9082. For example, Customer A network has 3 VRAs and customer B network has 2 VRAs and the cloud service provider network has 4 VRAs, then the following ports must be open in the firewall for each cloud: The cloud service provider’s VRAs need to use 6 ports to reach customer A’s VRAs, while customer A’s VRAs need 8 ports to reach the cloud’s VRAs. The cloud service provider’s VRAs need to use 4 ports to reach customer B’s VRAs, while customer B’s VRAs need 8 ports to reach the cloud’s VRAs.</td>
</tr>
<tr>
<td>9180</td>
<td>Communication between the VBA and VRA.</td>
</tr>
<tr>
<td>9669</td>
<td>HTTPS communication between:</td>
</tr>
<tr>
<td></td>
<td>• Machines running Zerto User Interface and Zerto Virtual Manager.</td>
</tr>
<tr>
<td></td>
<td>• Zerto Virtual Manager and Zerto REST APIs.</td>
</tr>
<tr>
<td></td>
<td>• Hyper-V hosts and the Zerto Virtual Manager.</td>
</tr>
<tr>
<td>9779</td>
<td>HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a ZVM.</td>
</tr>
<tr>
<td>9989</td>
<td>HTTPS communication between a browser and the Zerto Cloud Manager.</td>
</tr>
</tbody>
</table>

These ports must be included in port groups in the segmentation that is implemented.

**VLAN Isolation**

The ports in the above table, described in Port Group Isolation on page 11, can be mapped to specific VLANs.

---

1. The default port set during the Zerto installation. When pairing the ZVM to a Zerto Cloud Connector, this value must not be changed.
2. When the same hypervisor management tool, such as VMware vCenter Server or Microsoft SCVMM is used for protection and recovery, Zerto is installed on one site only and this port is ignored.
Change Control

Zerto provides a comprehensive audit report that shows the trail of tasks performed within Zerto. You can specify how you want to filter the audit trail in a number of ways, including by date, site, group of protected VMs, and event type.

A separate audit report of recent activities is also available for a specific group of protected VMs within the view displaying details about the group of VMs.

Logging and Monitoring

For details refer to the description of the Zerto Diagnostics utility in Local PCI Control Mode on page 6 and to What is Zerto Logging? on page 9.

Managing Zerto at Rest and In Transit

VMware vMotion does not encrypt data as it moves VMs from one location to another. However, vMotion cannot be performed on VRAs.

Conclusion

Organizations can implement Zerto as their BC/DR solution in PCI compliant environments.
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.

For assistance using Zerto’s Solution, contact: @Zerto Support.

© 2019 Zerto Ltd. All rights reserved.