Zadara Cloud Services Security Brief

Revision history:

Ver	Date	Author	Description
12.04	April 2012	Yair	Security considerations in Zadara Cloud 12.04 version
13.07	July 2013	Yair	Adding Remote Mirroring Authentication and Encryption
16.05	May 2016	Yair	- Some updates on Mirroring encryption - B2S3 encryption brief description
16.05 SP-2	January 2017	Oded	Updates for 16.05 SP-2
17.11	January 2018	Oded	Updates for 17.11
18.11	December 2018	Oded	Updates for 18.11
20.12	January 2021	Oded	Updates for 20.12
22.06	October 2022	Oded	Updates for 22.06, adding zCompute

Contents

Introduction 3
Data Classification 3
Physical Security 3
Logical Access Control 4
  Secure Communication 4
  Identity Management 4
Data Privacy 6
  VPSA Architecture 6
  CHAP 6
  Data Deletion 7
Data Encryption 7
  Encryption of Data-at-Rest 7
  Encryption of Data-in-Flight 8
Remote Mirroring 8
  Authentication 8
  Encryption 9
NAS Users Access 10
Backup to Object Storage (B2S3) 10
Object Storage Architecture 10
  VPSA Object Storage Hierarchy 10
  Object Storage Users and Roles 11
  Object Storage Access 11
  Encrypted Containers 11
Zadara Compute Architecture 12
  zCompute Users and Roles 12
  Protecting Virtual Machines 12
Billing info 13
Zadara Operations Access 13
Security Compliance 14

Introduction

Surveys reveal time and again that security and data protection concerns are the top barriers to Cloud adoption.

At Zadara™ we take these concerns seriously and have made security an integral part of our storage offering. We have architected security into our system and software from the ground up.

With multiple layers of security, our customers can enjoy full, end-to-end data privacy and protection, from Zadara's physical storage infrastructure all the way to customers' Cloud Servers.

Data Classification

Generally Speaking, Zadara maintains 3 types of data on its clouds:
1. Customer Data - Customers using Zadara clouds keep their data in volumes/containers they create on Zadara Cloud. Since Zadara has no visibility into the customer data, we treat it all as most sensitive and critical information. Access is restricted to the data owner only. Customer administrator controls users and access rights to the data. It is the customer's responsibility to define the data protection and high availability requirements for this data. Zadara provides the tools to ensure data privacy, availability and protection.
2. Customer Configuration Data – This category is the metadata for the above Customer data, and the system configuration information. Zadara uses this data to maintain and protect the customer data. This data is critical for the system operation but does not contain any sensitive information. Zadara is responsible for protecting it and backing it up.
3. Customer Information – This is the database of Zadara customers that contains details like contact information, email addresses, and billing details. This is highly sensitive data, but not critical. Zadara is responsible for protecting it and backing it up. This information is kept and protected by Salesforce.com, Zendesk.com and Oracle NetSuit.

Physical Security

The Zadara Clouds are physically located in the most secure data centers of the leading Public Cloud Providers. As of the writing of this document, Zadara Storage is hosted at Equinix for and

at Cyxtera and Equinix datacenters. Zadara Federated Edge is also used by a big number of Service Providers and enterprise customers around the globe, where Zadara cloud is hosted at the customer datacenter. These data centers feature, at minimum, the following important physical security attributes:

- Dedicated cages
- Biometric access controls
- 24x7 surveillance
- Redundant power feeds and generators
- Robust fire suppression
- Carefully monitored climate control (to protect the servers that store customer data)

In OPaaS (On Premises) deployments, the customer takes full responsibility for the physical security, physical health and access to the Zadara systems.

Logical Access Control

Secure Communication

- The Zadara Provisioning Portal, Command Center, zCompute and Zadara VPSA® (Storage Array and Object Storage) expose RESTful API calls via the **HTTPS** protocol. This requires 256-bit SSL-encrypted communication and securely identifies the Zadara web server with which the client is communicating.
- The Zadara GUI client also communicates with the Storage or Compute web server RESTful API via HTTPS to ensure the same level of security.
- For the HTTPS communication users can use the Zadara built in certificate or bring their own certificates.

Identity Management

- Each Zadara user creates an account within the Zadara Provisioning Portal. The user's **Password** is *not* stored as plain text in the Provisioning Portal DB. Instead, a cryptographic hash value (using a one-way SHA-1 hash function) is stored for further login authentications.
- Zadara Provisioning Portal supports Dual Factor Authentication using authenticator mobile app.
- When a user creates the first zCompute account or a VPSA , a corresponding tenant is created within the Zadara Storage Cloud Identity Management Server (which is based

on OpenStack Keystone).

- The Provisioning Portal generates a random 128-bit **Tenant Password** for that tenant and provides the password, in encrypted form, to the Identity Management Server.
- Thereafter, the Tenant Password is used by the Provisioning Porta and the storage system for retrieving a **Keystone API Token** and establishing a session-based communication for managing the objects (i.e, VPSAs) belonging to that tenant.
- For accessing the VPSA (via API or GUI), the Cloud Console provides (via email) an initial temporary access code. This code can be used only once. The user is requested to enter a strong **User Password** to replace the temporary access code.
- The Zadara Provisioning Portal Password the storage and compute User Password can be different. This enables support for different permission levels (roles) within an organization.
- Once customers login to the Providing Portal, they can view their existing compute account and VPSA's, create new systems, modify and delete. Customers do not have access to other customer's Systems. Customer access is limited to their provisioned systems and cannot see the rest of Zadara Cloud.
- In the event a user forgets the password, an email will be sent to the user with a new temporary access code. The existing User Password will protect access until the new access code is used.
- A cryptographic hash value (using a one-way SHA-1 hash function) of the User Password is stored in the VPSA database for further login authentication.
- Zadara employs a session-based authentication mechanism as a means to identify a user for every HTTP request to a VPSA. The client initiates a session by logging in with the User Password. Upon successful authentication, a **Secret API Token** is sent back to the client application, for any subsequent REST API communication with the VPSA to identify the authenticated user and validate the session.
- At any time, a user can generate a new Secret API Token, thus invalidating the previous token and any sessions using it.
- VPSA admin can control the user password policy, such as password expiration, password length and history retention.
- Users can change their passwords / reset their API access keys at any time
- VPSA admin can create additional users and set their roles that define the given access rights.
- zCompute account admin (tenant_admin) can create additional users for that account and set their roles that define the given access rights to specific projects within the account.
- All Zadara Web UI supports Dual Factor Authentication using authenticator mobile app. VPSA admin/Tenant adminn can enforce DFA on all members.

Data Privacy

VPSA Architecture

The VPSA architecture provides the basic building blocks for granting complete data privacy for Zadara Users:

- Each VPSA Virtual Controller is granted dedicated compute resources (RAM and CPU vCores) and dedicated networking resources (NIC VFs) to partition IO stack data handling per-tenant.
- Physical drives are the basic storage allocation unit. As a result, only a single VPSA and hence a single tenant has access to any given physical drive.
- Physical drives are exposed as iSCSI LUNs to the VPSA Virtual Controllers via a separate back-end network, which is not accessible from outside the Zadara Storage Cloud.
- IQN-based SCSI **LUN Masking** is used to ensure that physical disk drives are exposed only to the authorized VPSA system.
- Each tenant can look up the physical location (by Storage Node Number) of the drives assigned to that tenant.
- VPSA Block Virtual Volumes are presented as iSCSI/FC LUNs and are 'attached' to selected Cloud Servers. Again, SCSI LUN Masking and FC zoning is used to prevent access to those Virtual Volumes from other Cloud Servers.
- From the networking perspective the newly created VPSA is isolated in the customer's VLAN that is connected to the customer's Virtual Private Cloud (VPC) within the public cloud.

CHAP

- VPSA *requires* the usage of **Challenge-Handshake Authentication Protocol** (CHAP) over iSCSI to authenticate a Cloud Server to a VPSA. CHAP requires that both the Cloud Server and VPSA know a shared **CHAP Secret**. This secret is never sent on the wire.
- Each VPSA maintains its CHAP credentials. When a VPSA is created, it auto-generates a CHAP Username (corresponding to the VPSA name) and a random 12-character CHAP Secret.
- A VPSA User can modify both CHAP Username and CHAP Secret at any time. Existing iSCSI connections will remain valid, but the new credentials will be required for establishing new connections.

- A VPSA user must enter these values at the Cloud Server (iSCSI Initiator) side to be able to establish an iSCSI connection with the VPSA.
- The VPSA uses a 128-bit **Secret Key** to encrypt the CHAP Secret, using the Advanced Encryption Standard (AES), before storing the CHAP Secret on disk. The Secret Key itself is stored in a separate location in the Zadara Storage Cloud. The VPSA retrieves the Secret Key from the Zadara Storage Cloud at runtime, decrypts the CHAP Secret and stores it in **Kernel Space** only. This means that core-dumping the user-mode process of the VPSA will not reveal the decrypted CHAP Secret.
- The VPSA Supports optional **Mutual CHAP** authentication and **CHAP secret per Server**

Data Deletion

Zadara allocates dedicated drives for each customer. This allows drives shredding when the customers removes data or stops the services. When a customer deletes the data, she can use logical shredding (done according to DoD 5220.22-M standard), or buy the used drives from Zadara and physically shred them.

Data Encryption

Zadara Storage supports Encryption of **Data-at-Rest** (DAR) and **Data-in-Flight** (DIF). Because data encryption requires compute overhead, we leave it up to Zadara users to evaluate the trade-off between security and performance. Hence both DAR and DIF encryption are optional features and are disabled by default.

Encryption of Data-at-Rest

- Encryption management of Data-at-Rest is done at the VPSA Virtual Controller and is defined on a Volume-by-Volume basis, i.e. a user can decide that some Volumes are encrypted, while others are not.
- A VPSA generates a unique random 256-bit **Encryption Key** per encrypted Volume, and uses the Advanced Encryption Standard (AES) to encrypt and decrypt the Volume data.
- The Volume Encryption Keys are stored on disk as ciphertext, using AES with a 256-bit **Master Encryption Key**, which is generated from a *user-supplied* **Master Encryption Password**. Instead, the master password can come from a compliant Key Management system over KMIP protocol

  The Master Encryption Password is *not* saved on disk. Only its SHA1 hashsum is

saved on disk, for verification purposes only. Since it is virtually impossible to restore the Master Encryption Password from the SHA1 hashsum, each user is fully responsible to retain and protect the Master Encryption Password. During VPSA operation, the Master Encryption Password itself is held in kernel memory of the VPSA. Core-dumping any User Mode process within the VPSA will not reveal the Master Encryption Key.

- The above method ensures that encrypted Data-at-Rest cannot be accessed without explicitly knowing the user-supplied Master Encryption Password, thus providing full protection to Zadara users who opt for Data-at-Rest encryption.

Encryption of Data-in-Flight

- For advanced security needs, Zadara Storage supports encryption of Data-in-Flight between the User Cloud Server and the VPSA using **Internet Protocol Security** (IPSec).
- Zadara uses **Internet Key Exchange** (IKE) protocol to negotiate the IPSec encryption keys with a user's Cloud Server. The encryption keys used to encrypt the Data-in-Flight are stored in kernel memory only (of both the VPSA and Cloud Servers), and are *never* stored on disk in any form. Periodically, encryption keys are renegotiated by VPSA and Cloud Servers' IKE daemons.
- Users that use SMB file systems on Zadara storage can use "SMB Encrypt" to secure file traffic of Windows servers.
- A user can configure the renegotiation trigger for each Cloud Server. For example, encryption keys can be renegotiated every hour, every 10 Gb of sent/received data, etc.

Remote Mirroring

Remote Mirroring is the VPSA's Disaster Recovery (DR) service.
Volumes are mirrored from a source VPSA to a remote VPSA. Typically, the remote VPSA resides in a different region and the data is synchronized over the network.

Authentication

First step is to establish a trusted communication between the VPSAs. Establishing the trusted communication can be initiated from any VPSA. It is done by exchanging encrypted secrets using a **public-key encryption protocol** (RSA).

Let's call the initiating VPSA-Source and the other VPSA-Dest. The following are the detailed

steps to establish the trust:

- The user initiates the process via the VPSA-Source GUI, by selecting Remote-VPSA->Discover and providing the VPSA-Dest's IP address and User-login Password
- Each VPSA generates public and private keys, and passes the public key to the other VPSA
- VPSA-Source hashes the user password (using a one-way SHA-1 hash function), encrypts it and sends it to VPSA-Dest. VPSA-Dest compares it to its stored user-password SHA-1 to authenticate the VPSA-Source.
- VPSA-Source does not store VPSA-Dest password in any persistent storage. Therefore, VPSA-Source and VPSA-Dest exchange secret keys for future communication and re-authentication.
- Periodically, VPSAs re-authenticate. Each VPSA recreate a set of private and public keys, encrypt and exchange Secret keys.
- Public and private keys are session-based. i.e. re-generated for every new session.

Encryption

VPSA Remote Mirroring is snapshot-based. It creates and deletes snapshots at a given interval and mirrors\ships the modified data between two snapshots to the remote VPSA.

For Volumes which are already encrypted at-rest on the source VPSA (using AES-128\AES-256), the data is mirrored as-is to the destination VPSA. The Volume encryption key is mirrored as well. It is then stored, encrypted, in the destination VPSA, using the user-provided master password (which can be different than the user master password on the source VPSA).

For Volumes which are not encrypted at-rest on the source VPSA, the mirrored data is encrypted using AES-256-CBC before it is shipped to the remote VPSA to ensure that the in-flight data is always encrypted.

Similar to the authentication process, a **public-key encryption protocol** (RSA) is used to exchange random keys for the stream encryption. The following are the steps which occur whenever a new snapshot is mirrored:

- VPSA-Source generates a new public and private key pair, and passes the public key to VPSA-Dest
- VPSA-Dest generates a new cipher key and passes it back to VPSA-Source.

- VPSA-Source uses this key to encrypt the stream of modified data.
- Keys are session-based. i.e. re-generated for every new session.

Note:
Mirroring Traffic between 2 VPSAs which are connected via local FE network (not via Public IPs) is not encrypted.

NAS Users Access

File system access is granted to each user according to the defined permissions.
VPSA supports both local users and Active Directory central user management.

Backup to Object Storage (B2S3)

Data copy to\from S3 or any other equivalent object storage is done using HTTPS protocol, so the data in-flight is encrypted using SSL.

The data which is stored in S3 is encrypted using S3 server side encryption.

If the data is encrypted at-rest on the source VPSA, it is then decrypted before it is sent (over HTTPs) to the Object storage

Object Storage Architecture

The Object Storage architecture provides the basic building blocks for granting complete data privacy for Zadara Users:

VPSA Object Storage Hierarchy

The Object Storage system organizes data in a hierarchy, as follows:

- **Account** (also referred to as Tenant). Represents the top-level of the hierarchy. The account admin owns all resources in that account. Accounts are also used to control users access to objects and containers.

- **Container** (Also referred to as Bucket). Defines a namespace for objects. In addition to containing objects, you can also use the container to control access to objects.

Object Storage Users and Roles

There are 3 types of Roles assigned to VPSA Object Storage (ZIOS) Users:

- The user (registered in Zadara Provisioning Portal) that orders the VPSA Object Storage becomes its Administrator. ZIOS Administrator is a super-user with privileges to create accounts and users of any role. Users with ZIOS Administrator role can perform containers and objects operations across accounts.
- **Account Admin** can create an account (using the Self Account Creation Wizard) and can manage their own accounts. They can perform any user management and containers/objects operations.
- **Member** can do object storage operations according to the permission given by the account administrator, within the limits of that account. These operations include create/delete/list containers and create/delete/list objects.

Object Storage Access

Access to buckets and objects can be done either via OpenStack Swift or AWS S3 interfaces.

- **OpenStack Swift** (V3 Authentication) – Authentication over V3 Auth Endpoint, using username and password
- **AWS S3** – Using Access Key/Secret Key pairs

Encrypted Containers

Data-at-Rest encryption (data on the Disk Drives) is applied by the Object Storage on a per-Container basis. Encrypted and unencrypted Containers can coexist in the same account.

A VPSA Object Storage generates a random 256-bit unique Encryption Key per encrypted Container and uses the Advanced Encryption Standard (AES) to encrypt and decrypt the objects data.

The Encryption Keys are stored on disk as ciphertext, using AES with a 256-bit Master Encryption Key, which is generated from a user-supplied **Master Encryption Password.**

The User (ZIOS Admin) owns the Master Encryption Password. It is *never* stored on any persistent media. Instead, only its SHA3 hash-sum is saved on disk for password validation.

Instead, the master password can come from a compliant Key Management system over KMIP protocol

Zadara Compute Architecture

The zCompute architecture provides the basic building blocks for granting complete data privacy for Zadara Users:

zCompute Users and Roles

Member role allows the user to use the console, policies and APIs for creating, viewing, modifying and deleting virtual resources (e.g. VMs, volumes, etc.) belonging to projects to which the user has been assigned. This is the standard role for most users.

Tenant Admin can use all functions which are granted to a Member, in addition Tenant Admin role also allows the user to use policies and APIs for creating and managing new projects and users within a specific account. The user that is registered on the Zadara Provisioning Portal for Compute services, has the role of Tenant Admin and is responsible to manage the account on behalf of his organization. The Tenant Admin can create additional users with this role.

Cloud Admin/MSP Admin can do everything on the cloud including creation of new accounts and users of these accounts. Cloud Admin role is used by Zadara to manage the cloud resources, settings, etc…

Protecting Virtual Machines

In addition to the standard authentication provided by the VM operating systems (Windows/Linux) the following are provided by the Zadara compute architecture:

- Key pairs are used for ensuring the identity of a user connecting to a VM instance. Key pairs are generated when creating a new virtual machine.
- With zCompute "Security Groups" virtual machines are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing and restrict incoming connections to customer specified IP addresses/ports
- Each customer on zCompute has its own Virtual Private Cloud (VPC) is isolated from other customers at the networking level. Network communications within a VPC are isolated from network communications within other VPCs.

Billing info

Zadara Storage uses cloud services (such as FreshBooks, NetSuite) for billing invoices and Authorize.net as its Payment Gateway. Credit card information is neither collected nor stored by Zadara.

These cloud services serve thousands of businesses and have all the necessary security and compliance features and certifications, including TRUSTe, TrustWave, SOC2 and others.

More information can be found at their sites:
http://www.freshbooks.com
http://www.authorize.net

Zadara Operations Access

Zadara Operations team access the cloud infrastructure for monitoring and maintenance purposes. Access to production clouds and to Compute/Storage Nodes and Virtual Controllers is restricted only to authorized Operations and Support personnel.
In order to gain comfort that people who have access to Zadara's production clouds can be always trusted, Zadara takes the following measures:

- Employees are subject to background checks;
- Employees must respect the company security policy and code-of-conduct;
- Employees perform professional and security trainings

All incoming/outgoing traffic from the Zadara Cloud to the Internet is protected by complex firewall. Access is allowed from Zadara's IP addresses only and requires VPN login using dual-factor authentication with one-time password (OTP). Some Zadara's clouds support Teleport, based on outgoing traffic only into Zadara. Such access is also limited to Zadara's Ips and requires dual factor authentication.
Access to Virtual Controllers also requires dual-factor authentication with OTP. This access is allowed with limited command set with no visibility into the customer's file systems. Zadara personnel access is limited to the cloud and VPSAs metadata (Configuration Data).
Access to Command Center (Cloud management tool) can be controlled by the customer and requires dual-factor authentication with OTP.
Access to VPSA GUI for Zadara cloud administrators is controlled by the customer's VPSA

Admin.
Zadara maintains full auditing track for the cloud and the VPSA's in its Access Log. These logs are kept within the cloud and never expire.

Security Compliance

Zadara storage services are compliant with most of common security standards and regulations.
Zadara goes under annually audits to maintain the following certifications:

- SOC1 Type2 / SOC2 Type2
  SOC 1/2 compliance provides businesses with the confidence and peace of mind that their data is secured and highly available.
- ISO27001 / 27017 / 27018
  ISO27001 is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.
  ISO27017 standard provides guidance on the information security aspects of cloud computing.
  ISO27018 standard provides guidance aimed at ensuring that cloud service providers offer suitable information security controls to protect the privacy of their customers' clients
- HIPAA
  The Health Insurance Portability and Accountability Act (HIPAA) is a standard for sensitive patient data protection.
- GDPR / ISO27701
  The General Data Protection Regulation (GDPR) is the European privacy law that protects European Union (EU) citizens' right to privacy.

More information about Zadara certification can be found at our site:
https://www.zadara.com/platform_compliance.php

More information about Zadara Cloud Services can be found at our site:
http://www.zadara.com