VERITAS
APTARE IT Analytics™

APTARE IT Analytics Architecture and Security

APTARE IT Analytics can be deployed securely in a variety of operational environments, including a private LAN, virtual private network (VPN), corporate Intranet, multi-tenant, and even the public Internet. The security features for APTARE IT Analytics communications (for example, between Web Client and Host) can be customized for your operational environment. The system can be configured to provide an end-to-end security context between the user's browser and the Portal Server which provides security, privacy, user authentication and no repudiation. Messages between the Web Client and Portal Server are secured when the server is configured to use HTTPS/SSL, which provides for authentication and encryption of traffic. SSL communication between the Portal and the Data Collectors is fully supported.

Architecture

APTARE IT Analytics has a hub and spoke architecture with two main components:

- **Portal**: A centralized location (the underlying database is embedded and includes licenses, etc. for Oracle 12c).
- **Data Collectors**: For Backup Manager, the Data Collector interfaces with the underlying Backup Vendor Products (for example, Veritas NetBackup, Veritas Backup Exec, IBM Spectrum Protect (TSM), EMC Avamar, EMC NetWorker, HP Data Protector, Veeam Backup & Replication, Oracle Recovery Manager (RMAN or Commvault Simpana) using the standard published interfaces to that backup product. Likewise, for Capacity Manager, the Data Collector uses storage array mechanisms specific to each vendor's storage system (for example, HDS, IBM, EMC Symmetrix, EMC CLARiiON, Pure Storage, and NetApp). In addition, Host Resources data is acquired. The data is parsed and packaged into Java objects; serialized into an HTTP or HTTPS data stream, compressed and sent over network via port 80 (HTTP) or port 443 (HTTPS) and inserted into the underlying Portal database.

Portal Server Architecture

APTARE IT Analytics uses a three-tiered architecture on the Portal Server(s):

- **Web Server**: Embeds Apache and applies the latest set of Apache security patches to eliminate all known security vulnerabilities.
- **Apache Tomcat**: Uses Tomcat as the Java Servlet engine. The system communicates between Apache and Tomcat using standard Apache connectors.
- **Oracle 12c database**: Communicates with the Oracle 12c database using JDBC.

The Portal deploys Apache Tomcat on a single web server and the Oracle 12c database on its own dedicated system.

Web Browser Security

All Portal features, including Capacity Manager, are accessible through a standard web browser that supports HTML 5. This native browser integration eliminates the need for Java applets, ActiveX controls, or any other piece of client-installed software. This browser-based user interface allows corporations to leverage standards-based security, such as SSL, to protect and encrypt traffic between the Portal and the client browser.

User Authentication

The Portal supports the following user authentication methods:

- **Local LDAP**. The Portal bundles OpenLDAP to manage user login authentication. For information about OpenLDAP, go to http://www.openldap.org.
- **Enterprise LDAP**. Refers to any standard LDAP service, including Microsoft Active Directory. For information about Active Directory, go to Microsoft's Active Directory portal.

By default, the Portal uses OpenLDAP for user authentication.

General Data Collector Security

The APTARE IT Analytics Data Collector is a centralized and remotely managed data collection mechanism. This Java application is responsible for interfacing with backup servers and storage arrays to gather information related to storage backup/recovery and capacity management.

The Data Collector continuously collects data and sends this data, using an http or https connection, to the Data Receiver. This Data Receiver runs on the Portal Server and stores the data it receives in the Reporting Database.

The Data Collector obtains all of its monitoring rules from a Data Collector Configuration file. Passwords configured for policies in the Data Collector are encrypted prior to insertion into the database. They are decrypted in local Data Collector memory immediately prior to use. This configuration file resides in the Reporting Database in XML format. When the Data Collector first starts, it downloads this file from the Reporting Database. The Data Collector uses this file to determine the list of backup servers, hosts, or storage arrays that are to be monitored and included in its data collection process.

Capacity Manager provides end-to-end storage capacity reporting from the hosts to the storage arrays. The Capacity Manager Data Collector is a software component that is responsible for interfacing with one or more storage arrays for information related to the capacity management environment. In most cases, the Capacity Manager Data Collector module can reside on any server within your network that is Java 1.8 compatible and, where applicable, has a working copy of the specific storage array command line utilities already installed. The exception is EMC Symmetrix, which requires the Capacity Manager Data Collector to reside on the server that manages the arrays.

Backup Manager provides comprehensive reporting of major backup software environments. The Backup Manager Data Collector interfaces with each of the supported backup and recovery software systems to extract meta-data about the underlying backup and recovery environment such as backup job details and tape inventory information. The Backup Manager Data Collector can run on any standalone server, the Portal Server or any backup server for all backup solutions other than Veritas NetBackup.

Virtualization Manager provides views for monitoring storage utilization in a virtualized environment, enabling efficient capacity allocation and forecasting. Storage used by virtual machines is mapped to the actual storage array down to the file system level. Reports offer insight into storage that potentially could be reclaimed. In addition, performance statistics aid in identifying potential contention issues that impact overall performance. Performance can be monitored for Virtual Machines, Datastores, and Physical Disks. A Data Collector can collect data from Virtual Center (vCenter) or from specific ESX servers that are not managed by vCenter.

Managed Services Data Collection

The entire APTARE IT Analytics architecture, consisting of multiple Data Collectors pushing relevant information about the backup and storage environments to a centralized Portal Server, was designed for deployment within a globally managed services environment. In a managed services environment, many customers can be supported through deployment of specific Data Collectors in the customer's data center that interface securely over the Internet with the managed service provider's Portal Server. Each customer in this managed services environment is isolated to their specific content when their information in the Portal Server is viewed through a web browser.

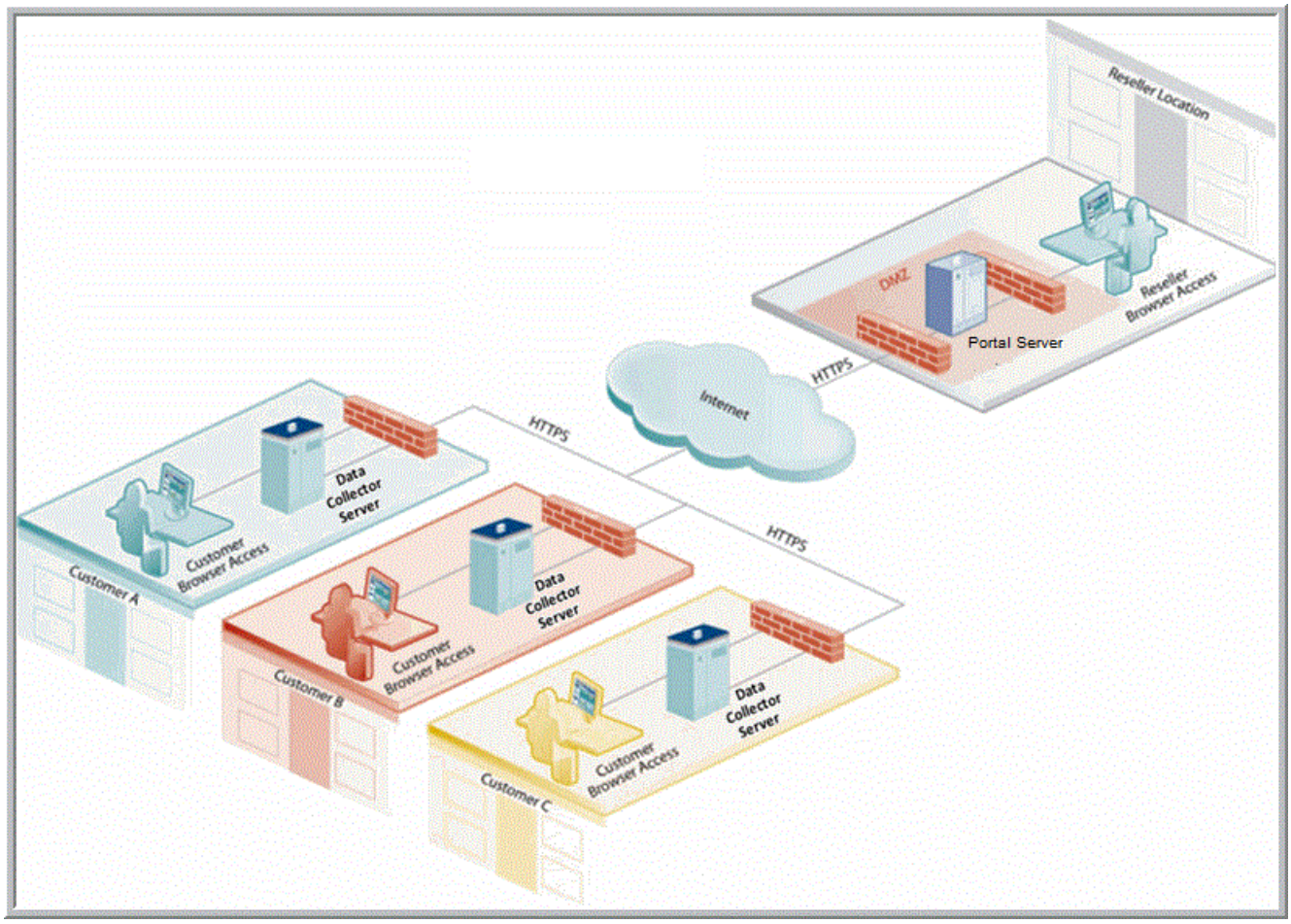

Figure 1.1 Data Collector Architecture in a Managed Services Environment

Network Security

The communications mechanism used by the Data Collector to interface with the Data Receiver is through Hypertext Transfer Protocol (HTTP) over the Internet or an Intranet. The Data Collector attempts to establish a “session” with the Data Receiver using its pre-configured URL (IP address), login identifier, and passcode. The Data Receiver validates these credentials and, if valid, goes into “session” with the Data Collector. The Data Receiver drops the connection, should the validation of the credentials fails. The Data Collector uses the HTTP post request method to submit data to be processed by the Data Receiver. The default transport mechanism between the Data Collector and the Data Receiver is done over secure HTTP (HTTPS) through the standard IP Secure Socket Layer (SSL) on port 443. However, the Data Collector can use any unused port and transport data to the Data Receiver via http or https. This allows users to adopt various secure approaches that best fit their network environment such as private LANs, virtual private networks (VPNs), corporate Intranets, and even secure public Internet access.