EMC CLOUD PORTAL & SERVICES
OVERVIEW & SECURITY MECHANISMS

ABSTRACT

This white paper describes concepts and security mechanisms provided by EMC Cloud Portal & Services (CPS), an EMC-provided SaaS management platform that extends EMC products to the cloud. The white paper further describes how the CPS approach to security supports and enhances CPS managed products such as CloudBoost, EMC's technology for enabling data protection to and within public or private clouds, and Virtustream Storage Cloud (VSC), EMC's hyper-scale object storage platform.

April 2016
To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit www.emc.com, or explore and compare products in the EMC Store.

Copyright © 2016 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

Part Number H15064
# TABLE OF CONTENTS

WHAT IS EMC CLOUD PORTAL & SERVICES ................................................................. 4
OUR APPROACH ............................................................................................................... 4
BENEFITS OF CPS ........................................................................................................... 4
   AVAILABILITY .................................................................................................................. 4
   SCALE ............................................................................................................................... 4
   SECURITY .......................................................................................................................... 4
   PROTECTION ..................................................................................................................... 4
   UPGRADES ....................................................................................................................... 4
PRODUCTS USING CPS .................................................................................................... 5
   EMC CLOUDBOOST ......................................................................................................... 5
   EMC VIRTUSTREAM STORAGE CLOUD ......................................................................... 5
SECURITY AND CONNECTIVITY ......................................................................................... 5
   SERVICE ISOLATION ......................................................................................................... 5
   CONNECTIVITY TO CPS .................................................................................................. 5
   CONNECTIVITY VIA PROXY ............................................................................................ 6
   MANAGEMENT INTERFACE ........................................................................................... 6
   MANAGEMENT PROXY .................................................................................................... 7
PRODUCT SPECIFIC INFORMATION ................................................................................. 8
   CLOUDBOOST ................................................................................................................... 8
   CLOUDBOOST SECURITY ................................................................................................. 8
   CLOUDBOOST CONNECTIVITY ....................................................................................... 9
   WHAT CPS STORES FOR CLOUDBOOST ................................................................. 9
   VIRTUSTREAM STORAGE CLOUD ............................................................................... 9
   PROVISIONING VIRTUSTREAM STORAGE CLOUD .................................................. 10
   VIRTUSTREAM SECURITY .......................................................................................... 10
   WHAT CPS STORES FOR VIRTUSTREAM ............................................................... 10
WHAT IS EMC CLOUD PORTAL & SERVICES

EMC Cloud Portal & Services (CPS) is an EMC provided SaaS management platform that extends EMC products and services to the cloud.

As a management platform, CPS provides both a single place to view and manage EMC products via a Web-based graphical user interface as well as HTTPRest API access to some features for automation purposes.

OUR APPROACH

CPS is a direct result of instituting an overall Cloud First policy to harness the benefits of cloud computing and storage.

The design and development of CPS has been focused on enabling management, automation, mobility and scale of multiple products while ensuring highest levels of security.

BENEFITS OF CPS

CPS delivers a single interface to access, provision, configure, monitor and control your cloud enabled EMC products and services.

AVAILABILITY

Designed as a cloud resident SaaS application without a single point of failure, CPS provides the highest levels of availability and resiliency while also benefiting from continuous monitoring and alerting systems.

CPS removes the need for separate management servers reducing the complexity of your deployments and facilitating ease of management.

CPS is currently managed and operated entirely within the US.

SCALE

As an EMC hosted, cloud resident application, CPS negates the need for a locally deployed management server infrastructure to service your EMC portfolio, regardless of size. CPS delivers unlimited scale and multi-node management across multiple locations.

SECURITY

CPS is continuously monitored and updated with the latest improvements and security fixes without the need for customer interaction.

The CPS development team follows the best practices for secure software development laid down by the EMC Product Security Office. Formal design reviews, risk assessments, thread modeling and static code analysis and testing are all inherent to our design and release workflow.

PROTECTION

CPS provides protection and disaster recovery services for all managed products thus removing the need for separate protection of EMC products.

UPGRADES

CPS provides upgrade services for all managed products. Upgrades can be scheduled at will and performed in a fully automatic manner without manual intervention.
PRODUCTS USING CPS

EMC cloud Portal & Services are currently used for management of the following products:

**EMC CLOUDBOOST**
CPS provides exclusive provisioning, monitoring, management and reporting services for CloudBoost 2.0 (and later) appliances.

**EMC VIRTUSTREAM STORAGE CLOUD**
CPS provides exclusive provisioning, monitoring, management and reporting services for Virtustream Storage Cloud (VSC).

*Note: Cloud Portal & Services will expand to support additional products in the future.*

SECURITY AND CONNECTIVITY

SERVICE ISOLATION
All services within CPS are accessed via a top-level domain URL - https://dpccloud.com. Access includes additional subdomains depending on the service type. For example, access to the Graphical UI is via https://console.dpccloud.com.

From there, the front-end security gateway authenticates, filters, and redirects requests to the appropriate back-end services running within CPS. Individual services are never accessed directly.

Access to each CPS service requires the correct individual authentication and authorization without exceptions.

CONNECTIVITY TO CPS
All external connectivity to CPS is via standard, outgoing-only, HTTP protocol encrypted with Secure Sockets Layer (HTTPS on TCP/IP port 443) using a 2048 bit RSA certificate.

It is important to note:

- Clear text communication is not allowed or enabled under any circumstances.
- CPS does not perform any interaction with 3rd party sites.
- CPS does not initiate any connections towards managed customer environments.

CLOUD PORTAL & SERVICES CONNECTION WORKFLOW DIAGRAM
CONNECTIVITY VIA PROXY
In cases where an environment does not allow for connectivity between a managed EMC product (e.g., CloudBoost) and CPS, connections may be established via a customer provided private HTTP proxy service.

If connectivity between a managed EMC product and CPS is disrupted, CPS will provide alerts while the actual products will remain functional. Connectivity is required to perform provisioning tasks and configuration changes. Connectivity is not required for standard operations.

MANAGEMENT INTERFACE
CPS connectivity is typically required from two places:

- A managed appliance (e.g., CloudBoost)
- A management workstation (e.g., a user’s desktop)
MANAGEMENT PROXY
From CloudBoost 2.1, the CloudBoost appliance includes a built-in HTTP proxy.

This new feature enables the CloudBoost appliance itself to be used as a connection point for environments where management workstations do not have direct access to CPS.
PRODUCT SPECIFIC INFORMATION

CLOUDBOOST

Cloud Portal & Services became the primary platform for CloudBoost management from CloudBoost 2.0.

The move to CPS enabled customers to easily control multi-node CloudBoost deployments. New appliances can be deployed in minutes with reduced configuration entry. Connecting to an object store becomes as trivial as selecting a pre-configured Cloud Profile.

Compatible appliance upgrades are identified and presented to the user for one-click-installation through the CPS UI ensuring your environment is always up-to-date with security fixes and functional enhancements.

Whilst CPS is not required for the normal operations of a CloudBoost appliance, CPS is required for provisioning, configuring, monitoring and alerting. Should connectivity between an appliance and CPS ever be disrupted, CloudBoost will alert users to the issue while continuing to functioning as usual.

In the event of a CloudBoost appliance failure, CPS enables rapid DR to a standby appliance thanks to the shared, account-level access to CloudBoost appliance configuration details. Comment

CLOUDBOOST SECURITY

CloudBoost supports a broad range of public and private object stores. Regardless of type, all data written to object storage is de-duplicated, compressed and encrypted within the appliance prior to transport.

A SHA-2 hash is generated per variable length chunk, and this hash is used as a key for AES-256 encryption. As each data chunk is encrypted using a self-generated key there is no master encryption key, negating the need to store one in the cloud. This technology has no known vulnerabilities, either in exploitable or theoretical form.
In addition to strong data encryption performed within the appliance and before transport, all over-the-wire transports are encrypted using secure HTTP (HTTPS). This applies to both data and control messages without exceptions and cannot be disabled.

**CLOUDBOOST CONNECTIVITY**

CloudBoost appliances make periodic requests to CPS on a well-known URL (https://dpccloud.com). These requests include checks for configuration changes made within CPS, health monitoring for alerting purposes, and appliance backups for DR purposes.

During the initial provisioning stage, each CloudBoost appliance must download additional components from http://mirrors.kernel.org. After the initial provisioning stage has been completed, no additional connectivity is required.

CloudBoost does not require connectivity other than the secure (HTTPS) outbound connections that the appliance itself establishes with CPS. CloudBoost does not require incoming connections from CPS or any other management source for any data or management operations.

**WHAT CPS STORES FOR CLOUDBOOST**

When a CloudBoost appliance is deployed within your CPS account, CPS will store appliance usage tracking along with active appliance configuration details and appliance generated events and alerts.

Stored data does not include copies of the key database, which is stored within each CloudBoost appliance, and as such does not allow for access to customer data. At no time does CloudBoost store customer data in CPS.

Additionally, usage tracking includes information on CloudBoost appliance usage only; it does not include any information on systems or endpoints using CloudBoost. An example would be backups performed by EMC NetWorker where CloudBoost usage tracking does not contain information on systems protected by EMC NetWorker.

The CloudBoost appliance periodically backs up its metadata (including key hash database) for disaster recovery purposes. The data is written to the active Cloud Profile (object store) set for the appliance. This object store is the same object store that is used for data storage by the appliance. This data is not stored within CPS itself.

The default CloudBoost backup interval is every 2 hours and can be configured as needed.

Starting with CloudBoost 2.1, the configuration backups can optionally be additionally encrypted with a customer provided private key prior to storage. Note that in case of possible loss of the private key used for encryption of appliance backups, there are no means to recover the appliance. If no private key is provided by the customer, the option remains to allow the CloudBoost appliance to encrypt the backups and manage the keys directly.

Support logs are transferred to EMC using EMC’s optional Secure Remote Services (ESRS). ESRS service is not enabled by default.

**VIRTUSTREAM STORAGE CLOUD**

Virtustream Storage Cloud (VSC) is built for the world’s largest enterprises, service providers, and public sector organizations, which need to secure, manage, and store large, mission-critical workloads in the cloud.

VSC provides a hyper-scale storage platform with enterprise-class resiliency and performance built-in. In addition to availability as a Web-scale object storage platform for cloud-native applications, VSC provides seamless cloud extensibility for on-premises EMC storage, providing customers with simple and efficient backup, archive and cold storage in the cloud.

Cloud Portal & Services is the primary platform for managing purchased VSC storage.

CPS delivers both a simple Graphical User Interface and an API for monitoring VSC usage and configuring EMC managed products to access VSC. Connecting a managed product to VSC object storage becomes as trivial as selecting a pre-configured Cloud Profile.
CPS is not required for the normal operations of VSC, or for the interconnections between a CPS managed product and VSC. CPS is required for provisioning, configuring, monitoring and alerting. Should connectivity between VSC and CPS ever be disrupted, CPS will alert users to the issue while continuing to functioning as usual.

**PROVISIONING VIRTUSTREAM STORAGE CLOUD**

When a customer purchases VSC, a storage account will be created and a linked CPS account will be created. If a customer already has an active CPS account, the existing account will now reflect the newly added storage access.

Storage credentials will be available to the CPS account and any managed products attached to the CPS account. Storage credentials are generated per customer account.

**VIRTUSTREAM SECURITY**

VSC comes with an industry standard 99.9% uptime guarantee for service reliability. Durability has been architected, designed and developed into every component. VSC delivers a data durability rating of 99.999999999% (11 9s) for standard (geographically protected) and 99.99999999999% (13 9s) for premium (regionally protected) buckets.

VSC is backed by an internal 24x7x365 security operations center that monitors threats and detects security issues before they happen. The Security Operations and Engineering team also perform threat level detection, external penetration testing and validation that all components are hardened for maximum resiliency.

**WHAT CPS STORES FOR VIRTUSTREAM**

CPS operates the concept of a Cloud Profile. A Cloud Profile is a combination of the VSC storage API endpoint URL, the Access Key ID and Secret Access Key. The Access Key ID is a specific and unique key that separates one
customer of the object storage service from another. The Secret Access Key is a specific and unique key that when combined with a valid Access Key ID forms the basis for all signed requests made to the VSC service.

VSC exposes an Amazon Simple Storage Service (S3) like object storage API. The CPS account storage credentials are used to sign each S3 API request and provide secure access to Virtustream Storage Cloud objects.