DATASTAX MANAGED CLOUD SECURITY OVERVIEW

The purpose of this document is to:

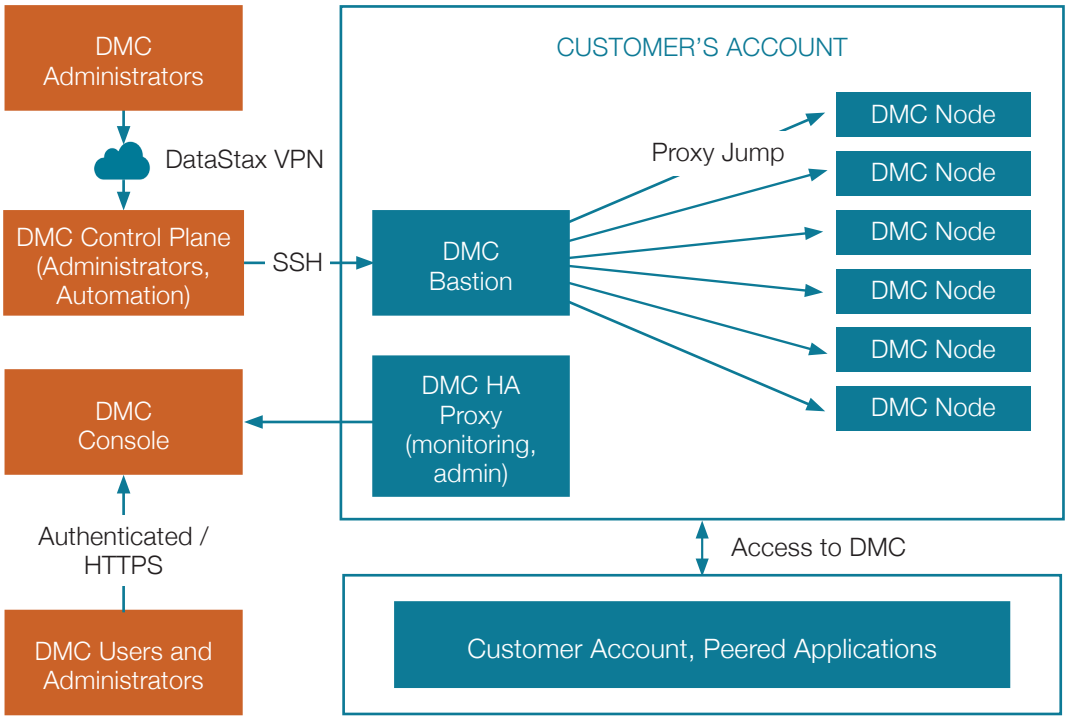
- Provide a brief overview of the architecture of the DataStax Managed Cloud platform and the customer environment
- Map the data flows of the sensitive data that exists in the DataStax Managed Cloud platform

The DataStax Managed Cloud platform consists of a Control Plane (CP) that exists in the DataStax account and a series of environments that are created in the customer account. For the purposes of this document, we will limit the discussion of the Control Plane to administrative access from users, and how that environment is used to access the customer account.

ARCHITECTURE OVERVIEW

The Control Plane is the primary way that administrators and automated processes access the customer account to monitor and administer DataStax Enterprise (DSE) clusters in the customer account. Access to these accounts is mediated by a DataStax managed VPN into the Control Plane that is used by DataStax administrators. A customer may have one or more environments associated with their account. These environments exist in an AWS account that is owned by the customer. The customer then grants rights and privileges for the AWS account to DataStax Managed Cloud administrators who then create the resources required to run DataStax Managed Cloud clusters in the account.

The picture below is a high level illustration of the DataStax Managed Cloud platform including DataStax owned components and customer owned components (Customer Account and Peered Applications).



AUTHENTICATION AND ACCESS CONTROL

DataStax Managed Cloud administrators who access the Control Plane must do so through a VPN that requires two factor authentication. Only after logging in through the VPN with their credentials and second factor can they access a customer bastion through the internet gateway egress IP address in the Control Plane. In addition to IP restrictions, the DataStax Managed Cloud bastion only allows authorized users to log into the machine using public key authentication.

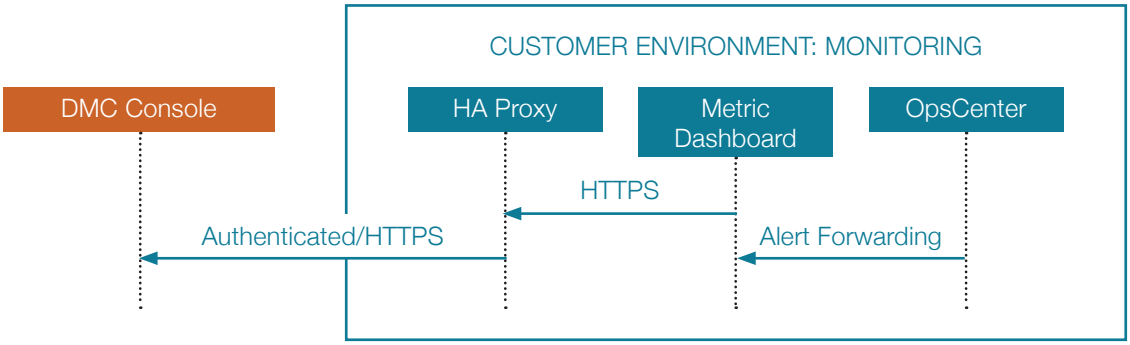
Logins from the bastion host are monitored using auditd, and DataStax has visibility into the actions taken on each of the data nodes inside the customer environment. All images are hardened using the CIS server hardening guidelines using elements from both the Level 1 and Level 2 benchmarks.

SENSITIVE DATA AND DATA FLOWS

The most sensitive data in DataStax Managed Cloud is the customer data that resides on the DataStax Managed Cloud node. This data is encrypted at rest and only stored in the customer account. During maintenance, backup, and recovery no data will leave the customer account. Ancillary data (DSE logs, Authentication logs, and monitoring data and tools) are made accessible by DataStax outside the cluster to authenticated accounts through the DataStax Managed Cloud Console and through OpsCenter.

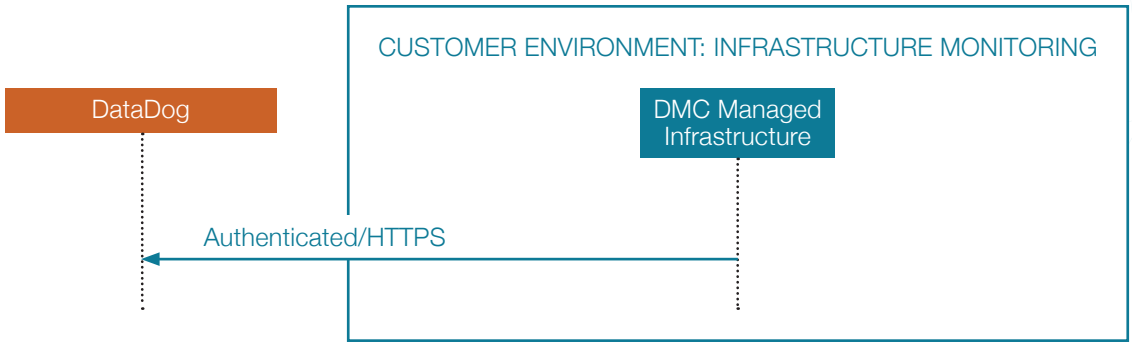
Those data flows are illustrated below:

DATASTAX MANAGED CLOUD MONITORING OF CUSTOMER ENVIRONMENTS



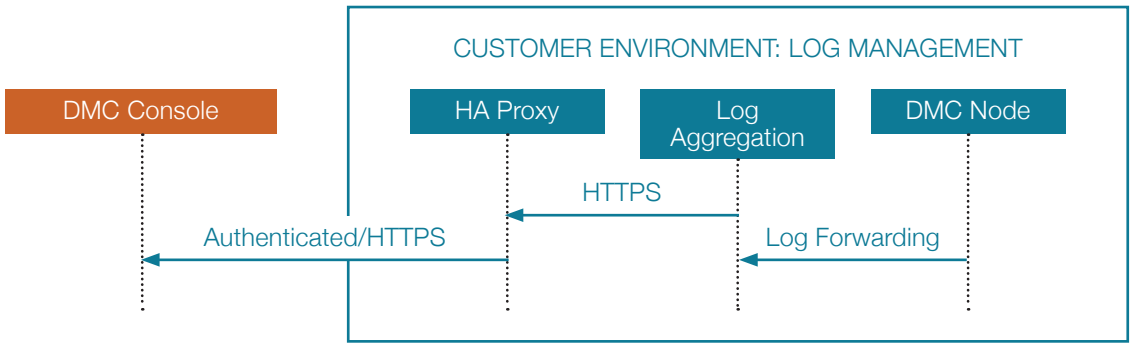
In this scenario, the metric dashboard (which exists in the customer account) is used to monitor metrics provided by the OpsCenter daemon. Those operational metrics are forwarded to monitoring services and used by the DataStax Managed Cloud Console to generate reports and alerts necessary for maintaining and monitoring DataStax Managed Cloud.

DATASTAX MANAGED CLOUD MONITORING OF CUSTOMER INFRASTRUCTURE



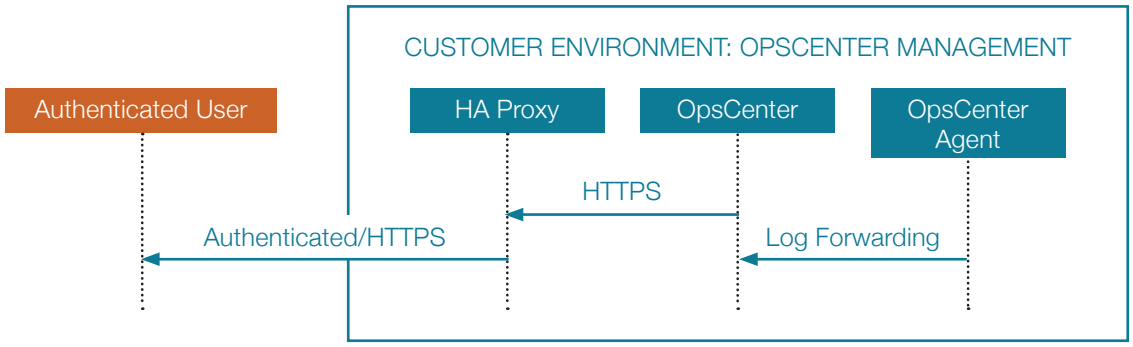
Critical infrastructure is monitored by DataDog, a monitoring service for cloud-scale applications. DataStax Managed Cloud installs an agent on each machine that forwards operational metrics to DataDog. These operational metrics monitor the health and status of machines in the environment.

DATASTAX MANAGED CLOUD LOG MANAGEMENT AND AGGREGATION



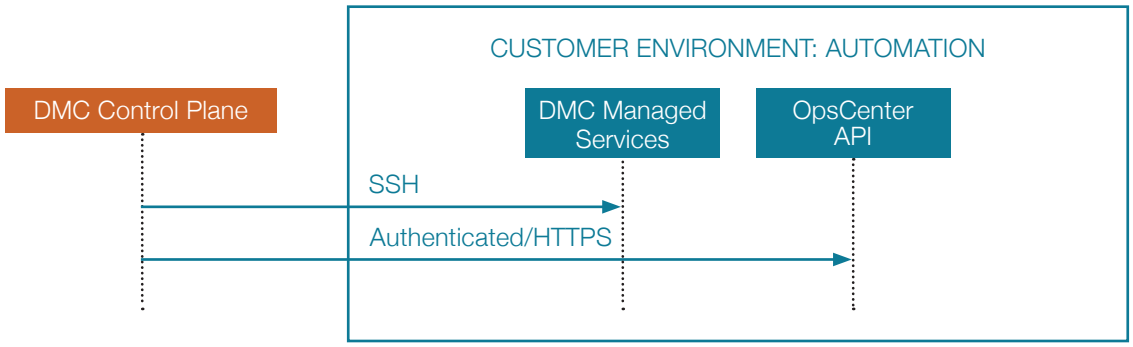
Administrators need access to DataStax Managed Cloud logs to be able to troubleshoot issues and perform ancillary analysis of the critical functions of DataStax Managed Cloud. In addition, DataStax monitors auth logs and critical metrics related to OS health and security (e.g. syslog, auth.log). Log data is collected on the DataStax Managed Cloud node and forwarded to a log aggregator which lives in the customer environment. That log information can be queried by the Cloud Console through an authenticated proxy.

DATASTAX OPSCENTER ADMINISTRATION



DataStax Managed Cloud administrators are given access to the OpsCenter instance inside of the customer environment to run routine management tasks on the DataStax Managed Cloud nodes. This service is an integral part of the DataStax Managed Cloud platform. Users authenticate to OpsCenter through a proxy and perform operations on the cluster through the web interface, or REST API.

DATASTAX MANAGED CLOUD API AUTOMATION



DataStax Managed Cloud administrators access our Managed Cloud API through the Control Plane. The Control Plane accesses the customer environment through a combination of the OpsCenter API and SSH access through a secure bastion.

SUMMARY

DataStax Managed Cloud provides a comprehensive set of security features to ensure your data is protected and the underlying systems can only be accessed by authorized users. DataStax Managed Cloud consists of a Control Plane that allows the administrators and automated processes to access, monitor, and manage the DSE clusters in the customer account. Access to Control Plane requires a two factor authentication, and IP whitelists allows only authorized users to log into the DataStax Managed Cloud nodes using public key authentication. All customer data is encrypted at rest and always remains in the customer account even during backup and maintenance. In addition, DataStax Managed Cloud provides operational metrics to monitor the DSE clusters and ensure peak performance.

DATASTAX