Breeze

Description

Breeze is a discovery and configuration management agent that streams OS-level data into Cloudaware CMDB and seamlessly enables other Cloudaware subscription services such as Intrusion Detection (IDS), Patch Management, Vulnerability Scanning, CIS Benchmarking, Event Monitoring. Customers can also develop their own Breeze plugins and extend the CMDB visibility or deploy their own services to Breeze-enabled hosts.

Key Design Goals

- Ease of deployment (make installation just a single command)
- Portability (run on everything with no OS and minimal network dependencies)
- Low resource utilization (do not break anything)
- Extendable (allow for pluggable framework and ability self upgrade to accommodate unforeseen future requirements, allow user to develop their own plugins)
- Reliable and reviewable security architecture (leverage standards like x.509 and SSL)
- Ability to enforce the desired state

Supported Ecosystems

- AWS EC2
- GCE
- MS Azure
- Kubernetes, AWS EKS, MS AKS
- VMWare
- Docker, LXC, Rocket containers
- Physical and Virtualized Servers

All major flavors of Linux and Windows are supported.

Required Network Dependencies

- Breeze requires outbound internet access only on port TCP 443
- Breeze does not require any inbound connections and can be deployed on private networks and servers with no public IP addresses

- Breeze supports IPv4 and IPv6
- If you need to lock down outbound access to a specific IP address, contact your technical account manager at tam@cloudaware.com

Supported Breeze Subscription Services

- IDS
- Vulnerability Scanning
- Patch Management
- CIS Benchmarking
- Event Monitoring

If customers subscribe to any of the above services, they are enabled on every server by installing Breeze.

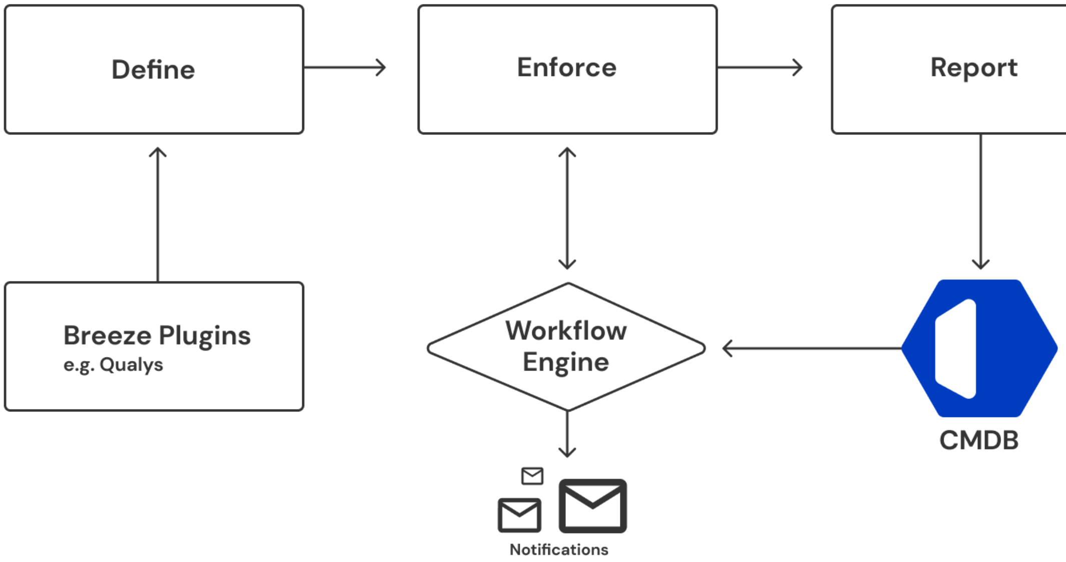
Using Breeze For Discovery

By default, Breeze has following discovery plugins enabled:

- Instance Facts
- OS Services
- Software Asset Management
- OS Users
- Mount Points (Linux Only)
- Drives (Windows Only)
- Upgradeable Packages
- Linux Repositories (Linux Only)

Using Breeze For Configuration Management

Customers can deploy Breeze for configuration management purposes. There are three stages in Breeze Configuration Management:



Define

Breeze plugins are written in a declarative language that specifies the desired state such as what users need to be present, what packages need to be installed and what services need to be running.

Enforce

Desired state is evaluated every 15 minutes. If a deviation is identified, Breeze will report it into CMDB and either:

- Notify and Not Enforce Desired State
- Notify and Enforce Desired State

Default behavior is to enforce the desired state.

Report

All Breeze reported data is available in CMDB and is reportable and dashboardable. Customers can configure additional workflows directly in CMDB to decide how a deviation or report data is to be handled. For example, a customer can create a notification or incident workflow when a deviation from the desired state is identified. Breeze agent can leverage CMDB data to decide whether and how desired state is to be enforced.

Additional Breeze Plugins

Plugin Name	Description	Type
Instance Facts	Retrieves basic information about the host.	Discovery
AWS Facts	AWS Specific Data including EC2 User Data	Discovery
Azure Facts	Azure specific data	Discovery
Performance Data	Available Memory, Disk, Processor Models, etc.	Discovery
Storage, Mount Points, LVM	Provisioned vs. Utilized Storage	Discovery
OS Packages	All Packages Installed on OS	Discovery
OS Upgradeable Packages	All Upgradeable Packages	Discovery
OS Users and Groups	All Users and Groups	Discovery
OS Package Repositories	All Package Repositories	Discovery
SSH Settings	All SSH Settings	Discovery
Splunk	Show Splunk Version and Agent Status	Discovery
Apache Tomcat	Shows information about Tomcat App Server	Discovery
Apache Kafka		Discovery
Apache ActiveMQ	Shows information about	Discovery

	ActiveMQ Messaging Server	
Apache Hadoop		Discovery
Apache CloudStack		Discovery
Apache Mesos		Discovery
Microsoft SQL Server	Show information about SQL Server	Discovery
Microsoft IIS Server	Show information about IIS	Discovery
Microsoft Sharepoint	Show information about Sharepoint	Discovery
HIDS OSSEC	Installs and configures Host Based Intrusion Detection Agent	Configuration Management
HIDS TrendMicro Deep Security	Shows Agent Version, Status and Last Connect Date	Discovery
Nessus	Installs, configures and registers Nessus Vulnerability Scanning Agent	Configuration Management
Qualys	Installs, configures and registers Qualys Vulnerability Scanning Agent	Configuration Management
Rapid7	Installs, configures and registers Rapid7 Vulnerability Scanning Agent	Configuration Management
New Relic	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery

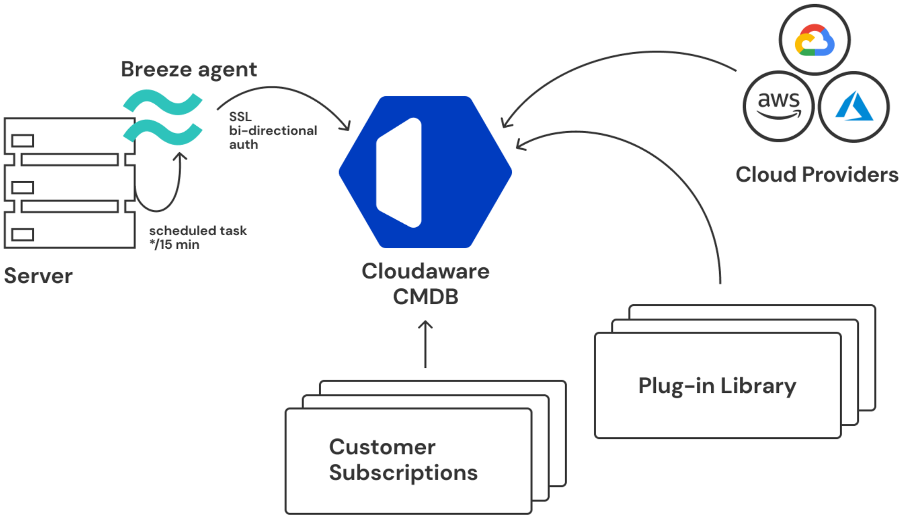
Nagios	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Pingdom	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Sensu	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
StackDriver	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Wormly	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Datadog	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
SolarWinds	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Zabbix	Shows agent status, version and last connect timestamp, performance	Discovery

	telemetry, incident statistics	
Nagios	Shows agent status, version and last connect timestamp, performance telemetry, incident statistics	Discovery
Chef	Shows agent status, version and last connect timestamp	Discovery
Puppet	Shows agent status, version and last connect timestamp	Discovery
Ansible	Shows agent status, version and last connect timestamp	Discovery
Yara	Run any custom yara scan for hard to detect vulnerabilities such as GrizzlySteppes and WannaCry	Command
ClamAV	Installs and deploys anti-virus agent	Configuration Management
Oracle WebLogic	Discovers all data about weblogic configuration	Discovery
Oracle MySQL	Discovers info about MySQL Configuration	Discovery
PostgreSQL	Discovers info about PGSQL Configuration	Discovery
IBM WebSphere[1]	Discovers all data about weblogic configuration	Discovery
Adobe Experience Manager	Discovers information about AEM configuration	Discovery

[1] Supports the entire suite of IBM WebSphere products, including Application Server, Message Broker, MQ, etc.

SAP Hybris	Discovers all data about SAP server configuration	Discovery
SAP Hana		Discovery
Adobe AEM		Discovery
Magento Ecommerce	Discovers all data about Magento server configuration	Discovery
WordPress	CMS Configuration	Discovery
Drupal	CMS Configuration	Discovery
Joomla	CMS Configuration	Discovery
Containers	Discovery information about Docker, Rocket and LXC containers	Discovery
GitHub	Discovery information about repos, users, branches, etc.	Discovery

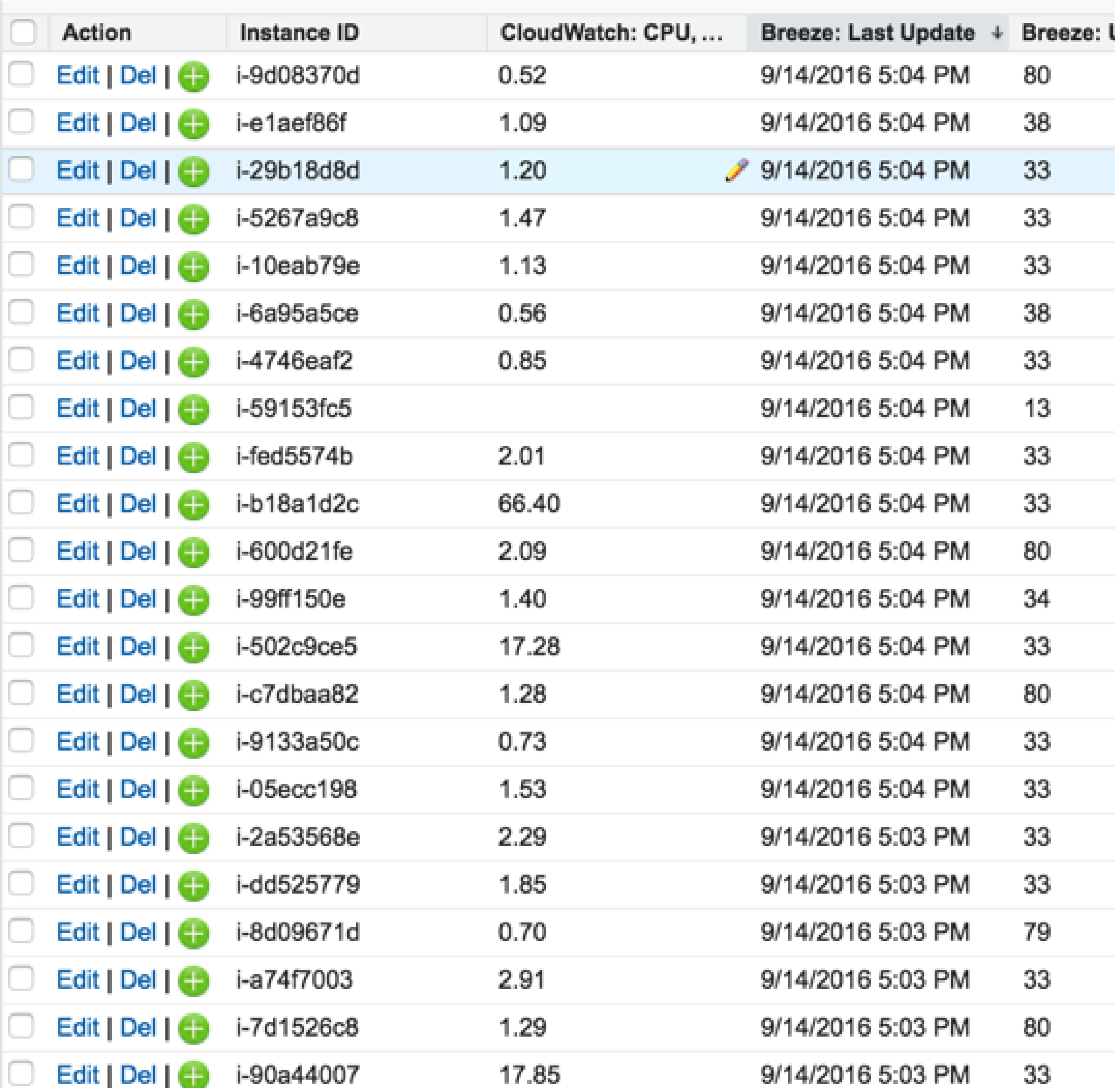
Architecture



1. At the host level, Breeze agent runs every 15 minutes as a scheduled task on Windows machines and as a cron task on Linux hosts.

2. Agents connect to CMDB. During the connection, both verify each other using pre-created SSL certificates. The agent will only trust pre-configured SSL certificates and CMDB will only establish connections with clients that can present SSL certificates signed by it.
3. Once CMDB knows which clients are connecting, it looks up what plugins and services are available to this customer and sends them to the agent. For example, if a customer is subscribed for IDS, Cloudaware will deploy an IDS plugin to the Breeze Agent.

CMDB keeps track of all hosts and the last time the Breeze agents connected to the CMDB.



□	Action	Instance ID	CloudWatch: CPU, ...	Breeze: Last Update ↓	Breeze:
□	Edit | Del | ⊕	i-9d08370d	0.52	9/14/2016 5:04 PM	80
□	Edit | Del | ⊕	i-e1aef86f	1.09	9/14/2016 5:04 PM	38
□	Edit | Del | ⊕	i-29b18d8d	1.20	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-5267a9c8	1.47	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-10eab79e	1.13	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-6a95a5ce	0.56	9/14/2016 5:04 PM	38
□	Edit | Del | ⊕	i-4746eaf2	0.85	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-59153fc5		9/14/2016 5:04 PM	13
□	Edit | Del | ⊕	i-fed5574b	2.01	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-b18a1d2c	66.40	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-600d21fe	2.09	9/14/2016 5:04 PM	80
□	Edit | Del | ⊕	i-99ff150e	1.40	9/14/2016 5:04 PM	34
□	Edit | Del | ⊕	i-502c9ce5	17.28	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-c7dbaa82	1.28	9/14/2016 5:04 PM	80
□	Edit | Del | ⊕	i-9133a50c	0.73	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-05ecc198	1.53	9/14/2016 5:04 PM	33
□	Edit | Del | ⊕	i-2a53568e	2.29	9/14/2016 5:03 PM	33
□	Edit | Del | ⊕	i-dd525779	1.85	9/14/2016 5:03 PM	33
□	Edit | Del | ⊕	i-8d09671d	0.70	9/14/2016 5:03 PM	79
□	Edit | Del | ⊕	i-a74f7003	2.91	9/14/2016 5:03 PM	33
□	Edit | Del | ⊕	i-7d1526c8	1.29	9/14/2016 5:03 PM	80
□	Edit | Del | ⊕	i-90a44007	17.85	9/14/2016 5:03 PM	33

Matching and Cloud Sensing, Container Sensing

Breeze agent self-detects whether it is running on a physical server, AWS EC2 instance, Beanstalk or Azure Instance. When the agent sends data to CMDB, CMDB attempts to match the agent data to the specific instance within a cloud provider.

If no match is made, Cloudaware assumes the agent is running on a non-cloud instance and creates a new entity/object in Cloudaware CMDB called Cloudaware Physical Server. If an AWS, GCE or Azure instance is matched, all agent-based data is recorded into the existing record.

Similarly, Breeze agent will detect if it is executing inside a container such as docker, and its agent data will be associated with the container record in CMDB.

FAQ

Question:

Can I develop my own plugins?

Answer:

Yes. At the moment, plugins are supported in Ruby only, however, other language plugins will become available as well.

Question:

Can I see what Breeze is doing on my machine?

Answer:

Yes, there is a Breeze log on every host.

Question:

Are there limits on how many plugins can be deployed?

Answer:

No, but deploying a high number of plugins might make Breeze runs tolling on the system's performance.

Question:

Can I control which plugins get deployed on a server by server basis?

Answer:

Yes. Using the Cloudaware CMDB management panel, you can select which plugins are available to individual servers. You can also configure plugins at the AWS Account, Azure Subscription or Google Project leve, based on tags and other custom attributes.