CA Performance Management Data Aggregator

Overview Guide

2.4.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA Performance Management Data Aggregator (Data Aggregator)
- CA Performance Management Data Collector (Data Collector)
- CA Performance Center
- CA Spectrum

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview

To get you started, this guide briefly explains the Data Aggregator concepts, how it works out of the box, and where you can modify it to suit your unique needs.

This section contains the following topics:

About Data Aggregator

As technology modernizes, most tools and processes you use to monitor your enterprise network environment quickly become outdated. And, if you are a service provider, this problem is multiplied by the number of tenants you support. How can you ensure operability, much less optimize, your infrastructure performance?

Data Aggregator integrates with CA Performance Center to provide a complete, scalable, and extendible solution for monitoring your evolving enterprise network environment. With built-in support for multi-tenancy, these products also help simplify management for service providers and large enterprises.

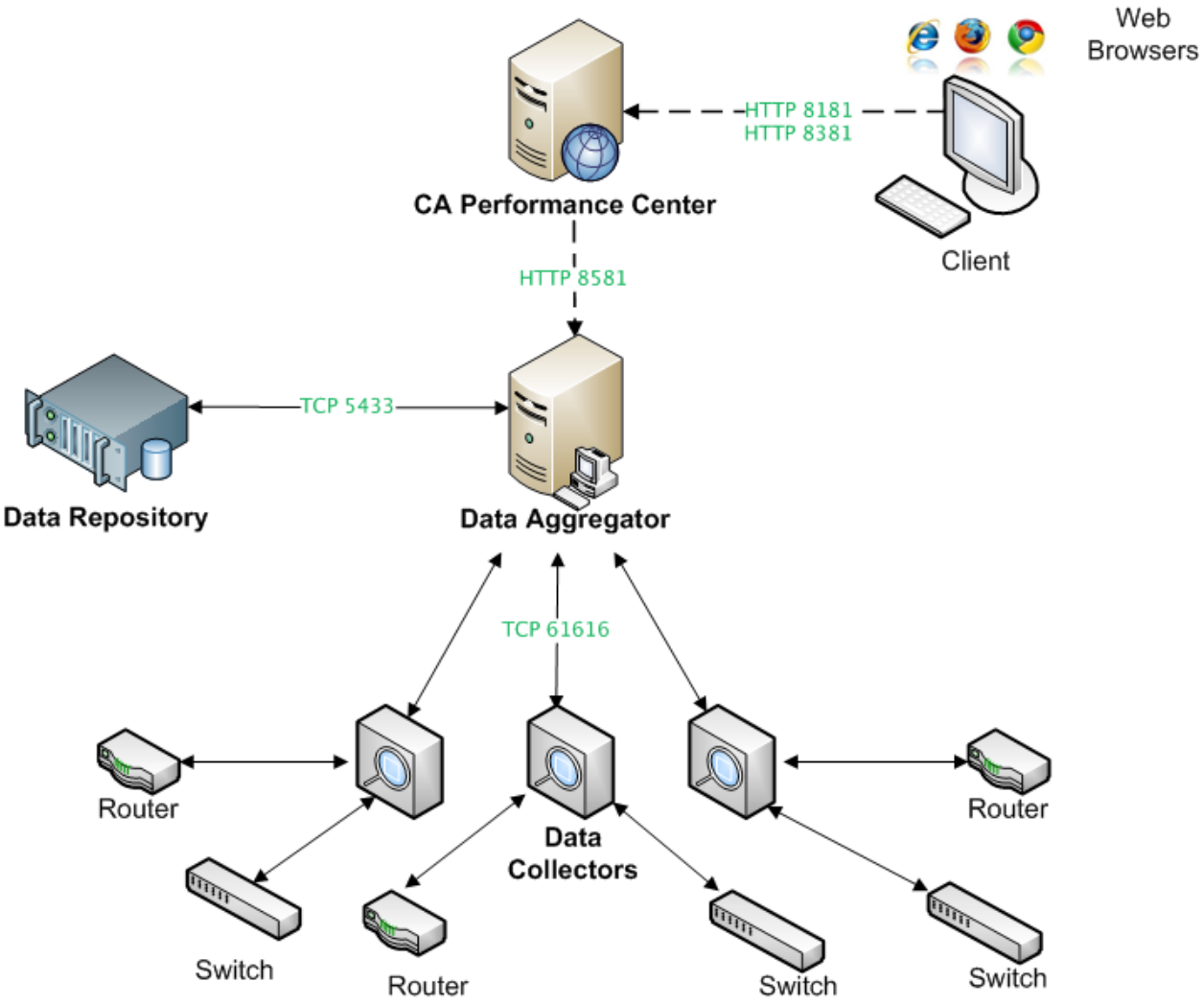
Data Aggregator works by creating an inventory of infrastructure devices through the "discovery" process. Then, it lets you select which metric data to collect on groups ("collections") of devices.

CA Performance Center provides the web-based user interface for both *configuring* Data Aggregator and *reporting* the infrastructure data. Using this data, you can create dashboards and reports to track trends, identify patterns, or troubleshoot abnormal behavior.

How Data is Collected

To understand your infrastructure and manage it, Data Aggregator must create an inventory. Data Aggregator builds the inventory through the discovery process. After it identifies your inventory, Data Aggregator collects information about each inventory device and passes it to CA Performance Center for viewing and reporting.

The following diagram shows a basic deployment scenario for Data Aggregator:



This diagram shows how the Data Aggregator components work to collect and report data from your infrastructure:

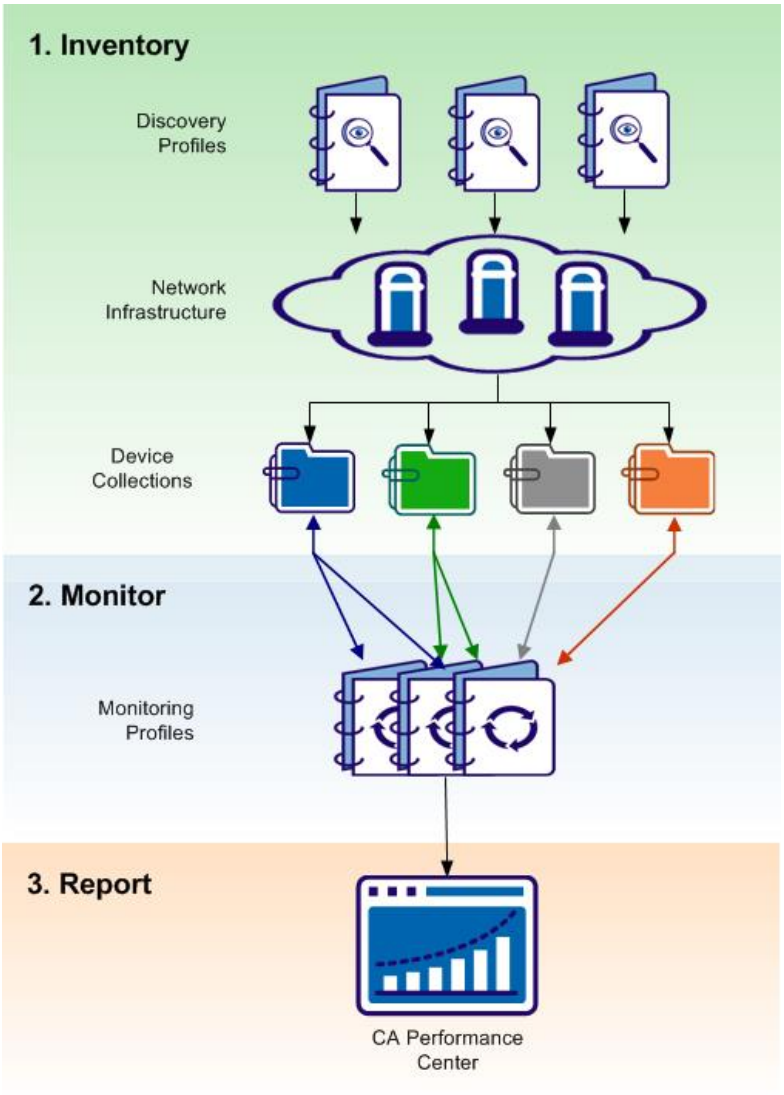
1. Data Collector coordinates data collection. The Data Collector components actively poll for data that is used for reporting and event analysis. You can deploy multiple Data Collector components throughout your infrastructure to help ensure adequate coverage of your infrastructure.
2. Data Aggregator gathers the data from each Data Collector and stores it in Data Repository.
3. CA Performance Center is the web-based interface for configuring Data Aggregator to manage your physical and virtual networks, applications, and devices. Also, CA Performance Center dashboards and views display the performance data that Data Aggregator, a data source, collects and processes.

Note: For more information about deployment strategies, see the *Data Aggregator Release Notes*.

Factory and Customized Features

Data Aggregator is configured to give you results right out of the box. After you install, the only required step is to **create and run a discovery profile**. This profile tells Data Aggregator where to find your devices and how to build your inventory.

Immediately, Data Aggregator gets to work—using its default monitoring configuration, Data Aggregator monitors and collects data about the devices in your discovered infrastructure:



As shown, Data Aggregator monitors your infrastructure in three stages:

1. **Inventory**—Data Aggregator builds your device inventory using discovery profiles. Based on their type, devices are added to device collections.
2. **Monitor**—For each device in a device collection, Data Aggregator collects metric data using the corresponding monitoring profiles. Data Aggregator also uses event rules to monitor the state of your devices.
3. **Report**—Data about your infrastructure displays in CA Performance Center dashboards and views.

To achieve the best performance while providing the appropriate level of detail, adjust the default profiles, as needed.

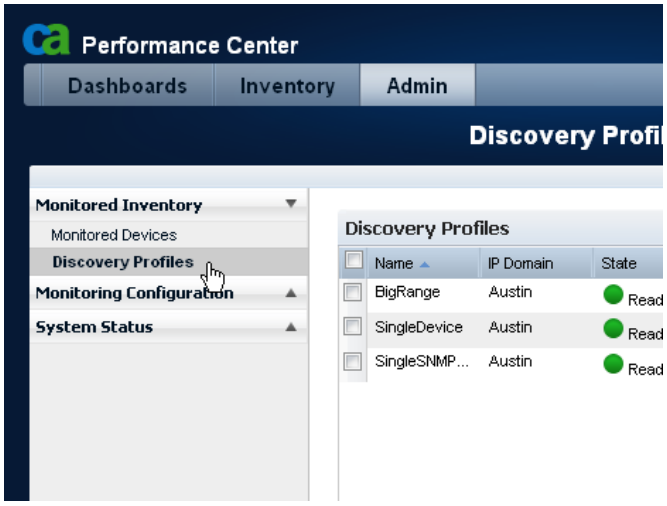
Note: For information about installing, see the *Data Aggregator Installation Guide*. For more information about registering a data source, see the *CA Performance Center Administrator Guide*. For more information about managing your monitoring configuration, see the *Data Aggregator Administrator Guide*.

Building Your Inventory

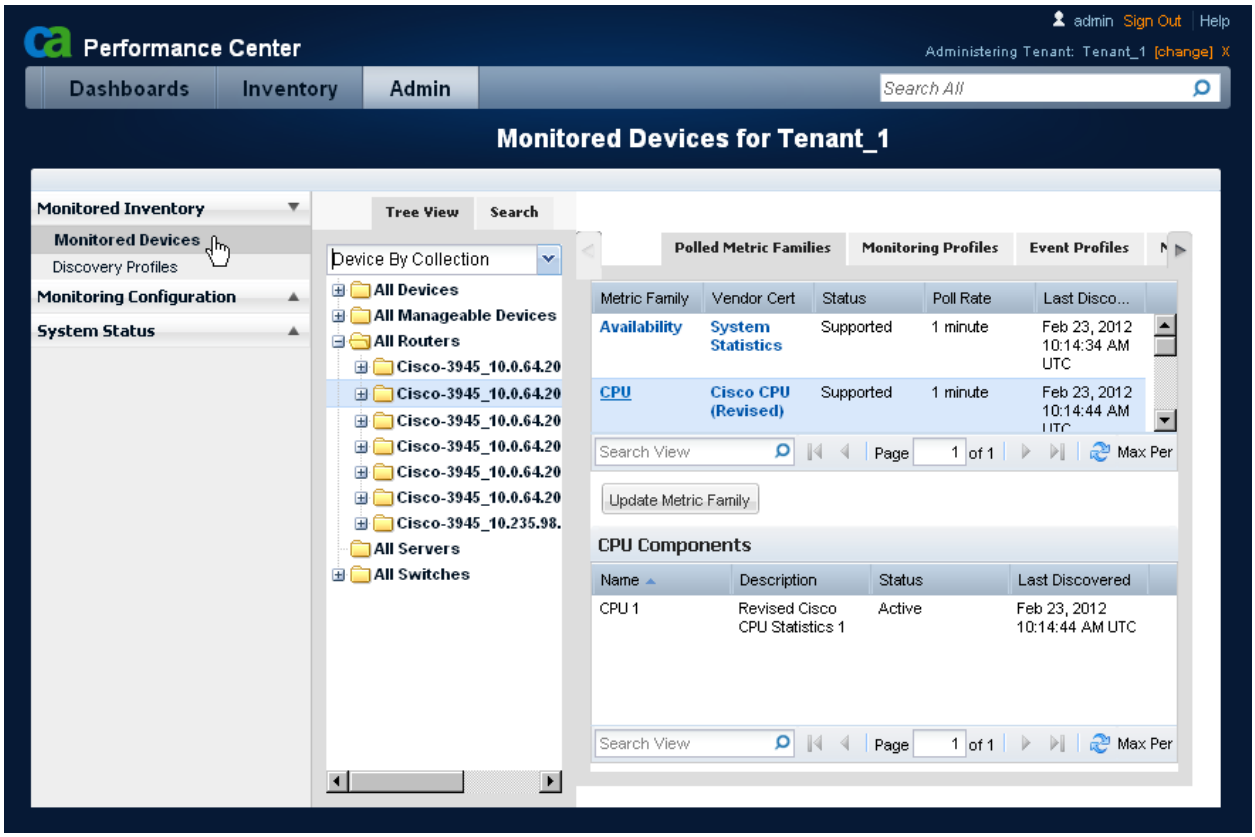
Before Data Aggregator can work, it must build a device inventory. Data Aggregator builds the inventory using discovery profiles. After discovery, Data Aggregator adds your devices to the appropriate device collections.

Note: Data Aggregator does not include factory (out-of-the-box) discovery profiles, so create at least one profile to begin.

Everything that you need to manage and monitor your inventory is available in CA Performance Center. As an administrator, open your data source in the Admin menu to view the Discovery Profiles List.



After you run a discovery, view your devices in the Monitored Devices List.



Customize Discovery Profiles

To optimize performance, you can create multiple profiles to customize discovery options for different devices. Configurable options include:

- Discovery of one or more devices using the IP address or host name
- Scheduling interval
- Device naming options
- ICMP discovery

For example, you can create discovery profiles for the following situations:

- Schedule weekly discovery for an East coast branch office.

  Note: We recommend that you have a discovery profile and IP Domain for each regional area/tenant—make sure your SNMP profiles correctly support each IP domain.

- Discover a new host manually after bringing it online.
- Create a discovery profile for each tenant.

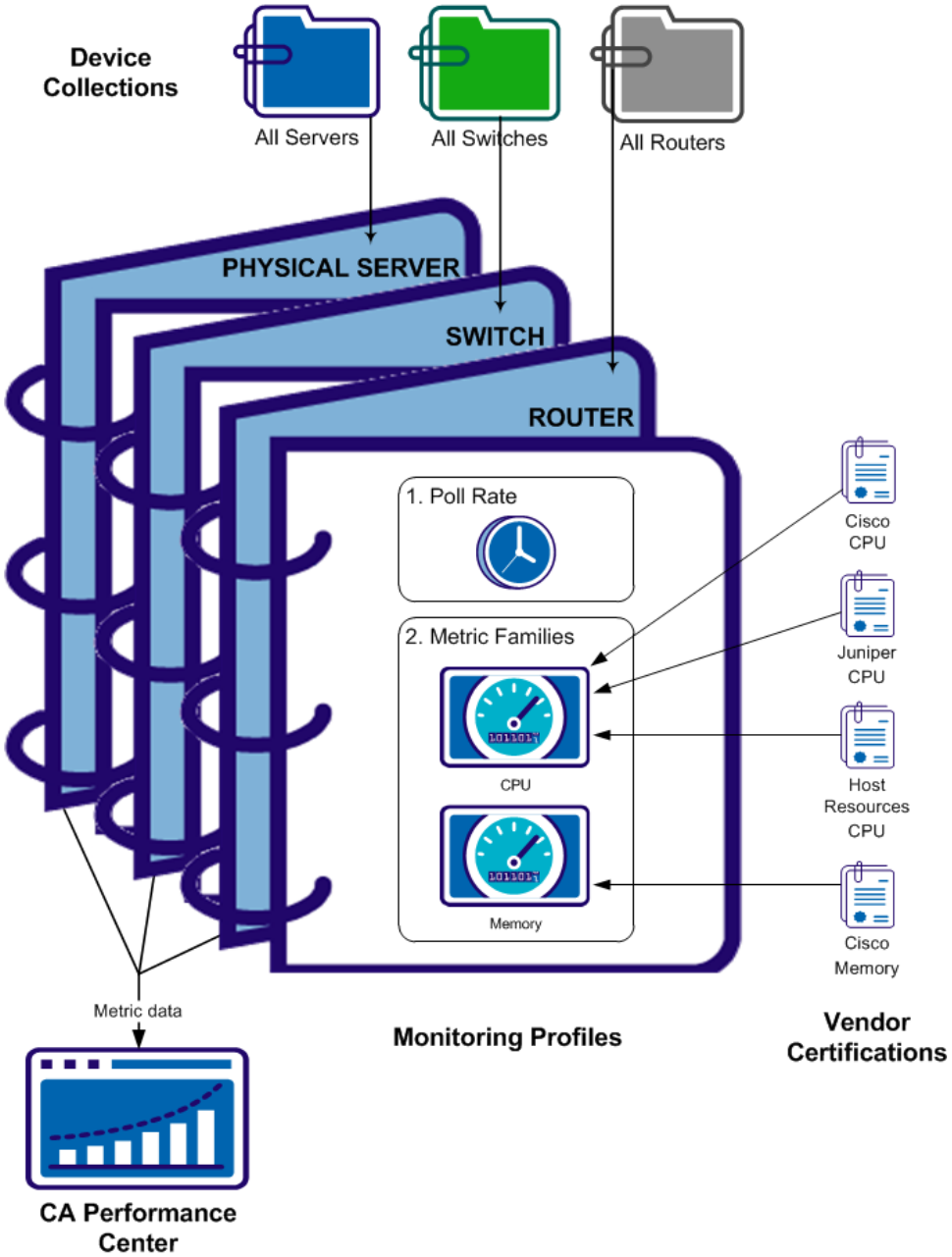
- Create a discovery profile that uses an external file of addresses or host names.
- Schedule discovery for an IP address range when you anticipate new devices coming online.

Note: For information about discovery profiles, see the *Data Aggregator Administrator Guide*. For more information about SNMP profiles and tenants, see the *CA Performance Center Administrator Guide*.

Selecting the Data to Monitor

Out of the box, Data Aggregator is configured to collect *basic* data about your devices using default monitoring profiles and certifications, as shown.

Note: To collect additional data, customize the monitoring configuration (see page 15).



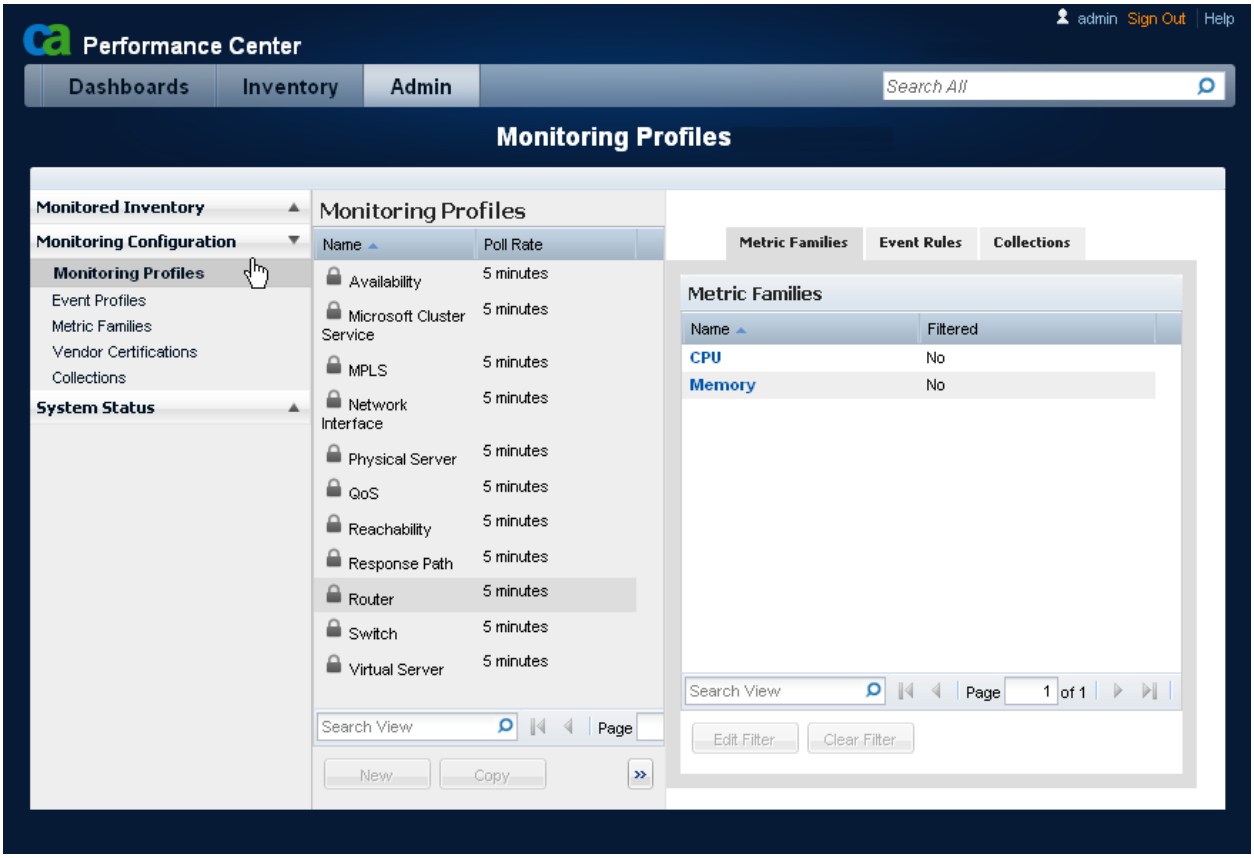
As shown, Data Aggregator collects data from devices using the relationships between the following components:

- **Device Collections**—Device collections are groups of similar devices. These groups can be based on the device type (such as routers) or levels of service (such as high availability/high frequency polling).
- **Monitoring profiles**—A monitoring profile defines a polling rate and a set of metric families. When you associate a monitoring profile with a device collection, Data Aggregator knows to poll all devices in that device collection. A monitoring profile can be associated to one or more device collections.
- **Metric families**—A metric family defines a set of related metrics and determines how to report the values for each metric. Monitoring profiles can reuse the same metric families.
- **Vendor certifications**—A vendor certification supports devices from third-party vendors by mapping the vendor MIB attributes to the metrics in a metric family. Mapping these values helps ensure that Data Aggregator uniformly reports the metric values, regardless of the device vendor.

Working together, these profiles and certifications determine which metric data to send to CA Performance Center.

Important! *The key to starting and stopping the monitoring process is the device collections*. Data Aggregator cannot use a monitoring profile unless you associate it to at least one device collection.

You can manage the relationships between these device collections, profiles, and certifications using CA Performance Center. As an administrator, open your data source in the Admin menu to view the Monitoring Configuration.



Customize the Monitoring Configuration

To achieve the best performance while providing the appropriate level of detail, you can adjust the default monitoring configuration to help ensure:

- Metric data that you want is available.
- Metric data that you *do not* want is ignored.
- Metric values are formatted correctly.
- Network performance is impacted minimally.

For **collections**, we recommend that you *always* create custom device collections. Custom device collections help you:

- Minimize unnecessary poll data.
- Reduce network management traffic and load on your monitored infrastructure, improving monitoring performance.
- Get granular control of your monitoring configuration by applying refined monitoring profiles to specific device collections.

For **monitoring profiles**, create new or copy factory profiles to adjust (customize) the following aspects:

- Polling rate (Example: Decrease the polling rate of the Physical Server profile)
- Metric families—Select or remove metric families to adjust which metric values are collected (Example: Remove a metric family from a monitoring profile to reduce the metric values that are polled for a device collection).
- Filtering—Configure the component filtering to determine which interfaces are monitored. Data Aggregator provides composite filtering rules that you can use.
- Device collections—Configure the associated device collections to establish which devices are monitored (Example: Create a custom monitoring profile to support a custom device collection).

  Note: Data Aggregator supplies a rich set of monitoring profiles. Most of these profiles are *not* associated with any device collections (such as, the Interfaces monitoring profile).

  Tip: Do not associate factory monitoring profiles to a device collection. Instead, always use a copy as a template—configure the name, poll rate, metric families, and any filters and event rules. Then, associate it to a custom device collection. Because the factory monitoring profiles can change, this process helps minimize the impact to your monitoring environment.
- Change detection for components—Choose whether to update configuration data automatically for your components. Also, set the rate of change detection (Example: Increase the change detection rate for components that change frequently, such as interfaces).

For **metric families**, create one to collect metric values that are not supported out of the box. For example:

- Processes metric family
- Applications metric family

For **vendor certifications**, advanced administrators can create them for third-party devices for which Data Aggregator does not provide a factory certification. You need the vendor MIB to get started.

Note: For more information about metric families and vendor certifications, see the *Data Aggregator Self-Certification Guide*. For more information about managing device collections and monitoring profiles, see the *Data Aggregator Administrator Guide*.

Monitoring Metrics with Event Rules

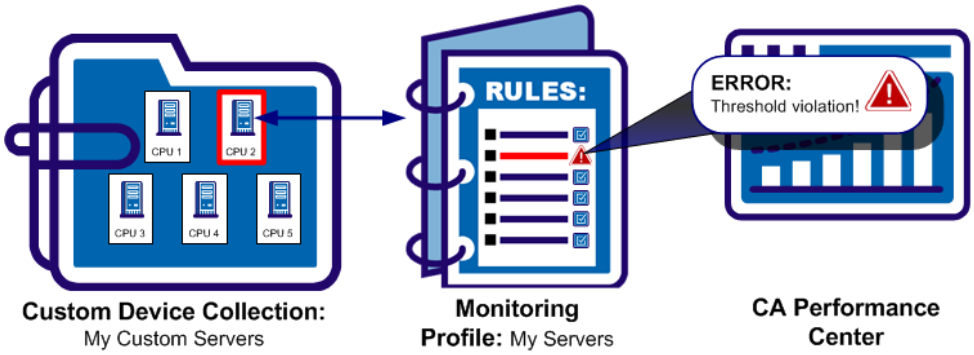
Events provide useful information when monitoring the health and status of your network environment. Data Aggregator events can be viewed in CA Performance Center, forwarded to other applications as SNMP traps, or emailed to other engineers. If you have CA Spectrum integrated with CA Performance Center, you can send events to CA Spectrum for enhanced fault management and incident management.

Data Aggregator generates events upon evaluating event rules that are contained in monitoring profiles. Using metrics (from your metric families), these rules define the conditions that you want to watch for.

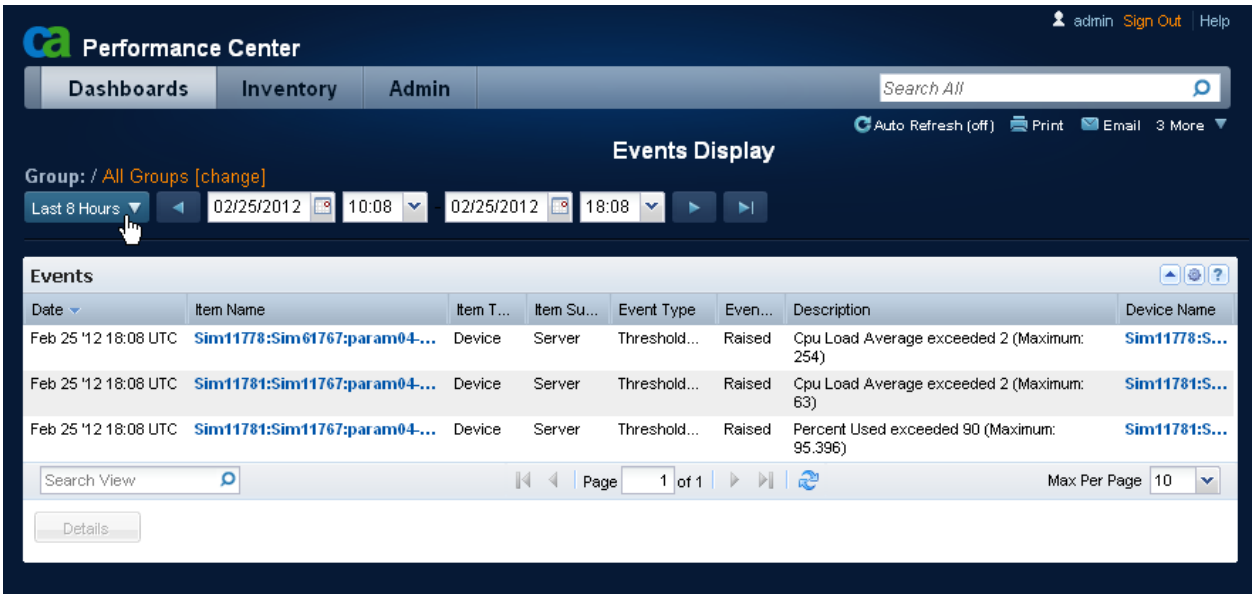
To implement your event rules, associate the monitoring profile with a custom device collection.

Important! *The key to starting and stopping the monitoring process is the device collections.* Data Aggregator evaluates event rules only when the parent monitoring profile is associated to a specific device collection. If no association is made, event rules are ignored.

Immediately, Data Aggregator applies the event rules in that profile to the devices in that device collection. Using the metric values that are polled for these devices, the rules trigger events as needed.



Events display in a CA Performance Center dashboard.



Note: You can generate user-visible alarms in CA Spectrum from events that are processed and logged in Data Aggregator. For more information, see the CA Spectrum documentation.

Customize Event Rules

Customize event rules so that Data Aggregator generates only events that matter to you. You can create multiple event rules. For example, you can apply different thresholds for memory metrics for different device collections. Other ways to customize how Data Aggregator monitors events:

- Assign or remove device collections to or from a monitoring profile.
- Add or remove event rules to or from a monitoring profile.
- Adjust the values in a rule, such as the threshold values, severity level, or more.

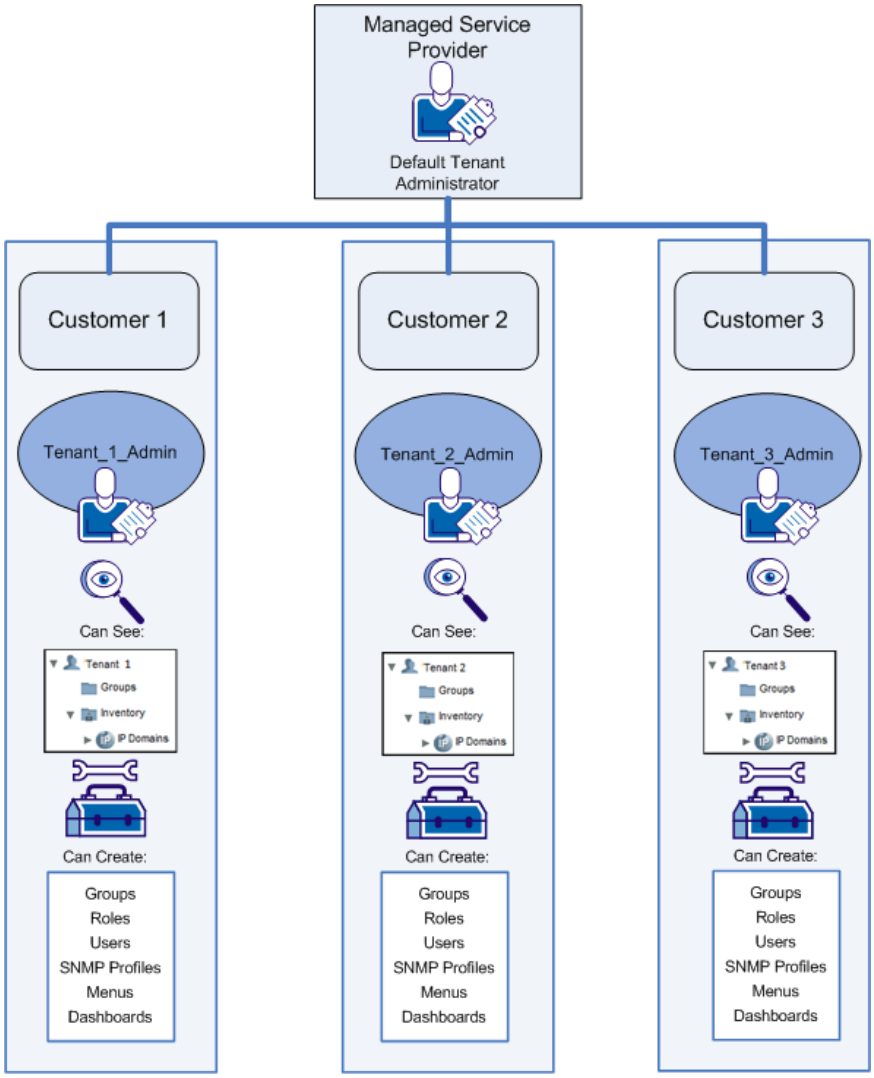
Note: For more information about managing event rules, see the *Data Aggregator Administrator Guide*.

Managing Multiple Tenants

For service providers or large enterprises, Data Aggregator supports multi-tenancy—a capability that allows shared use of the same tool deployment across multiple groups of users. A *tenant* represents a customer (group of users) that a service provider administers. This feature lets you create multiple tenants and monitor their environments separately.

Multi-tenancy is especially helpful for managed service providers, but large enterprises can also apply this feature. For example, they can separately manage different departments or branch offices.

At every level, the distinction between tenants is complete—users that are assigned to a tenant cannot see data from other tenants. Even with overlapping IP address ranges, Data Aggregator helps ensure this separation using unique IP domains for each tenant. When multi-tenancy is deployed, Data Aggregator supports two distinct administrator roles: Default Tenant Administrator and Tenant Administrator.



The Default Tenant Administrator creates and manages the following Data Aggregator components:

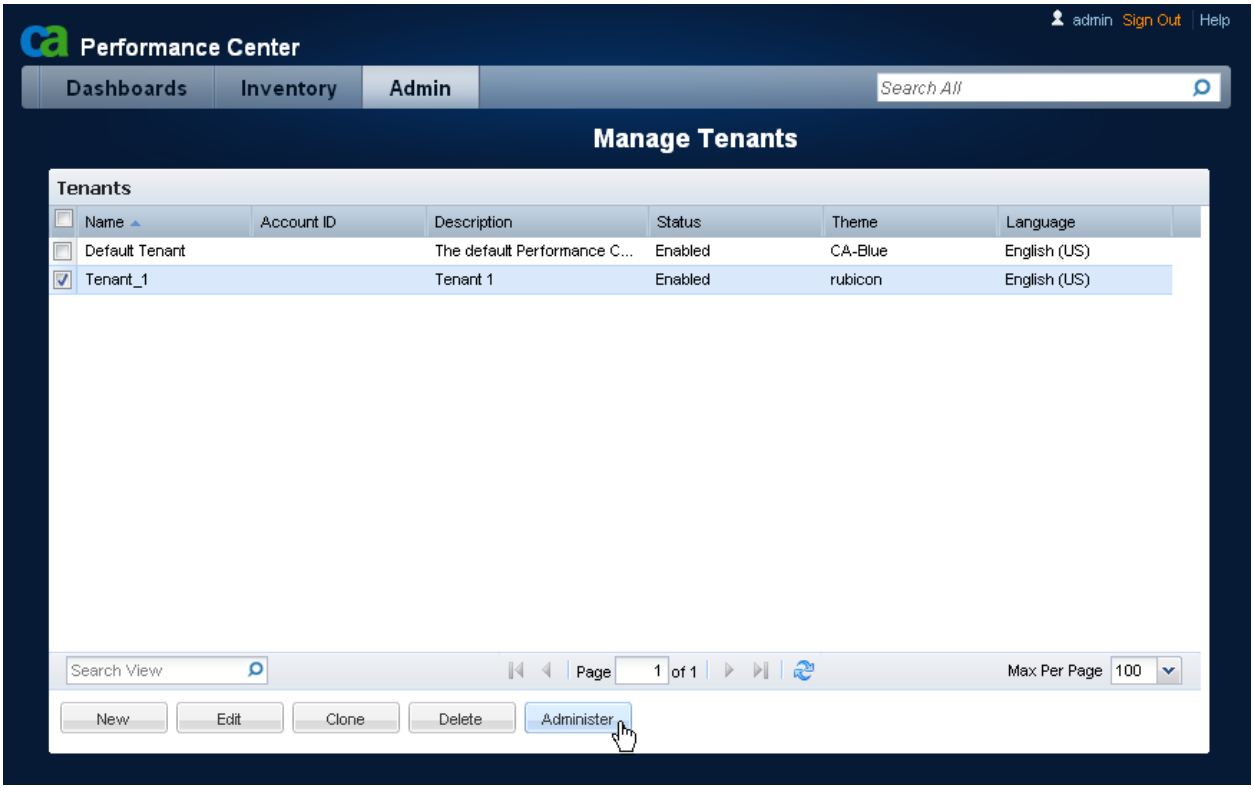
- Monitoring profiles

- Metric families
- Vendor certifications

Tenant Administrators are responsible for applying these components to their own environments, as follows:

- Associate device collections with monitoring profiles
- Create and manage discovery profiles
- Create and manage SNMP profiles
- Start and stop Data Collector installations

The Default Tenant Administrator can manage individual tenant environments using the "Administer" feature. Open the Manage Tenants view from the Admin menu to select a tenant environment.



Note: For more information about deploying multi-tenancy, see the *CA Performance Center Managed Service Provider Guide*. For more information about the Default Tenant Administrator and Tenant Administrator tasks, see the *Data Aggregator Administrator Guide*.

Resources to Optimize Data Aggregator

After you configure your basic setup, review the following guides and consider these additional tasks to optimize how you use Data Aggregator.

CA Performance Center Administrator Guide and *CA Performance Center Operator Guide*:

- Create and manage user accounts.
- Create and manage tenants.
- Create custom dashboards, reports, and views in CA Performance Center to highlight the data you need.

Data Aggregator Administrator Guide:

- Adjust memory usage for poll caching or large-scale deployments.
- Avoid collecting unwanted data by setting an interface filter.
- Delete any devices that you no longer want to monitor.
- Decide how Data Aggregator manages component changes in your infrastructure by adjusting device reconfiguration settings.
- Start or stop Data Aggregator, Data Collector, or Data Repository to perform maintenance on the host server.

CA Performance Center Single Sign-On User Guide:

- Enable single sign-on between CA Performance Center and Data Aggregator by configuring authentication settings.

Data Aggregator Administration Using REST Web Services Guide:

- Improve the performance of sensitive devices by configuring SNMP traffic and timeout thresholds.
- Use REST web services to manage administrative operations using an API, such as retrieving data or managing relationships between profiles and tenants or device collections.

Data Aggregator RIB API Guide:

- Build custom reports using a web services interface to access the Data Aggregator database.

Glossary

dashboards

Dashboards are dynamic report-building pages within the CA Performance Center user interface. They appear as menu items that are accessible from the Dashboards tab. Each dashboard is a collection of views that present data from registered data sources on a single web page. The layout, views, time interval, and group context of each dashboard can be customized.

Data Collector

Data Collector coordinates data collection and actively polls for data that is used for reporting and event analysis. Operational metrics and configuration data are polled on discovered devices and their monitored components. The collected data is passed through Data Aggregator and is stored in Data Repository.

data sources

Data sources are the supported products that provide performance and configuration data to CA Performance Center. Data source products that monitor, collect, and aggregate data can often function independently. However, once they are registered to an instance of CA Performance Center, they are known as data sources.

device collection

A *device collection* is a logical grouping of monitored devices, such as servers or routers.

Discovery profile

A d*iscovery profile* specifies how inventory discovery operates, including the IP addresses, IP address ranges, and host names that are used to locate your devices.

factory

The term "*factory*" in Data Aggregator describes items that CA Technologies provides and are often installed with the product. For example, Data Aggregator provides factory vendor certifications, monitoring profiles, and more. These out-of-the-box items can help you get Data Aggregator operational upon installation. They can also serve as examples for creating or importing custom versions of the same item. Mostly, Data Aggregator users cannot edit these factory items.

item

An *item* can be a device, component, or an interface that Data Aggregator monitors.

metric family

A *metric family* defines the set of values to collect and report on for a given technology. These values are normalized so that reporting is uniform regardless of the data source. When included in a monitoring profile, metric families determine which values to collect for the devices that are associated with that monitoring profile.

monitoring profile

A *monitoring profile* is associated with a collection of devices to specify the information to poll and the polling rate. These parameters are applied to each device in the device collection. A selection of default monitoring profiles that are based on types of devices such as routers, switches, and servers is provided.
The monitoring profile also contains the event rules that are applied to each device item in the associated device collection. Rule evaluations occur on each device item in the device collection, and on each metric that you specify in the event rules. These rule evaluations generate either raised or clear events. These events are then sent to Event Manager in CA Performance Center, CA Spectrum, and to CA Performance Center Notifier for further action.

reports

Reports are static output from an on-demand selection or an exported dashboard page. Reports that you export from a dashboard create a static data set from the data and information in the associated dashboard. On-demand reports capture a data set from a single managed item or group in the Inventory. You can print reports, send them by email, or export them in CSV or PDF format. For each format, the report captures a selected data set.

SNMP profiles

SNMP profiles are definitions that contain the information necessary to enable secure queries of device MIBs using SNMP.

vendor certification

A *vendor certification* maps attributes from a vendor MIB to the metrics specified in a metric family. Also, vendor certifications determine how metrics collected from an item are formatted for use in the CA Performance Center UI and reports. Metrics that are provided for an item can vary, depending on the vendor for the item. Mapping these values helps ensure that the metric values are reported consistently, regardless of the vendor. Different vendor certifications can associate with the same metric family. If multiple vendor certifications apply to a metric family, Data Aggregator maps metric values using a ranked list of vendor certifications. Therefore, Data Aggregator calculates a metric value using the highest priority vendor certification that matches the polled item.

view

Views, or *data views*, present statistical data, usually in a graph or table format. Each view represents a discrete set of collected data. Depending on your user account role rights, you can add and edit individual views or remove them from a dashboard page. In some cases, you can export the data to a file in CSV format.