CA Spectrum®

Deployment Capacity and Optimization Best Practices Guide

Release 9.4

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: Capacity and Optimization for CA Spectrum

This section contains the following topics:

Introduction

Welcome to CA Spectrum. You are using one of the most powerful tools available to monitor your network infrastructure. As always, with power comes responsibility. Like a Formula One race car, CA Spectrum is a highly capable system. However, both the race car and the software are highly susceptible to their operating environment and to the control of their human drivers. Just as a rain-soaked track can end a race, a lack of system resources or an over-subscribed system workload can sideline CA Spectrum.

In this guide, we have captured the best practices and advice to help you keep CA Spectrum performing at its highest levels. These best practices are derived from systematic, controlled performance testing, and from years of real-world experience supporting our global customer base.

In highly dynamic IT environments, monitoring the capacity of your systems and optimizing your CA Spectrum deployment cannot be a one-time task. Regular, periodic reviews are required to keep CA Spectrum operating optimally in larger environments (more than 1,000 monitored devices).

Prerequisites

To understand the advice that we offer in this guide, you must be familiar with CA Spectrum concepts, architecture, and terminology. Specifically, we recommend that any CA Spectrum administrator take the following CA Training courses:

- CA SPECTRUM r9.0: Operator 200 (02SPC20080) – self-paced training
- CA SPECTRUM r9.0: Foundations 200 (02SPC20091) – instructor-led
- CA SPECTRUM r9.0: Optimization & Customization 300 (02SPC30051) – instructor-led

In addition, we recommend reading the following documents:

- *Installation Guide*
- *Concepts Guide*
- *Operator Guide*
- *Administrator Guide*
- *Database Management Guide*
- *Distributed SpectroSERVER Administrator Guide*
- *Event Configuration User Guide*
- *Modeling and Managing your IT Infrastructure Administration Guide*
- *Report Manager Installation and Administration Guide*

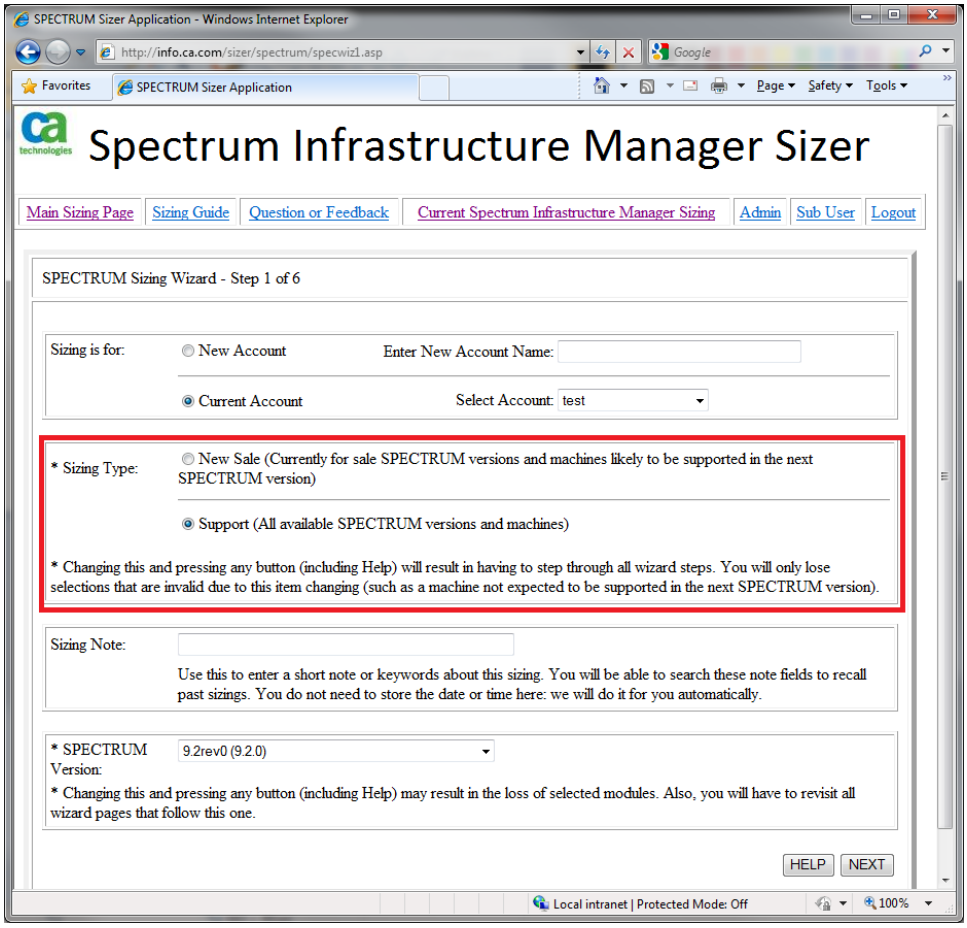
CA Spectrum administrators must be familiar with the CA Spectrum component documents for the various applications and integrations that are heavily used in their environment.

Note: This guide replaces the *SpectroSERVER Performance Administration Guide*.

Getting Started

The best place to start is to request a sizing estimate that is based on your deployment intentions or existing deployment. You can request a sizing estimate through your technical sales contact before the purchase, or through CA Support. CA Support must perform the most advanced and detailed sizing for an existing deployment. Many details that are needed for the Support type of sizing are not available when sizings are performed during the sales cycle. The Sizing estimation requires some key pieces of data to estimate the number of SpectroSERVERs required to manage your workload.

Note: The CA Spectrum sizing tool is no longer available for users and CA Partners. Open a request with CA Support when you require assistance with sizing a deployment.



Managing your environment with fewer than the recommended number of SpectroSERVERs risks instability or performance problems that affect a production deployment. Validate the system utilization metrics early and regularly in a production deployment. This validation ensures that the resource utilization predictions from the Sizer are accurate. Many features of CA Spectrum are not accounted for in the predictive model of the Sizer. The Sizer works from a steady state, without major faults, reconfigurations, or other sources of variability. Therefore, validation is an important activity post-deployment.

The sizing guidelines and best practices in this guide help CA Spectrum servers operate below the capacity of your system and operating environment. Do not consume your total capacity. The CA Spectrum workload is dynamic and can vary greatly based on usage patterns, periodic automated operations, or network outages. An optimally tuned CA Spectrum server does not exceed 40%of CPU capacity or 75% of process RAM or physical system total RAM. The spare capacity enables periodic workload increases.

Chapter 2: Operating Environment and Systems Setup

This section contains the following topics:

Environment: Areas of Focus

As with any memory-, CPU-, or disk-intensive, sophisticated application, CA Spectrum is susceptible to its operating environment. This environment breaks down broadly into the following categories:

- Hardware (see page 12)
- Virtualization (see page 13)
- Operating System (see page 14)
- Isolation (see page 14)

The processes that perform most of the work on the CA Spectrum servers are written for a 32-bit architecture. As a result, they are limited to total memory (RAM) access of no more than 4 GB (or lower, depending on the operating system configuration). Most processes also employ only limited native multi-threading. As a result, the operating system cannot spread the processing workload over multiple CPUs (or cores). However, the system does context-switch processes to any CPU that appears to have available time.

Hardware

The minimum hardware requirements for the major CA Spectrum components are described in the respective installation guides. For large deployments with relatively low-cost system hardware resources, you can minimize the potential of exhausting physical resource capacity. We recommend the following hardware for a heavily loaded CA Spectrum Component:

SpectroSERVER or OneClick Server

- Server-class, Intel-compatible or Sun hardware
- 4 CPUs or cores running at 2 GHz or higher processor speeds
- 8 GB of RAM, encompassing the following requirements:
  - 4 GB for major CA Spectrum processes
  - 2 GB for the OS
  - 2 GB for smaller CA Spectrum processes and other transient requirements
- Locally attached disk subsystem
- Hardware RAID (levels 1/0, 5, or 1 recommended, in that order)
- 50 GB of available disk space
- Physical disk using SAS or SCSI technology. We recommend 10,000 RPM minimum.

  For Fiber Channel, SAN, or other disk technologies, the performance characteristics of the locally attached disk subsystem recommendations must be met.

Spectrum Report Manager Server

The minimum hardware requirements for Spectrum Report Manager and SpectroSERVER or OneClick are the same, except for the available disk space. Given the historical data storage nature of Spectrum Report Manager, disk space is a major consideration. For more information, see Spectrum Report Manager (see page 32).

Virtualization

In a virtual environment, you can share resources to maximize your return on hardware investment. However, CA Spectrum reacts to network conditions in real time. As a result, the product requires CPU resources, memory resources, and disk speeds to be running at optimal capacity. If any one of these resources is affected because of another virtual machine, CA Spectrum performance is affected. Therefore, we recommend running CA Spectrum with CPU and memory resources that are dedicated 100 percent of the time. If you are using a storage area network, use the performance requirements that we recommend in the Hardware (see page 12) section.

Note: Do not run VMware VMotion on virtual machines (VMs) that are running CA Spectrum because CA Spectrum always requires dedicated resources. However, if you stop all CA Spectrum processes on VMs, you can run VMware VMotion on those VMs.

As a best practice for virtual machines that are used for CA Spectrum, dedicate system resources as specified in the Hardware (see page 12) section. For VMware environments, consider the following points:

- Ensure that required resources are always available (reserved). Assign dedicated resource groups to the CA Spectrum virtual machines regardless of the state of other VMs that are running on the same server. Make resource group allocations according to the sizing information from the CA Spectrum Sizing Tool and the recommendations in this document.
- Create specific RAID volumes or LUN with dedicated disks/spindles to the CA Spectrum system. These volumes help to avoid disk I/O contention with other applications that share the same RAID or storage array. Allocate large volumes of disks/spindles to the RAID volume or LUN. Larger volumes enable a greater I/O distribution and maximum read/write times for the CA Spectrum processes.
- The VMware administrator can reserve memory and CPU resources within Clusters or Resources Pools, rather than making reservations on individual VMs.
- On the SpectroSERVER hosts, lower CPU percent ready times were observed with two vCPUs than with four vCPUs. More vCPUs are not always better.
- Disk access times of more than 10 (ms) noticeably affected performance on a SpectroSERVER with a significant load.
- Do not allow the VM snapshots to continue for long periods of time. The delta implementation of snapshots can affect the SpectroSERVER performance.
- The VM HBA assignments can also affect SpectroSERVER performance.

Basic Configuration for VMware

Set the following values from the Hardware tab on the Edit Settings dialog:

- 2 vCPUs
- Configured memory: 8 GB (The guest operating system assumes this value as the available physical memory)

Additional Configuration for VMware

If a VM contention affects the ESX server, set the following values from the Resources tab on the Edit Settings dialog:

- Memory
  - Shares: High
  - Reservation: 2-4 GB (hardware-dependent; use with care)
  - Limit: Unlimited
- CPU
  - Shares: High
  - Reservation: 0 ((hardware-dependent; use with care)
  - Limit: Unlimited

Operating System

The individual CA Spectrum processes cannot use more than 4 GB of RAM. However, it is best to run CA Spectrum on 64-bit variants of supported operating systems. On 64-bit variants, processes can take advantage of 4 full GB of addressable RAM. Some 32-bit variants of supported operating systems actually limit individual processes to 2 or 3 GB.

Isolation

The ideal environment for the CA Spectrum servers is one in which they are not contending for resources with other processes. Moreover, avoid or thoroughly test some environments as they impact affect the performance of CA Spectrum. Such environments include Antivirus, Security software, and Backup utilities.

Also check for Automatic disk backups, operating-system backups, automatic antivirus scans, and network security scans, which affect the performance of CA Spectrum. These processes place temporary locks on files to which CA Spectrum needs constant access. Therefore, they can lead to crashes and performance issues. This guidance applies to any hardware or virtual machine where a SpectroSERVER, Archive Manager, or SRM database is deployed.

Perform automatic disk backups, operating-system backups, and operating-system updates only after gracefully shutting down all CA Spectrum processes.

Configure antivirus scans to skip the CA Spectrum root directory. If a scan of the CA Spectrum root directory is required, run it with all CA Spectrum processes gracefully stopped.

Chapter 3: Additional Considerations

This section contains the following topics:

Distributed Deployment Considerations

If you plan to deploy CA Spectrum in a large environment, start by understanding how CA Spectrum scales to manage larger environments. Scaling is achieved primarily by adding SpectroSERVER instances, spreading the workload by splitting the monitored infrastructure among these servers.

Network bandwidth and reliability can come into play with larger distributed deployments. In general, we advise you to place the SpectroSERVERs close (from a network-efficiency perspective) to the largest number of monitored devices. Place OneClick servers close to the most of the user community that will actively run the OneClick clients.

Substantial communication takes place between the OneClick servers and the SpectroSERVERs. Therefore, the available bandwidth and resiliency of the networks between them must be monitored closely. SpectroSERVERs also communicate with each other, but less frequently and less intensively. However, those network pathways must also be monitored closely to ensure resiliency.

Workload: Where to Focus Optimization Efforts

Workload is an important area of focus for your optimization efforts. The following list provides examples of CA Spectrum deployment variables that affect workload and are candidates for an optimization:

- The total number of models, numbers of models being polled and polling rates
- Searches (Global Collection search criteria, user-initiated searches, and condition correlations)
- Alarms (total active and rates – an impact on OneClick concurrent users)
- Events (logging and traps)
- Network device interfaces
- Auto-discoveries and trap-based discovery
- Managed network health
- Spectrum Report Manager

As you can see, this list is already fairly long, yet it highlights only the major aspects of workload. Many other dimensions of workload can also affect a CA Spectrum deployment, although typically to a lesser extent. For instance, the CA Spectrum documentation set covers more than 40 additional major features, integrations, and customization or integration toolkits. Many variables are involved. We cannot be exhaustively prescriptive about exactly how much of every capability, in every possible combination, will perform adequately in a given deployment.

Without being fully prescriptive, we can provide best-practice recommendations for keeping workloads within relatively safe tolerances. This type of workload balancing maintains the entire CA Spectrum environment at high performance levels.

The topics in this section provide guidance on best practices when confronted with a requirement to split workload across existing or new SpectroSERVERs.

Total Number of Models

The CA Spectrum Sizing tool can help you determine the total number of advisable models. Contact CA Support or your sales representative to request a sizing analysis. This analysis also helps you determine optimal polling rates.

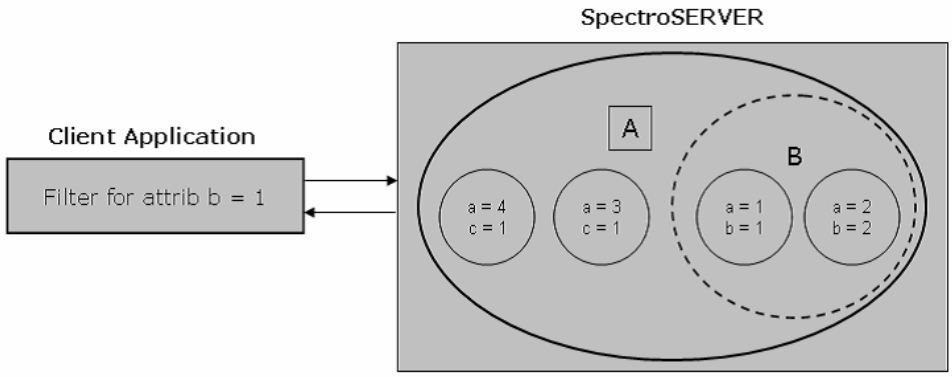
Searches

CA Spectrum offers powerful search capabilities. Searching for models can have an outsize impact on system performance. Such operations can consume significant system resources and can generate substantial I/O. The required resources depend on how searches are constructed and how often they occur.

Global Collection searches, custom OneClick searches, SANM, Southbound Gateway, and versions of Policy Manager earlier than 9.2.1 are some of the CA Spectrum features that rely on search operations. Before you use a search, verify whether that search is essential. For example, Global Collections can be constructed manually; as a result, searches are not required if a collection is small. In that case, a better option can be to use the Favorites feature of OneClick rather than a global collection.

When constructing a new search, spend some time to determine whether any internal attributes exist exclusively on the desired models. If two or more attributes are needed in the search, which ones must be used first?

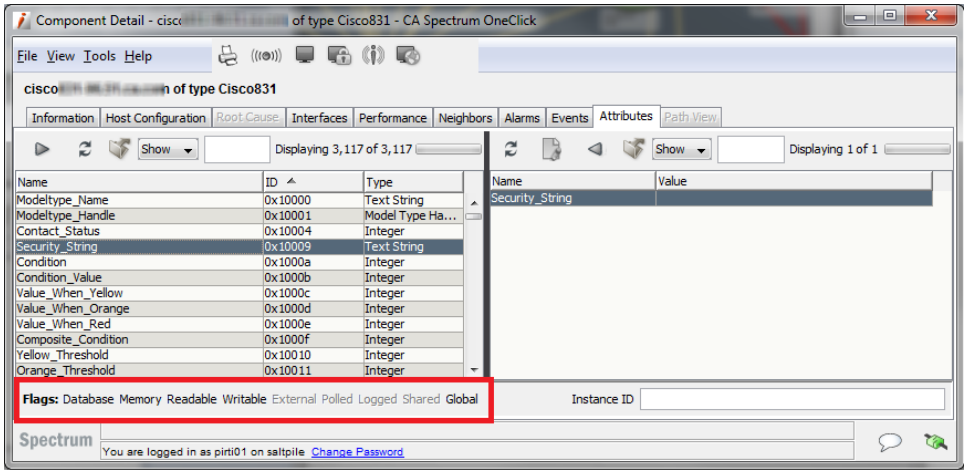
The following diagram describes how attributes group models. All models with Attribute "A" are depicted by the large oval. All models with Attribute "B" are shown as a circle. To limit the number of models that are searched, select the attribute “B” over “A” as a first criterion. As a result, the search is optimized.



After narrowing search expression results based on attributes, consider attribute flags and data types.

The attribute flags provide an indication of the time that is required to retrieve or access the information from a model. They are therefore an important aspect of optimization. A memory attribute has the fastest access times, followed by database attributes, calculated attributes, and, finally, external attributes. The calculated attributes are typically attributes whose values are determined on demand. And the slowest type of attribute for purposes of searching is the external type. Extra time is required to contact multiple devices over the network and wait for them to respond.

Attribute flags and data types can be viewed from the Attributes tab of the Component Detail panel in OneClick:



The following list places attribute storage flags in order from least CPU-intensive with quickest access to most CPU-intensive and slowest access:

a. Memory Flag

b. Database Flag

c. Calculated

d. External Flag

Data Types for comparison also require consideration. The following list places attribute data types in order from quickest comparison to slowest comparison:

a. Integer, Counter, Enumeration, Model Type Handle

b. IP Address, Octet String

c. Text String

The following lists place overall attribute flags and data types for complex searches of AND/OR in order from the most efficient to the least efficient:

Memory Flag

a. Integer, Counter, Enumeration, Model Type Handle

b. IP Address, Octet String

c. Text String

Database Flag

a. Integer , Counter, Enumeration, Model Type Handle
b. IP Address, Octet String
c. Text String

Calculated Attribute

a. Integer, Counter, Enumeration, Model Type Handle
b. IP Address, Octet String
c. Text String

External Flag

a. Integer, Counter, Enumeration, Model Type Handle
b. IP Address, Octet String
c. Text String

Example Search

A Global Collection search contains, in no particular order, ifDesc, Topology Model Name String, Network Address, and Model Type Handle. From top to bottom, the search should include the following items for best performance:

a. Model Type Handle - Memory : Handle
b. Network Address - Memory / Database : IP Address
c. Topology Model Name string - String : Calculated
d. ifDesc - String : External

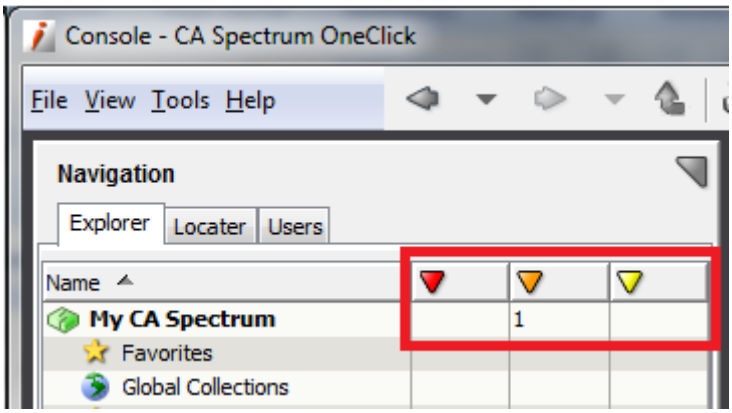
Users typically deploy the search feature in a Global Collection. After you create a Global Collection, the SpectroSERVER immediately performs the search. If a SpectroSERVER determines that the search calls for excessive processing for a long time, a minor alarm (0x10f21) appears on the GlobalCollection model. When you see this alarm, review and optimize the search expression according to the information that we provided here.

Alarms

Two aspects of alarm management in CA Spectrum can have undesired effects on the performance of the SpectroSERVER and OneClick service:

- **Outstanding alarms**, the aggregate number of outstanding (or active) alarms that appear in the OneClick client from a standalone or distributed SpectroSERVER environment.

  This value can be easily determined from the OneClick client. In the Navigation panel Explorer tab, check the columns for **My CA Spectrum**, as shown in the following image. Verify that no alarm filters are applied to this view to see an accurate total count.

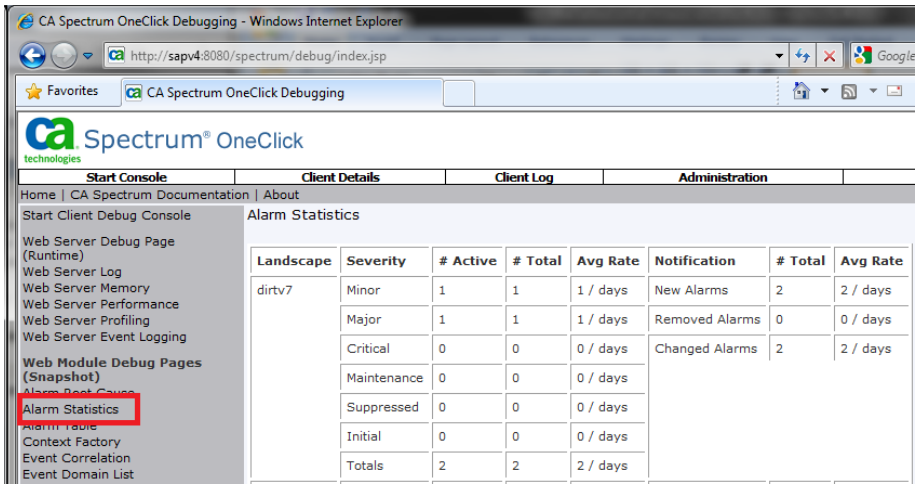


  Outstanding or active alarms consume memory in the OneClick server at a rate of roughly 10 through 20 Megabytes of RAM for every 4000 alarms. However, another capacity concern arises when the SpectroSERVER is starting up or failing over. The OneClick server needs CPU time to load the alarms and distribute them to the active OneClick clients. During this time period, excessive outstanding alarm counts can cause OneClick clients to perform sluggishly or even to disconnect.

  Therefore, we recommend always keeping alarm counts as low as possible. Approximately 4000 total outstanding or active alarms is a recommended maximum as a preventative measure to stay within the best-practice tolerance.

- **Alarm rate**, the number of alarms that are generated or cleared per second.

  Sometimes the alarm rate is not apparent. When an alarm is generated and then is cleared shortly afterward, the alarm information is not immediately updated in the OneClick client view. Use the Alarm Statistics in the Client Debug Console to review the alarm rate from the OneClick Administration page.



Alarm Process Flow

Every alarm that is generated, updated, or cleared follows the same process flow, which is illustrated in the following diagram:

As shown in the diagram, the alarm information comes in from the SpectroSERVER process. The OneClick service takes these alarms and processes them according to the alarm filter that you configure in the user preferences of each active client. As a result, the OneClick service can incur performance issues. Factors that affect performance include the complexity of the client alarm filter, number of active OneClick clients, and the alarm rate.

As the number of active clients with alarm filters increases, CPU and memory utilization also increase under different alarm rate loads. As a best practice, keep sustained alarm rates below five per second. Alarm bursts at 200 per second can cause temporary spikes in CPU usage.

Assume that the OneClickserver is at capacity with 20 concurrent active clients in an environment with a high alarm count and high alarm rate. The number of concurrent OneClick clients can reach 50 per OneClick server, if the active alarm count is below or 1000 and the alarm rate is below five per second. If higher numbers of concurrent OneClick clients are required, multiple OneClick servers are required to distribute the client load. However, do not exceed the best-practice limit of four OneClick servers that are connected to a single SpectroSERVER.

The following chart shows an example of the CPU and memory requirements that are associated with alarms:

CPU for OC Process (Percent CPU)							
	Base Alarms	4000	4000	4000	4000	4000	4000
	Alarm Rate (Alarms / sec)	0	20	50	100	150	200
Active OC Clients	10	0		8	33	51	70
	20			27	60	90	
	30		20	56			
Memory After Test After Garbage Collection (MB)							
	Base Alarms	4000	4000	4000	4000	4000	4000
	Alarm Rate (Alarms / sec)	0	20	50	100	150	200
Active OC Clients	10	379		379	379	379	379
	20	586		564	564	457	
	30	803	805	805			

Be sure to review the Events section for help in determining the source of high alarm rates.

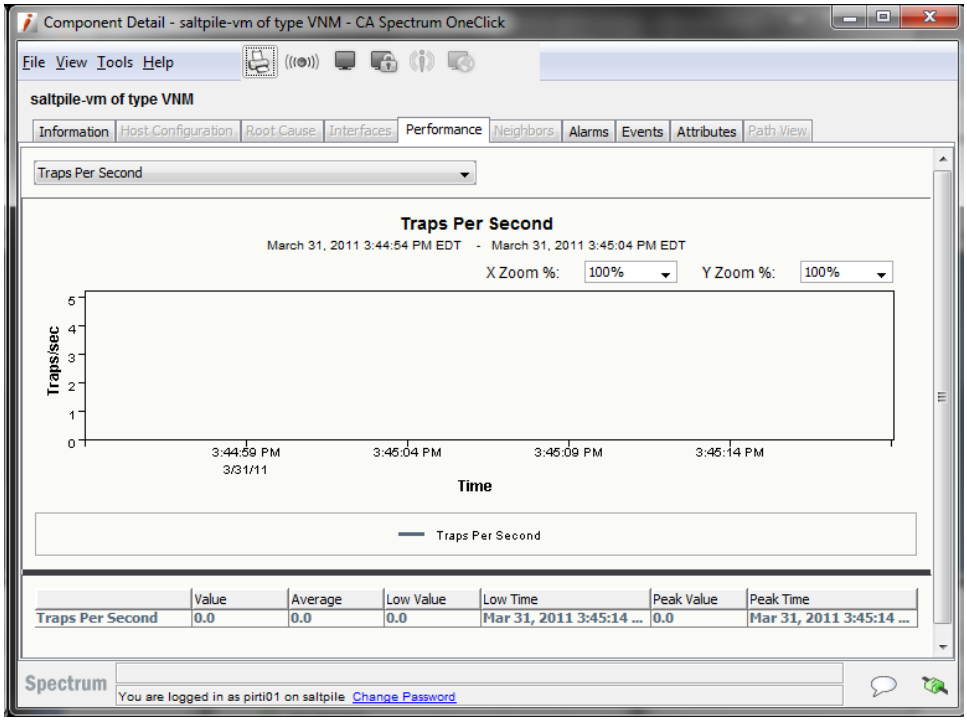
Events

Events can have a major impact on SpectroSERVER performance and can increase the size of the Archive Manager and SRM databases. Events are generated from external sources, such as an SNMP trap from a network device or log file monitoring, or from internal conditions.

In most cases, when the SpectroSERVER process becomes excessively busy, we recommend verifying that event rates are not excessive. SNMP traps are usually the reason for excessive event rates. One indication that the SpectroSERVER process is experiencing high trap rates is an alarm on the VNM model. Starting with CA Spectrum 9.2, a critical alarm is generated when the SNMP trap rates exceed 100 traps per second for 5 minutes. The probable cause code of the alarm is 0x10f94.

Pay attention to trap rates and to the high trap rate alarm. A burst of traps for a certain time consumes CPU. For a rate of 100 traps per second, the SpectroSERVER process incurs 3% - 4% of CPU time to process those traps. For example, if the SpectroSERVER receives traps at 250 traps per second, 7.5% - 10% of CPU time is required to process these traps.

Another, more familiar, indicator is a trap storm alarm (0x10253) on the VNM or device model. The SpectroSERVER VNM model provides trap rate performance data. Access this information from the VNM Performance tab:



You can also determine the type of a trap or event from Log Monitoring by using SQL queries. Using the following steps, you can determine the trap type and source of the events and traps.

Follow these steps:

1. Log in to the MySQL database.
2. Run the following query to report the event counts by type for a given time range:

   SELECT hex(type), hex(node_id), count(*) as c from ddmdb.event where utime > UNIX_TIMESTAMP('2010-08-20 00:00:00') and utime < UNIX_TIMESTAMP('2010-08-21 00:00:00') group by type order by c desc;

   Note: The times that are provided here are examples. Replace the dates with the actual time ranges. Keep in mind that SQL queries can take a significant amount of time to complete.

3. From the report of event counts that is returned, determine the event type that is increasing the most over time.
4. For that event type (0x1030a in the following example), run the following command to see which model is seeing the event generated

   ```
   SELECT hex(model_h), count(*) as c from ddmdb.event where utime > UNIX_TIMESTAMP('2008-11-12 00:00:00') and utime < UNIX_TIMESTAMP('2008-11-12 09:00:00')and type=0x1030a group by hex(model_h) order by c desc;
   ```

5. From the breakdown of events for a given model, determine the source of the events from the network address of the model.

Also take constant event rates into consideration. Record the total number of events per day. If a SpectroSERVER shows 11 traps per second, what initially appears to be a low rate equates to approximately 1,000,000 events per day. This number of events can have a serious impact on processing and the database space requirements of the Archive Manager and Spectrum Report Manager.

The steps that were outlined earlier can help you to determine whether any heavy event producers can be addressed. But also consider unmapping high-volume trap events that provide no management value.

Network Device Interfaces

Device interfaces are involved in two aspects of performance considerations.

ifTable Entries

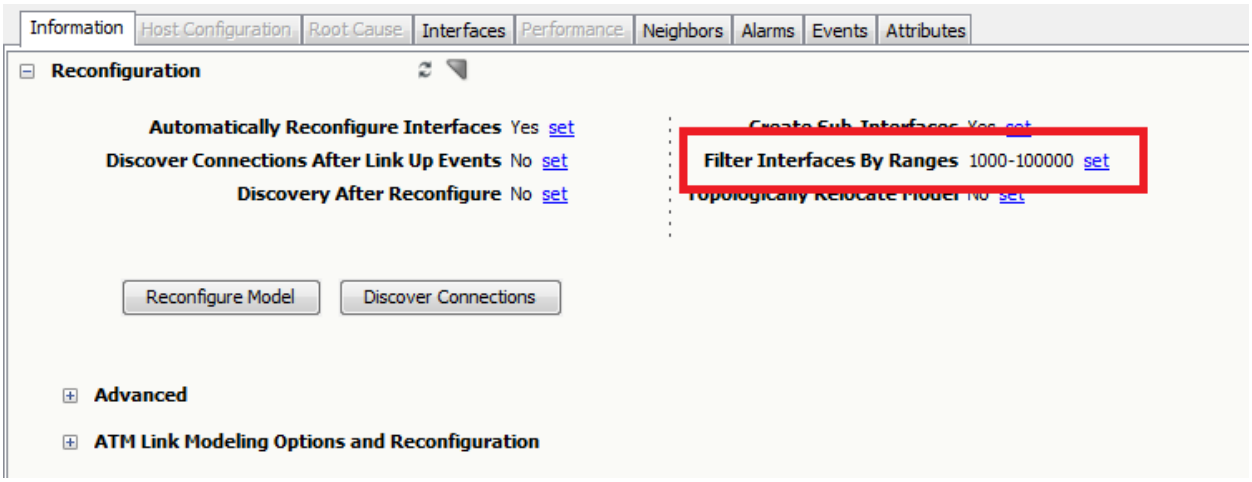
By default, the SpectroSERVER process models all interfaces in the MIB 2 ifTable, all Frame relay DLCI interfaces from RFC1315 and RFC2115, and all ATM VCL interfaces from RFC2515.

In the ifTable, it is common to find virtual technologies including VoIP calls and virtual routing interfaces. As a result, you must review the number of entries in the ifTable when you model a device for the first time. Large quantities of entries (in the thousands or tens of thousands) can have an impact on SpectroSERVER performance.

Reconfiguration Operations

Typically, the more interfaces on a device, the longer the interface reconfiguration operation takes. When devices have 1000 or more physical or logical interfaces, reconfiguration operations can take minutes to complete. This process adds a minimum of 6 - 8 percent CPU time and increases traffic levels on the network.

When some interfaces are not required for effective monitoring, filtering capabilities are available to speed up the process. An example is shown in the following image from the OneClick Component Details Information tab:



Other methods of filtering interfaces are more complex. Consult with CA Support before proceeding with complex interface filtering. Or, try one of the following options:

- Selectively disable the automatic reconfiguration if the interfaces are fairly stable, with few changes.
- Model the device as a Pingable model. You thus gain the device status information and do not gather status data from the individual interfaces.

The frequency of interface reconfigurations for a device can affect the performance. At every poll interval, the device model reads both the ifTableLastChange and ifStackLastChange MIB objects. The ifTableLastChange is a timestamp that indicates when the interface table added or removed interfaces. The ifStackLastChange is a timestamp that indicates when the order of interface stacking last changed. If neither attribute is supported, ifNumber (the ifTable interface count) is monitored for changes. If the value of any of these MIB objects change, automatic reconfiguration starts by default.

Problems can occur when CA Spectrum monitors a VoIP router. Such routers from some vendors constantly change the interface stacking order as VoIP calls are made and then closed. At every poll cycle, CA Spectrum sees a change in the stack timestamp and reconfigures. In this case, CA Spectrum incurs an unnecessary workload with the extra overhead of the reconfiguration and interface table reads. This situation can also have implications for configured product integrations, such as CA eHealth. Updates to the eHealth side can be triggered, based on the reconfigurations occurring in CA Spectrum.

The Spectrum Event Rate Window rule identifies reconfiguration issues and raises attention to CA Spectrum operators. The rule, which is in place by default, states that if a device experiences 6 interface reconfiguration events 0x1001d in 31 minutes, an alarm of type 0x10050 is generated on the device. Review the event log for the affected device and filter for Event Type 0x1001d. Each event of that type identifies the cause of the interface reconfiguration.

Cause Indicator	Description
Interface-Stack-Change-Reconfiguration	The reconfiguration was caused by a change in the stacking order of the interfaces. MIB object ifStackLastChange has changed in value. If this object changes every polling cycle, then we recommend that you turn off Use_If_Stack_Last_Change. Attribute Use_If_Stack_Last_Change 0x000130bc can be set to false to disable this trigger
Interface-Table-Change-Reconfiguration	The reconfiguration was caused by the creation or deletion of an interface in the table. MIB object ifTableLastChange has changed in value. If this object changes every poll cycle, we recommend that you turn off Use_If_Table_Last_Change. Attribute Use_If_Table_Last_Change 0x00011f7f can be set to false to disable this trigger.
Interface-Count-Change-Reconfiguration	The reconfiguration was caused by a change in the number of interfaces in the table. MIB object ifNumber has changed in value. If this object changes evey poll cycle, we recommend that interface reconfiguration be turned off. Attribute If_IsAutoCnfgActive 0x00011dd4 can be set to false to disable automatic interface reconfiguration.
SNMP-Contact-To-Device-Re-established	Review the event log for the device to see whether the device model has lost and regained contact. In such a situation, you may have a network problem.

Discovery

Questions often arise from CA Spectrum customers about Discovery and associated performance issues. The most important consideration for Discovery is knowledge of the network that you are discovering. How many devices does it contain? What types of devices compose the network, such as switches, routers, and hosts? And what are the port densities of these network devices?

The answers to these questions often have an impact on Discovery. They also affect the decision whether the entire network can be modeled on one SpectroSERVER, or whether multiple SpectroSERVER are required.

Important! Do not discover or model the entire network at once, if you have not performed these activities before.

The best practice for first-time discoveries is to run a scan of the devices in a particular address range to understand what devices are present. We recommend starting with a Class B address range, or smaller. Then model sections of the network one at a time, paying attention to the memory consumption of the SpectroSERVER process. Use a tool such as the CA Spectrum Performance View to monitor the memory usage. Keep in mind the recommendations for memory capacity that we discussed in Alarms (see page 22) and other topics.

Try to distribute the CPU workload as much as possible. The following table provides some recommended numbers, but pay attention to the port densities, which affect the batch count. Review the network for any devices with excessive ifNumber counts. Counts of 1000 ports or more add significant time to the Discovery process. We recommend discovering these devices one at a time.

Items Discovered	Size of Batch to Discover
Switches / Routers with 100 ports each	250 Devices
GnSNMPDev with 40 ports	500 Devices
Hosts with 2 ports	250 Devices
Pingables	1000 Devices

Technologies such as VLAN, MPLS, VPN, VRRP/HSRP, Multicast, and Virtual Host Management are other optional Discovery types. For each technology, the numbers that are provided in the following table are a guide for strategic planning for Discovery before initiating it. The following table summarizes the recommended totals:

Technology	Large Deployments	Predeployment Recommendations
MPLS VPN	1000 or more VPNs, 10000 or more sites	Use hub and spoke VRF testing back to the corporate network. Do not use full mesh.
MPLS VPLS	1000 or more VFIs, 10000 or sites	Use hub and spoke testing back to the corporate network. Do not use full mesh.
MPLS TE	1000 or more LSPs	Separate logically by location or use some other partitioning method on different SpectroSERVERs to distribute load.
Multicast	1000 or more groups	Separate logically by location or use some other partitioning method on different SpectroSERVERs to distribute load.
Enterprise VPN	1000 or more sites	Use hub and spoke IP SLA testing back to corporate. Do not use full mesh.
QoS	Policies, map classes, behaviors, with 1000 or more interfaces	Set poll interval to 300 seconds or longer.
VRRP/HSRP	20 or more groups	Do not use active polling, use trap-based passive notification.
VLANs	50 VLANs or more with VLAN overlay enabled	Separate logically by location or use some other partitioning method on different SpectroSERVERs to distribute load.
Virtual Hosts	1000 or more VHM	Separate logically by data center or by some other partitioning method. For more information, see the *Virtual Host Management Guide*.

Operators sometimes enable trap-based discovery as a means of discovering new devices as they come online, which is how the feature was designed. However, if using this feature (which is disabled by default), it is important to know the frequency of new device additions. Failure to understand this metric can cause a SpectroSERVER crash due to memory exhaustion. When using this feature, review the rate of unmanaged traps per day to understand how many new devices are likely to be modeled.

When CA Spectrum processes a trap for the first time but the IP address is not modeled, an unmanaged trap event is generated on the VNM model. Use these traps to calculate the approximate rate of devices additions per day.

Managed Network Health

Network health affects business services and also can affect CA Spectrum, which monitors network health for business services. With increased focus on the health of business services, we sometimes overlook chronic network health issues that do not appear to impact business. To monitor business services and resolve faults down to the network layer, any infrastructure management strategy must monitor and react-to constant change. Chronic network health issues can increase the amount of change and the resulting work for CA Spectrum by an order of magnitude.

Consider the case where a single link on a core router is going down and coming back up several times each minute, a condition known as "flapping". In this case, CA Spectrum receives a link-down and link-up trap and will also poll the interface for status each time the link flaps. In addition, this flapping link can result in a temporary loss of contact with many of the devices in the network behind it. The result can be more polling and fault-isolation overhead as CA Spectrum works to determine the state of the devices in this network. However, this single case is not an issue, as far as CA Spectrum capacity is concerned.

But imagine a second scenario in which several core routers and switches each have multiple "flapping" interfaces. The effect of thousands of link-down/link-up traps, subsequent polling, and fault-isolation overhead in this example could result in a high and continuous CA Spectrum workload. The increased workload can include tens of thousands of alarms being generated and cleared continually.

Generally and in the earlier two cases, CA Spectrum provides the data in terms of events and alarms to locate and resolve network health issues. CA Spectrum operators must pay attention to network health issues and must take steps to resolve them, or tune CA Spectrum to mitigate their impact. In the earlier examples, resolving the flapping interface problem is the solution. When the connectivity between CA Spectrum and the managed devices is generally unreliable, or if devices are slow to respond, verify your polling timeout thresholds and retry thresholds. Failure to do so can result in large numbers of "false" alerts due to failed polls, which increase fault isolation overhead.

Finally, connectivity among CA Spectrum components (SpectroSERVERs and OneClick servers) is an important consideration. Everything from basic server-to-server communications to cross-server searches relies on the network connectivity. Therefore, reliable communications among servers are critical for CA Spectrum performance.

Spectrum Report Manager (SRM)

Most of the advice that we have provided thus far has focused on the major real-time aspects of a CA Spectrum deployment. Many customers have come to rely also on Spectrum Report Manager for historical data collection, analysis, and reporting. Report Manager includes a separate database that archives data from all connected SpectroSERVERs. Therefore, pay particular attention to the disk capacity and disk I/O performance of the system. Tuning can be required, depending on the amount of data being stored, the opportunities for filtering unnecessary data, and the size of the report.

A best-practice recommendation is to determine the total database size that is required to store event history, and then allocate twice the space on that disk partition to accommodate transient space requirements. The topic titled Spectrum Report Manager Sizing Guidance (see page 33) provides advice and formulas to help you calculate disk space requirements.

The following considerations are also important for Spectrum Report Manager performance and capacity:

- Consider the volume of the data and system resources for the Report Manager performance. Running reports from a smaller volume minimizes report generation failure especially for event and alarm reports. Smaller volume of data decreases the response time of the database query.
- When the result set is large, or when a large amount of data is sorted or grouped, the database writes the results to disk. This activity affects the Report Manager performance.
- If your environment generates a high volume of events without generating event reports, consider purging the event table periodically. Purging this table saves space on the reporting DB system.

- If you generate event reports on a specific set of events, consider purging the event types that you do not require. Or, if selected event types are not required to produce alarm, asset, availability, or other reports, consider filtering these events before they reach the reporting database. For more information, see the *Spectrum Report Manager Installation and AdministratorGuide*.
- If your environment generates a large volume of events on models that you do not include in reports, consider filtering these events from the reporting database. The *Spectrum Report Manager Installation and Administrator Guide* contains more information.
- Some of the filtering mechanisms on the reports themselves can cause performance issues. We are still researching this possibility, but we have seen anecdotal evidence that alarm and event filters, when used on reports, degrade the performance. Where possible, try to limit their use.
- CA Support maintains some best-practice recommendations for the CA Business Intelligence (CABI) component that Spectrum Report Manager uses for reporting capabilities. These considerations also apply to any CA product that uses CABI. Contact CA Support for more information.

Spectrum Report Manager Sizing Guidance

The following formula can help you estimate the amount of disk space that is likely to be required to support the Reporting database for a user-specified amount of time.

The total number of required disk spaces in GB equals:

```
((# of devices) * (avg # of events per device per day) * (# of days
of storage desired) * (avg size of event in KB)) / 1048576
```

# of devices

Environment-specific value. Consider future growth when specifying this value.

avg # of events per device per day

Represents the total number of events that are (1) generated daily and (2) are associated with the creation of a single device model. This total includes all events that result from related application, port, and interface models. The easiest way to approximate this number is to look at the total number of events that were generated on one SpectroSERVER in a day. Divide that total by the number of devices that are modeled on that SpectroSERVER.

# of days of storage required

Environment-specific value.

avg size of events, in KB

An estimation of the amount of disk space a single event consumes in the Reporting database. This value is measured in KB.

1048576

The product of the earlier equation is divided by this number to get a measurement in GB.

You probably have an idea of the number of devices and the number of days of storage that you want. Only two variables are then required in the calculation:

Average number of events, per device, per day

Environment-specific value. You can query the DDMDB to see the average number of events that are generated on a given day.

If you are a new CA Spectrum user, or if you are unsure how to determine the average number of events, use a reasonable default value. Consider that 300 events per day, per device, for 500 devices equate to 150,000 events per day. A default value of 300 is a good starting-point.

To get an idea of the average daily number of events that are generated per device, find out how many events are generated daily. The following query returns the total event count for the last ten days:

```
SELECT date(from_unixtime(utime)) as x, count(*) as cnt
    FROM event GROUP BY x
    ORDER BY x DESC LIMIT 10;
```

The following query returns the days and event volume for the busiest ten days:

```
SELECT date(from_unixtime(utime)) as x, count(*) as cnt
    FROM event GROUP BY x
    ORDER BY cnt DESC LIMIT 10;
```

Use the results of these queries to devise a reasonable event count. Once you know the event count, divide that number by the total number of devices that are modeled on that server. The result is the average event count per device, per day.

Average size of events in the Reporting database (KB)

We recommend 1 KB as an appropriate amount of space to store your average event and the corresponding records. This number can obviously rise if most events are large–containing large amounts of data. The types of events also affect data size. Alarm events turn into multiple Reporting table records. NCM events only affect a single table (event). But for purposes of generalizing the behavior, 1 KB seems to be an appropriate measure.

Sizing Guidance Examples

Here are a couple of examples that illustrate useful calculations of the required storage capacity:

- **Example A**. Your environment contains 600 devices, and you want to retain data for 4 years (1460 days).

  Note: You do not know how many events are generated per device, so we default to 300.

  The total data in GB that must be stored equals:

  ```
  (600 * 300 * 1460 * 1) / 1,048,576 =
  262,800,000 / 1,048,576 =
  250 GB
  ```

- **Example B**. You have 1900 devices across three servers, and you want to retain data for 2 years (730 days). Your deployment seems to be averaging 400 events per device, per day.

  Note: In this example, we ignore the fact that you have three servers.

  The total data in GB that must be stored equals:

  ```
  (1900 * 400 * 730 * 1) / 1,048,576 =
  554,800,000 / 1,048,576 =
  530 GB
  ```

Sharing Monitoring Workload among SpectroSERVERs

When one or more of your SpectroSERVERs is oversubscribed, balance the workload or split it among additional SpectroSERVERs. Depending on the size, complexity, and scope of CA Spectrum feature use, and on the number of users, this project can require careful planning and execution. Careful planning can minimize production impacts and can ensure that the results achieve your objectives and have a good life span.

Many users find that they can benefit greatly from the help of CA Services or of our partner network at this stage.

Further discussion of this complex topic is beyond the scope of this document. We plan to leverage the information that we gather from our active Infrastructure Management User Community to make further updates to this topic in future releases of CA Spectrum. We recommend searching the message boards for information that is related to a workload optimization.