Monitor Extreme Management Center Server Health

The following sections provide detailed information on how to use specific Extreme Management Center reports and Extreme Management Center features to monitor your Extreme Management Center Server's health. These reports provide you with the information you need to monitor, analyze, and troubleshoot Extreme Management Center server problems.

- <u>Track Extreme Management Center Server CPU/Memory Trends</u>
- Monitor Extreme Management Center Server Disk Access
- Monitor Server and Database Connectivity

Track Extreme Management Center Server CPU/Memory Trends

The Extreme Management Center report on Extreme Management Center Server CPU/Memory utilization provides trending information on server performance over a period of time. Use this information to establish a baseline and identify changes in the system.

Knowing the system's normal operating behavior makes it easier to identify when the server's behavior deviates from the norm and when exactly the change occurred. It also makes it easier to identify whether the deviation corresponds to a recent change on the system or network.

If a change in CPU/memory usage is identified, real-time CPU and memory data can be used to further investigate which specific processes are consuming system resources. For more information, see the <u>Extreme Management Center</u> <u>Server Real-Time CPU and Memory Usage</u> section under Extreme Management Center Troubleshooting.

To access the Extreme Management Center Server CPU/Memory report, launch Extreme Management Center and select the **Reports** tab. Expand the Server folder and select the report, as shown below.



Extreme Management Center Server CPU/Memory

Monitor Extreme Management Center Server Disk Access

The Extreme Management Center Server Disk Access report provides information about disk activity levels on the server. Consistently heavy disk activity causes server performance issues and requires further investigation. Use this report to track read and write operations for both the Extreme Management Center server and the mySQL database.

To access the Extreme Management Center Server Disk Access report, launch Extreme Management Center and select the **Reports** tab. Expand the Server folder and select the report, as shown below.



Extreme Management Center Server Disk Access Report

Monitor Server and Database Connectivity

The Extreme Management Center server has a built-in mechanism that issues an alert in the event the server is unable to communicate with the database. This alert can be configured to trigger an email notification to be sent to a defined email address, so that network administrators can be alerted to the problem in a timely manner.

It is important to configure this email notification, because the Extreme Management Center server is central for monitoring, alerting, and diagnosing problems that may arise on the network.

NOTE: In the event communication between the server and database is lost, refer to the Extreme Management Center server.log (see <u>Accessing the Server Log File</u>) for troubleshooting information, as well as other troubleshooting tools that diagnose server CPU, memory, and current disk utilization (see <u>Extreme Management Center Troubleshooting</u> for more information). Use the Extreme Management Center Suite options to configure the email notification. From any Extreme Management Center application, select Tools > Options from the menu bar. Expand the Suite Options folder and select Extreme Management Center Server Health. Select the **Send email** checkbox and enter an email address that will be notified in the event of a database failure.

Extreme Management Center Server Health Options



Performance Tuning

The following sections provide detailed information on how to use specific Extreme Management Center tools and features to monitor and improve Extreme Management Center server performance.

- Tuning NetFlow Collection Settings
- Server Database and Memory Tuning
 - Changing the MySQL my.ini File
 - Increasing JBoss Memory
- Tuning Database Backup Storage
- Binding the Server to One Interface

Tuning NetFlow Collection Settings

NetFlow is a data collection protocol that provides details and analysis of protocol information derived from monitoring flow-based traffic as it traverses a network. K-Series, S-Series, and N-Series devices support NetFlow flow collection. The Extreme Management Center server can be configured as a flow collector for the devices on your network using the Flow Sensor Configuration window in Console.

Enabling NetFlow collection on your network can add significant overhead to Extreme Management Center server operation. Incoming flow data collection consumes a large portion of server memory and impacts the overall disk utilization footprint of the Extreme Management Center server. It can also lead to extended time required to perform an Extreme Management Center server backup, if reporting data is included in the backup.

In addition, name resolution for NetFlow traffic displayed in Extreme Management Center adds overhead to the server. NetFlow traffic bursts can lead to a spike in name resolution traffic which also adds to the overall load on the network.

You can adjust NetFlow collection settings using Extreme Management Center options. From the Console menu bar, select Tools > Options to open the Console Options window. Expand the Console folder and select NetFlow Collection. The

NetFlow Collection options are displayed. Click the Advanced Settings button to open the NetFlow Collection Advanced Settings window.

For most implementations, the default settings are recommended. However, in some cases, these settings can be adjusted to improve Extreme Management Center server performance. For example, you can change the maximum number of flows and aggregate flows to maintain in memory. Changing this number would adjust the amount of memory used to store flows.

You can also disable host and port name resolution for NetFlow. Disabling name resolution would affect the display of Extreme Management Center data because IP addresses would not be resolved to names. Other than that, the Extreme Management Center data is not impacted. Disabling name resolution would also reduce the DNS traffic on the network and to the DNS server(s).

The Advanced settings for the NetFlow flow collection let you limit resources used by Extreme Management Center Flow Alarm handling.

NOTE: Perform any change in the default flow collection parameters with caution and make adjustments taking into account items such as the size of the network and features enabled in Extreme Management Center. Advise all Extreme Management Center users of changes to the default flow collection parameters so that they can monitor any changes in server performance.

NetFlow Collection Options

NetSight Console Options		
Carlo Suite Options	NetFlow Collection	
Advanced SNMP Settings	NetFlow Settings	
Advanced Suite Settings	-	
Alarm Configuration	Enable NetFlow Collector:	✓
Gient Connections	Maximum Flows To Maintain In Memory:	30000
Database Backup	(· · · · · · · · · · · · · · · · · · ·	
Oata Display Format	Maximum Aggregate Flows To Maintain In Memory:	50000
Oate/Time Format	Maximum Number Of Flows Allowed Per Table View:	1000
Diagnostic Configuration	Send/Receive NetFlow Data On Socket:	2055
ExtremeNetworks.com Update		
MAC OUI Vendor List	Export Interval (minutes):	1
NetSight Feedback Program	NetFlow v9 Template Refresh Rate (packets):	30
• NetSight Server Health		1
• Port Monitor	NetFlow v9 Template Timeout (minutes):	<u> </u>
Services for NetSight Server	NetFlow Host Name Resolution:	
SMTP E-Mail Server	Med Flags Dark Marco Report diary	
Status Poling	NetFlow Port Name Resolution:	
System Browser Tree		
Web Server	Advanced Settings	
Console		
Oevice Manager	Charles and the start	
Discover	NetFlow Collection Advanced Settings	×
FlexView	-NetFlow Collection Advanced Settings	
Vielcome View Property View	-NetFlow Settings	
Compass		
VLAN View		
Basic Policy View	NetFlow Socket Data Size (Bytes): 2048	
VVreless Manager	NetFlow Socket Buffer (Bytes): 51200	
Topology Manager		
Policy Control Console RoamAbout Wireless Manager	NetFlow Socket Receive Queue Size: 2000	
TopN Collector	Flow Collector Filter (Warning: Changing updates current Flows to match):	
NetFlow Collection		
OneView	NetFlow Alarm Dispetcher Options	
OneView Collector	Flow Alarm Queue Service Period (seconds):	5
OneView Engine		
ACL Manager	Max Flow Alarms Serviced each Period:	100
	Max Flow Alarm Queue Size:	1000
		Restore Defaults
	OK .	Cancel Help

Server Memory Tuning

The Extreme Management Center software requires a significant amount of system resources. It is intended to run on a dedicated system where it does not compete with other software for system resources. Upon installation, Extreme Management Center detects whether the system has the minimum memory required to run correctly. It will then scale its memory usage to take advantage of the available system memory. It should not be necessary to manually adjust memory usage. If you suspect that you are experiencing performance issues related memory usage, please contact <u>Global Technical Assistance Center</u> (<u>GTAC</u>).

Tuning Database Backup Storage

The Extreme Management Center Server can be configured to run an automated backup on the day(s) of the week and time of your choosing. An up-to-date database backup is an important component to ensuring that critical information pertaining to all Extreme Management Center applications is saved and readily available, if needed.

However, while scheduling regular server backups is a best practice, it can lead to unintended side-effects in some environments. For example, backing up multiple copies of the database consumes disk space on the server. Ensuring there is plenty of free space prior to enabling this feature as well as checking the overall size of each backup is helpful in determining whether space issues may become a problem. (See Extreme Management Center Server Disk Utilization for more information.)

Another option is to save backups to a separate location such as a network share. It is important to verify periodically that the backups are running as expected and actually completing. You might also schedule quarterly database restores on a lab server to ensure the integrity of the backups.

In addition, the size of the database backup should be checked after major changes to the environment, for instance enabling Extreme Management Center data collection or implementing ExtremeControl on the network. If there are concerns regarding the available disk space, place limits on the number of backups saved and/or adjust the frequency of backups.

Database backups are configured in the Extreme Management Center Suite options. From any Extreme Management Center application menu bar, select Tools > Options to open the Options window. Expand the Suite Options folder and select Database Backup.

Database Backup Options

S NetSight Console Options	
Suite Options Advanced SNMP Settings Advanced SNMP Settings Alarm Configuration Alarm Event Logs and Tables Client Connections Contacts Esclus Data Display Format Dete/Time Format Dete/Time Format Edit Configuration ExtremeNetworks.com Update MAC OUI Vendor List Name Resolution ExtremeNetworks.com Update MAC OUI Vendor List Name Resolution NatSight Server Health Pert Monitor System Browser Fisz View Vieb Server Console Device Manager Discover Fisz View Vielcome View Property View Compass VLAN View Basic Policy View Wireless Manager Vireless Advanced Services Topology Manager Policy Control Console Device Manager Discover Pice View Edit Policy View Compass Nume Resolution Console Device Manager Discover D	For All Users Schedule Database Backup Sunday Monday Thursday Friday Stunday All days of week At 12-2 0-2 AM Mark Midnight Number of backups to save O Do not limit the number of backup files saved Limit the number of backup files saved All Database Backup Path The database is backed up to the server location entered in the following field. The specified location must exist and must be writable or it will not be accepted. C:Program Files/Extreme Networks/NetSight/backup P Backup Alarm and Reporting Database Database Backup File Format MMMODYYYY YYYYMMDD MMMODYYYY DDMMYYYY Example Backup File Name: Inetsight_02282014.sql Apply Restore Defaults
	Career Help

Binding the Server to One Interface

If the Extreme Management Center server has multiple NICs (Network Interface Cards) installed, it is a good practice to configure the server to always bind to the preferred IP address. If the server does not bind to the correct interface, local and remote clients and ExtremeControl engines are unable to connect to the Extreme Management Center server.

During the startup process, the Extreme Management Center server automatically binds to the first available NIC, which may not be the correct interface for the server to use. In addition, changes on the network can cause the server to bind to an incorrect interface, should the server restart during a change. You will need to make configuration changes in order to bind the server to the correct interface. On Windows systems, you need to set the binding order of the network interface cards and configure the Extreme Management Center server to bind to the correct IP address. On Linux systems, you need to configure the Extreme Management Center server to bind to the correct IP address.

For instructions, see the Extreme Management Center Installation Guide section on Systems with Multiple NICs.

Troubleshooting

The following sections provide information on tools that can be used when troubleshooting Extreme Management Center server issues.

- System-Wide Extreme Management Center Server Diagnostics
- Extreme Management Center Server Real-Time CPU and Memory Usage
- Extreme Management Center Server Disk Utilization
- Extreme Management Center Server Diagnostics
- Extreme Management Center Client Diagnostics
- Extreme Management Center Certificates
- Generate a Show Support Report

System-Wide Extreme Management Center Server Diagnostics

The Administration tab in Extreme Management Center provides detailed statistical and diagnostic information regarding the overall performance and operation of significant Extreme Management Center server functions. It is important to review all the reports available on the Administration tab (Diagnostics sub-tab) so that they can be leveraged when diagnosing and troubleshooting problems.

There are three levels of information available: Basic, Advanced, and Diagnostic. The Basic level provides reports indicating the overall status of the server. Increasing the level to Diagnostic adds additional reports providing more granular insight into the overall operation of the server.

For example, the Diagnostic level adds reports on Database Disk Usage, Partition Information, and Web Application Details, providing in-depth information such as how much each Extreme Management Center component contributes to the overall size of the server database, and DWR statistics including the number of calls made and the average time to complete.

The Diagnostic level also includes a menu of Diagnostic Actions which provide the ability to Save Diagnostic information (similar to the Show Support function) and also enable additional advanced diagnostic logging levels. (Note: As with any diagnostics, care should be taken when enabling increased diagnostic logging and is advised only with the guidance of an Extreme Networks Support Engineer.)

	41	Database Disk Usage				
evel: Diagnostic +	Diagnostic Actions *	2 Refresh				
Basic	Save Diagnostic Information	[netsightrpt] rot_default_raw216.44 MB				
Advanced	Diagnostic Levels	All Server Side Reporting Debug			Off	
Diagnostic	Clean OneView Data Tables	OneView Web Applications	Þ	٠	log4j File Override	
Identity and Acce	55	Data Collector Server	Þ		Critical	
Server		OneView Device Family Menu	Þ		Warning	
Database Di	sk Usage	Reporting Engine SQL for data points, age	gregation, and archiving		Informational	
E Partition Inf	ormation	OneView Heat Maps	÷		Verbose	
Server CPU		10(8). 10,011 10				
📰 Server Diag	nostics	[netsight] invarchivedcustomattribute	18.0 MB			
E Server Licer	ises	cticountry 16.0 MB				
📰 Server Log		invarchivedportinfos 13.0 MB ctlist 10.0 MB				
📰 Server Perf	ormance	polpolicydomains nsmapimage	2.0 MB 2.0 MB			
Server Utilities		invarchivedentityobjectinfos invcustomattribute	832.0 kB 624.0 kB			
E Web Application Details		wm_cc_template 608.0 kB nac_portalconfiguration 512.0 kB				
Wireless		invconfigurations	464.0 kB			
Support		invarchiveddeviceinfos nac_rule nac_appliance invoortinfos	432.0 kB 352.0 kB 352.0 kB 288.0 kB			

Administration Tab Diagnostics

Extreme Management Center Server Real-Time CPU and Memory Usage

Troubleshooting Extreme Management Center server performance issues related to CPU and memory utilization is easier when you can refer to a CPU utilization baseline that was charted over a period of time.

Knowing the system's normal operating behavior makes it easier to identify when the server's behavior deviates from the norm and when exactly the change occurred. It also makes it easier to identify whether the deviation corresponds to a recent change on the system or network.

For more information on how to establish a baseline, see the <u>Track Extreme</u> <u>Management Center Server CPU/Memory Trends</u> section under Monitor Extreme Management Center Server Health.

Once you have your baseline, use these four tools to monitor the Extreme Management Center server CPU and memory usage in real-time and compare that data to the baseline.

Server Statistics Window

The Server Statistics window provides a real-time view of server CPU and memory usage. Access the window by clicking the Server Information icon on the toolbar of any Extreme Management Center application, or by selecting Tools > Server Information from the menu bar. In the Server Information window, click on the Server Stats button to open the Extreme Management Center Server Statistics window, as shown below.

The window shows real-time CPU and Object Heap Memory usage. (Heap memory refers to the amount of free memory available to the Extreme Management Center server program.) Consistently high CPU usage and/or memory usage that continues to steadily increase are indicators that the system may be under duress. This would typically manifest through degraded performance or server stability issues. Both provide valuable data points when trying to understand the root cause of an issue, for example, whether performance is tied to a CPU spike, and whether that spike is specific to Extreme Management Center or the overall system.

Server Information		[- 0 %
Server: 134.141.90.55			
Uptime: 0 days 07:22:03			
Client Connections Database Loc	s Server Log License Certificates		
Display: Last 250 lines 💌			Clear Filter
Find Filter File	M NetSight Server Statistics		Refresh
	Server: 134.141.90.55		
Find	Uptime: 0 days 07:22:04	Find	
Case Sensitive Match Who	CPU: 0.00%		
Direction			
 Forward 	Object Heap Memory in Use: 260990(K)		
L			
NOT FILTERED			
at java.util.concurrent.1	Advanced Close Help)	^
at java Jang.Thread.run	makunana aka commenta matakiwa nagomenta or yorgator y	Notification(): Ealer	its register for
	m.siemens.bk.mgmt.event.EventListener][ControllerPostV731		
	m.siemens.bk.mgmt.common.RedundantLogManager]WARN	,	
	m.siemens.bk.mgmt.event.EventListener] [SensorResetEvent		
2012-11-29 11:31:18,896 WARN [co	m.siemens.bk.mgmt.event.EventListener] [ThreatEventListene	er] activate(): Connec	t to EVVC(10.20
2012-11-29 11:31:23,305 WARN [co	m.siemens.bk.mgmt.event.EventListener] [SensorResetEvent	Listener] activate(): (Connect to EVVC
	m.siemens.bk.common.net.AbstractSocketHandler] TCP error	.,	
	m.siemens.bk.mgmt.event.EventListener] [ThreatEventListene		
	m.siemens.bk.langley.GarbageCollector] RemoteAddr is null [
	m.siemens.bk.mgmt.common.RedundantLogManager]VVARN		
	m.siemens.bk.mgmt.common.RedundantLogManager]WARNI m.siemens.bk.mgmt.event.EventListener] [MUEventListener] a		
2012-11-29 11.32.55,755 WARN [CO	materiere av angine even in even indaterier ((indevenier) e	autroace(). Contridet to	2
	Configure Serv	er Stats Cic	ise Help

Extreme Management Center Server Statistics Window

Windows Task Manager

Windows Task Manager is a utility on Windows-based systems that provides a real-time view of system CPU and memory utilization. It monitors the entire system's performance to help identify whether an issue is specific to Extreme Management Center or a side effect of another process running on the system.

On the **Processes** tab, sorting the CPU and Memory columns lets you monitor the activity of the individual active processes, giving a real-time picture of the specific processes that may be consuming a larger than normal share of resources.

The **Performance** tab is an excellent overview of global CPU and Memory trends, providing a view into whether elevated usage has been sustained for a period of time or whether it changes at regular intervals, perhaps as the result of performing a specific task or action.

Windows Task Manager



Linux "top" Command

The Linux equivalent of Windows Task Manager is the "top" command, which displays the most CPU-intensive processes on the system and provides an ongoing look at processor activity in real-time.

The command displays system summary information as well as the processes currently being managed by the Linux kernel. The display continuously refreshes, providing valuable insight into the processes that are consuming the most resources and the ability to quickly monitor incremental usage of specific processes that may be slowly consuming resources over time. The output contains useful information such as CPU, Memory, Process Time, and Process ID.

Refer to Linux operating system documentation for more information about the "top" command.

Linux "top" Command Display

											, 0.42, 0.41
										opped,	
Cpu (s)											, 0.0%si, 0.0%st
Mem:	8178400	0k tot	al,	2402	576k 1	ised,		577572	24k fr	ee, 126	692k buffers
Swap:	838860	ik tot	al,		0 k 1	ised,		83886()4k fr	ee, 532	696k cached
PID	USER	PR	NI	VIRT	RES	SHR	S	\$CPU	\$MEM	TIME+	COMMAND
1075	root	20	0	4772m	935m	20m	5	1	11.7	22:33.19	java
15508	root	20		17332	1280	968	R		0.0	0:00.01	top
1	root	20		24456	2368	1356			0.0	0:01.52	init
2	root	20							0.0	0:00.00	kthreadd
3	root	20							0.0	0:00.94	ksoftirgd/0
4	root	20							0.0	0:00.00	kworker/0:0
5	root	20		0			\$		0.0	0:00,28	kworker/u:0
6	root	RT							0.0	0:00.00	migration/0
7	root	RT							0.0	0:00.33	watchdog/0
8	root	RT							0.0	0:00.00	migration/1
9	root	20							0.0	0:09.65	kworker/1:0
10	root	20							0.0	0:00.48	ksoftirgd/1
11	root	20							0.0	0:01.13	kworker/0:1
1.2	NOOT	DT	0	0	0	0	0	0	0.0	0.00 20	up robdog / 1

Linux "vmstat" Command

The Linux "vmstat" (virtual memory statistics) command displays summary information about operating system memory, processes, interrupts, paging and block I/O. The first report displayed provides the averages since the last reboot.

If you want to use the command to monitor the virtual memory activity on your system, it is best to specify a sampling interval. Executing the command at predefined intervals helps to identify the rate of change in specific values. The command "vmstat -an 10 15" executes with a display that runs every 10 seconds for 15 iterations, and includes active and inactive memory usage.

Of particular interest would be whether the system is using swap memory, and if so, how frequently and what are the overall memory conditions when this occurs. Keep in mind that it is normal for Linux-based systems to have higher memory consumption due to the operation of the OS, but further investigation is warranted when swap memory is being used.

Refer to Linux operating system documentation for more information about the "vmstat" command.

Linux "vmstat" Command Display

	root@NS-Dev.Dev.com:~\$ root@NS-Dev.Dev.com:~\$ vmstat													
pro	CS		memo	ory		swa	p	io-		syste	m		cpu	
r	b	swpd	free	buff	cache	si	30	bi	bo	in	CS	us s	y id y	wa
1	0	0	5775760	126772	532744	0	0	1	2	91	75	0	0 10	0 0
roo	root@NS-Dev.com:~\$													

Extreme Management Center Server Disk Utilization

Unmanaged log data or backup files can quickly consume disk space, creating a disk space problem on the Extreme Management Center server. Disk space issues can cause problems such as an upgrade that fails to execute due to inadequate disk space or, more seriously, an Extreme Management Center server crash.

Here are three tools you can use to troubleshoot disk usage problems on the Extreme Management Center server.

Windows OS Properties

For Windows-based systems, access the Properties window to view disk usage data. In Windows Explorer, right-click on the drive where the Extreme Management Center server is installed and select the **Properties** option from the menu.

Use the data in the window to verify that there is adequate space available for normal Extreme Management Center server logging and operations, and investigate low disk availability immediately. There are two Extreme Management Center-specific directories that you can check for excessive disk space consumption:

<install directory>\backup

```
<install directory>\appdata\logs
```

You can control the automatic file size management of these directories using Extreme Management Center options. For more information, see <u>Tuning</u> <u>Database Backup Storage</u> under Extreme Management Center Performance Tuning and Tuning Data Persistence under NAC Performance Tuning in the NAC Technical Reference.

Security	Previo	Previous Versions				
General	Tools	Hardware	Sharing			
i)S					
Type: Li	ocal Disk					
File system: N	TFS					
Used space:	81,103	3,286,272 bytes	75.5 GB			
Free space:	168,953	3,774,080 bytes	157 GB			
Capacity:	250,057	7,060,352 bytes	232 GB			
	D	rive C:	Disk Cleanup			
Compress this Allow files on file properties		disk space ve contents index	ed in addition to			

Windows Properties

Linux "vmstat -D" and "vmstat -d" Commands

The Linux "vmstat" (virtual memory statistics) command with the "-D" or "-d" option displays disk read and write activity. The "-D" option provides a summary of total disk activity for the entire system, while the "-d" option displays individual disk activity statistics for each disk on the system.

These commands are useful when monitored disk activity (see <u>Monitor Extreme</u> <u>Management Center Server Disk Access</u>) indicates an abnormal change that corresponds with performance-related issues on the Extreme Management Center server. The disk statistics provide a real-time view into disk activity that can perhaps be tied to specific actions.

Refer to Linux operating system documentation for more information about the "vmstat" command.

Linux "vmstat -D" Command Display

root@NS-Dev.Dev.com:~\$
root@NS-Dev.Dev.com:~\$ vmstat -D
28 disks
3 partitions
36531 total reads
9025 merged reads
1657216 read sectors
173536 milli reading
123437 writes
21262 merged writes
2933468 written sectors
533064 milli writing
0 inprogress IO
53 milli spent IO
AND DEP DEP C

Linux "df" and "du" Commands

The Linux "df" command displays how much free disk space is available on the file system. Use "df" to view the overall system disk utilization and identify whether certain directories are at or near full capacity. Use the "-h" option to display the statistics in human readable format.

The "du" command can be used to identify the size of specific files or directories within a parent directory. This command is useful when trying to narrow down specific areas of the file system that are consuming large amounts of disk space.

NOTE: Running the "du" command from a parent directory with the "-ha" option may return a large amount of data. Use the "|more" option or redirect to a file to view the total results for the command.

Refer to Linux operating system documentation for more information about the "df" and "du" commands.

Linux "df -h" Command Display

root@NS-Dev.Dev.com:~\$ df	-h				
Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/systemvg-root	52G	8.3G	41G	17%	
udev	3.9G	4.0K	3.9G	1%	/dev
tmpfs	1.6G	244K	1.6G	1%	/run
none	5.OM	0	5.0M	0%	/run/lock
none	3.9G	0	3.9G	0%	/run/shm
/dev/sda1	228M	25M	192M	12%	/boot
root@NS-Dev.Dev.com:~\$					

Extreme Management Center Server Diagnostics

Use the Administration tab (Diagnostics sub-tab) to obtain detailed debug information for Extreme Management Center server processes and applications. Select from a list of diagnostic options to enable targeted debugging of specific system functions. This allows for the collection of relevant data and also helps to limit the overall impact to the system when debugging is enabled.

CAUTION: Extreme Management Center server diagnostics should only be enabled when a specific area of an issue has been identified, or under the guidance of Extreme Networks Support. Certain debug options generate verbose output and could cause adverse effects to the system if enabled for extended periods of time. Debug options should only be enabled long enough to capture data from the behavior under investigation.

Access Server Diagnostics in Extreme Management Center by clicking the **Administration** tab and then expanding the Server section on the **Diagnostics** sub-tab. Enable the different diagnostic groups by setting the Diagnostic Level to "Verbose" for the applications and processes of interest. Debug diagnostic information is mainly saved to the active server.log file on the Extreme Management Center server.

Server Diagnostics

	Server Diagnostics		
evel: Basic •	OK Reset Defaults		
System	Name	Description	Diagnostic Level
Flows	AdMgr Server	ACL Manager Server	log4j File Override 🌱
Historical Statistic Collector	Alarm and Events	Alarm and event Logging	log4j File Override 💙
Identity and Access	AppIdMgr Server	AppID Manager Server	log4j File Override 🌱
Server	Authentication	User authentication and profile cache.	Verbose 👻
E Server CPU	Automated Security Manager	Automated Security Manager Application	log4j File Override 🎽
E Server Diagnostics	Certificates	Certificate Validation and Configuration	log4j File Override 🌱
E Server Licenses	Database	Database connection and transactions	log4j File Override 🌱
📰 Server Log	Device Management	Device information cache	log4j File Override 🛛 🌱
E Server Performance	Device Status Poller	Device Status Poller	log4j File Override 🛛 👻
🔄 Server Utilities	Distributed Cache	Distributed Cache	log4j File Override 🌱
Wireless	Inventory Manager	Inventory Manager Application	log4j File Override 💙
Support	Licensing	Application licensing	log4j File Override
	MSTP	MSTP management	log4j File Override 💙

Accessing the Server Log File

The server log file records server activity such as start-up log data, unexpected behavior messaging, and server debug diagnostic log data when enabled. Reviewing previous server log file output can be helpful for determining when a specific issue started to occur or for uncovering additional system issues that may be contributing to a current problem.

The file is archived daily into the same directory and is generally named in the server.log.date format.

The server log file can be accessed from the Extreme Management Center Launch page by clicking the **Administration** tab and then the **Server Log** tab. You can also view the Server Log in the Server Information window, which can be launched from the Tools menu or toolbar in every Extreme Management Center application. The Server Log can also be accessed from the <install directory>\appdata\logs directory on Windows-based systems or from the /usr/local/Extreme_Networks/NetSight/appdata/logs directory on Linuxbased systems.

Examples of the server log file locations are shown below.

Server Log File Locations

Si Uj

Client Diagnostics	Server Diagnostics	Server Utilities	Server Log	NAC Server	
2012-11-30 07:43 2012-11-30 07:43 2012-11-30 07:43 2012-11-30 07:43 2012-11-30 07:43 2012-11-30 07:45 2012-11-30 07:45 2012-11-30 07:45 2012-11-30 07:45	29,476 INFO [com 29,492 INFO [com 33,747 INFO [STD 53,780 INFO [STD 22,775 INFO [com 22,775 INFO [com 25,778 INFO [com	.enterasys.nets nenterasys.nets OUT] com.sun.ne OUT] com.sun.ne nenterasys.nets nenterasys.nets	ight.api.ServerInfologg ight.api.ServerInfologg ight.api.ServerInfologg t.ssl.internal.ssl.SSLS t.ssl.internal.ssl.SSLS ight.api.ServerInfologg ight.api.ServerInfologg ight.api.ServerInfologg ight.api.ServerInfologg	er] ** The Net: er] Starting N essionContextIn essionContextIn er] Starting E er] Starting N er] Starting N	Sigh etSNI mp10. mp10. vent tatu. etSi.
Server Information					
Server: 134.141.90.144 Uptime: 0 days 06:48:58 Client Connections Database Loc s Display: Last 250 ines Find Filter File Find Case Sensitive Match Whole W Direction		icates	 Enterasys Networks NetSight installer appdata AppId AutoSecMgr CommandScript' fileSandbox InventoryMgr isaac 		Name nacESE.2012_11_27_01.log nacESE.2012_11_28_01.log nacESE.2012_11_29_01.log nacESE.2012_11_30_01.log pccEvents.log Policy.log server.log server.log.2012-09-20 server.log.2012-09-21
Forward	O Backward		license logs		server.log.2012-09-24
NOT FILTERED			ga rogs		

2012-11-30 10:18:09,450 VVARN [com siemens bk.mgmt.event.EventListener] [ThreatEventListe 2012-11-30 10:18:27,395 ERROR [com siemens bk.common.net.invoker.AbstractSocketHandler 2012-11-30 10:18:27,398 ERROR [com.siemens bk.common.net.invoker.AbstractSocketHandler 2012-11-30 10:19:36,465 VVARN [com.siemens bk.mgmt.common.RedundartLogManager] VVAR

Extreme Management Center Client Diagnostics

Troubleshooting unexpected behavior encountered while running applications in Extreme Management Center is not limited to server-side investigations. Some behavior may be specific to individual end-systems or may be the result of a configuration on an end-system.

Use the following steps to enable diagnostics for Extreme Management Center client-specific debugging of individual Extreme Management Center applications.

 From the Extreme Management Center Launch page, click on the Administration tab. Click on Client Diagnostics. You need to log in with your username and password. Select the User Configured Diagnostics radio button and click Apply.



2. Once client diagnostics are enabled, the Launch page displays "(User Configured Diagnostics)" following each application name. Launch the desired application (for example, Console or Policy Manager).



3. The Diagnostics Configuration window opens where you can enable diagnostic message logging for a specific application or process. Click on the table entry for

the application or process and open the table editor using the Table Editor button in the upper right corner. In the Table Editor row at the bottom, set the diagnostic level. Be sure to apply your changes using the **Apply** button in the upper right corner. Click **OK** to close the window.

Alarm and Events Authentication Automated Security Manager Basic Policy	Description ACL Manager Client Alarm and event Logging User authentication Automated Security Manager Application	Level log4j File Override log4j File Override log4j File Override	
Alarm and Events Authentication Automated Security Manager Basic Policy	Alarm and event Logging User authentication	log4j File Override	
Authentication Automated Security Manager A Basic Policy I	User authentication		
Automated Security Manager A Basic Policy		log4i File Override	
Basic Policy	Automated Security Manager Application		
		log4j File Override	
Certificates	Basic Policy Management	log4j File Override	
	Certificate Validation	log4j File Override	
Compass	Compass search tool	log4j File Override	
Database	Database connection and transactions	log4j File Override	
Device Discovery	Device discovery	log4j File Override	
Device Management	Device information cache	log4j File Override	
Device Manager	Device Manager Application	log4j File Override	
Exception Handler	User interface unhandled exception handler	Verbose	
Flex Views	Flexible table views	log4j File Override	
nventory Manager	Inventory Manager Application	log4j File Override	
Licensing	Application licensing	log4j File Override	
MIB Tools	MIB Tools Application	log4j File Override	
MSTP	MSTP management	log4j File Override	
NAC Manager	NAC Manager Application	log4j File Override	
NAC Notification Engine	NAC Notification Engine	log4j File Override	
NAC Rules Engine	NAC Request Rules Engine Evaluation	log4j File Override	
NAC Rules Engine Criteria	NAC Request Rules Engine Criteria Evaluation	log4j File Override	
	NetSight Server User Authentication	log4j File Override	
	Data Collector Client	log4j File Override	
Online Help	Online help	log4j File Override	
Options	User and system option management	log4j File Override	
	Plugin discovery and management	log4j File Override	
	Policy Control Console Application	log4j File Override	
	Policy Manager Application	Warning	
Policy Manager Client SNMP	Set Verbose for all PM Client SNMP	Inneli File Override	
		(log4) File Override	-
		Restore Defaults	
		log4j File Override	
		Off	
		Critical	
		Warning	
		Informational Verbose	

4. Perform the action that generates the undesirable/unexpected behavior. The relevant debug is saved to the corresponding application log file on the client machine, located in the \Users\<user>\AppData\Roaming\NetSight\logs directory on Windows 7 or the \Documents and Settings\<user>\Application Data\NetSight\logs directory on Windows XP.

Extreme Management Center Certificates

Extreme Management Center uses server certificates to provide secure communication for application web pages and for internal communication

between server components.

On the Extreme Management Center server, use the Server Utilities page to view Extreme Management Center server communication certificates. Access the page from the Extreme Management Center Launch page by clicking the **Administration** tab. Click on **Server Utilities**. You need to log in with your username and password. Click on the **Certificates** link to open a new window that displays the Server Certificate Chain.

For more information on updating and configuring the Extreme Management Center server certificate, see the top-level Help topic Extreme Management Center and NAC Secure Communication and the How to Update the Extreme Management Center Server Certificate Help topic in the Server Information section of the Suite-Wide Tools User Guide.

Server Utilities

Client Diagnostics	Server Diagnostics	Server Utilities	Server Log
Server Utilitie	5:		
NetSight	t Suite Web Monitor (Flex V	iews) (RMON Views)	
Tomcat	status (full) (XML)		
JMX Con	sole		
JBoss W	eb Console		
JBoss M	essage Queue		
Certifica	tes		
Threads			

Generate a Show Support or Show Support Lite Report

Generate a Show Support or Show Support Lite report to provide to GTAC when requesting assistance with Extreme Management Center. These reports collect important statistical and diagnostic data.

Show Support

The Show Support report provides information pertaining to each of the applications within Extreme Management Center and creates a single archive that your support technician can review.

This data helps to answer many of the upfront questions typically asked when opening a support case, and also provides a comprehensive collection of key data that can reduce follow-up requests for more data and expedite a resolution to the issue.

The Show Support report is generated from the **Administration** tab. Click the **Diagnostics** sub-tab and then expand the **Support** section. Click the **Start Show Support** button to start generating the report.



Show Support provides information about the following:

- Core Service
- Client log files from attached clients
- Extreme Management Center ReportingServer
- Reporting diagnostic collections
- Collector Status
- Network Task Engine Details
- Vendor Profile Cache
- LoggerUtils Details
- Statistics
- Collector Config
- Device Usage Data csv file
- System Environment log file
- System Properties log file
- Rolling log file
- FlexView Details

- Domain details
- Database details
- Targets
- OneView Engine Details
- TopN Engine Details
- Host/Port Name Cache Details
- License Details
- SNMP Target Availability Summary
- SNMP Statistics Summary
- Search Details
- Target Type Counts
- Device Details Status
- Vendor Profile Details deviceTypes/myDeviceTypes.properties
- Vendor Profile Details deviceTypes/MyVendorProfile.json
- Flow Engine Details complete.
- Alarm/Event Details complete.
- Site Details complete.
- Console ConsoleMBean
- Inventory Manager InvServerManager
- Topology Manager TopologyService
- Mediation Agent MediationServer
- Application Analytics AppldMgrServer
- Extreme Management Center MapServer
- Policy Manager PolServerManager
- Policy Manager diagnostic data collection
- Domain statistics complete.
- NAC Manager TrustedAccessMgrService
- ExtremeControl engines
- Wireless Manager BkWirelessMgr
- BK Wireless Manager diagnostic data collection.

- BkManagementServer
- SSHConnectionPool
- ConfigurationManager
- DomainObjectCacheManager
- EventListeners
- ThreatObserverMgr
- ApObserverMgr
- MuObserverMgr
- RogueObserverMgr
- WlanServiceObserverMgr
- NSWMIntegration
- Langley
- BkSchedulerMBean
- TemplateMgrTestMBean
- ThirdParty log files
- Extreme Management Center GovernanceServer

Upon completion, archived data is stored on the Extreme Management Center server in the *<install directory>*\appdata\ShowSupport folder in a single zipped archive that can be sent to update an open support case.

Show Support Lite

The Show Support Lite report provides information about a smaller set of Extreme Management Center features. Selecting this report creates a much smaller file that Extreme Management Center generates more quickly than the full Show Support report.

Use the Show Support Lite report when looking to gather initial diagnostic information or when instructed by GTAC.

The Show Support report is generated from the Administration tab. Click the **Diagnostics** sub-tab and then expand the **Support** section. Click the **Start Show Support Lite** button to start generating the report.

Show Support Lite provides information about the following:

- Core Service
- ReportingServer
- Reporting diagnostic collections
- Collector Status
- Network Task Engine Details
- Vendor Profile Cache
- LoggerUtils Details
- Statistics
- Collector Config
- Flow Engine Details
- Alarm/Event Details
- Site Details
- Console ConsoleMBean
- Inventory Manager InvServerManager
- Topology Manager TopologyService
- Mediation Agent MediationServer
- Application Analytics AppldMgrServer
- Extreme Management Center MapServer
- Policy Manager PolServerManager
- NAC Manager TrustedAccessMgrService
- ExtremeControl Engines
- Wireless Manager BkWirelessMgr
- Extreme Management Center GovernanceServer

Upon completion, archived data is stored on the Extreme Management Center server in the *<install directory>*\appdata\ShowSupport folder in a single zipped archive that can be sent to update an open support case.

1/2020 PN: 9036596-00 Rev. AA Contents Subject to Change Without Notice