Exinda How To Guide:

Accelerate File Transfers

Exinda ExOS Version 7.4.3

Copyright

Document Built on Friday, July 22, 2016 at 2:40 PM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

Documentation conventions

These documentation conventions apply across all of the Exinda documentation sets. All instances of the following may not appear in this documentation

Typographical conventions

- **bold** - Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
- *italics* - Reference to other documents. For example: Refer to the *Exinda Application List*. Also used to identify in the various procedures the response the systems provide after applying an action.
- **>** - Separates navigation elements. For example: Select **File > Save**.
- `monospace text` - Command line text.
- `<variable>` - Command line arguments.
- `[x]` - An optional CLI keyword or argument.
- `{x}` - A required CLI element.
- `|` - Separates choices within an optional or required element.

Links

With the exception of the various tables of contents, all links throughout the documentation are **blue**. Most links refer to topics within the documentation, but there may be links that take you to web pages on the Internet. In this documentation we differentiate between these types of links by **underlining** only the external links.

Tips, Notes, Examples, Cautions, etc.

Throughout this manual, the following table styles are used to highlight important information:

- **Tips** include hints and shortcuts. Tips are identified by the light blub icon.

TIP

text

- **Notes** provide information that is useful at the points where they are encountered. Notes are identified by the pin and paper icon.

NOTE

Text

- **Important** notes provide information that is important at the point where they are encountered. Important notes are identified by the amber triangle.

IMPORTANT

Text

- **Cautions** provide warnings of areas of operation that could cause damage to appliances. Cautions are identified by the orange triange.

CAUTION

Text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a pale green background.

EXAMPLE

Text

- **Best Practices** are identified by the "thumbs-up" icon.

Best Practice:

It is a best practice to

Table of Contents

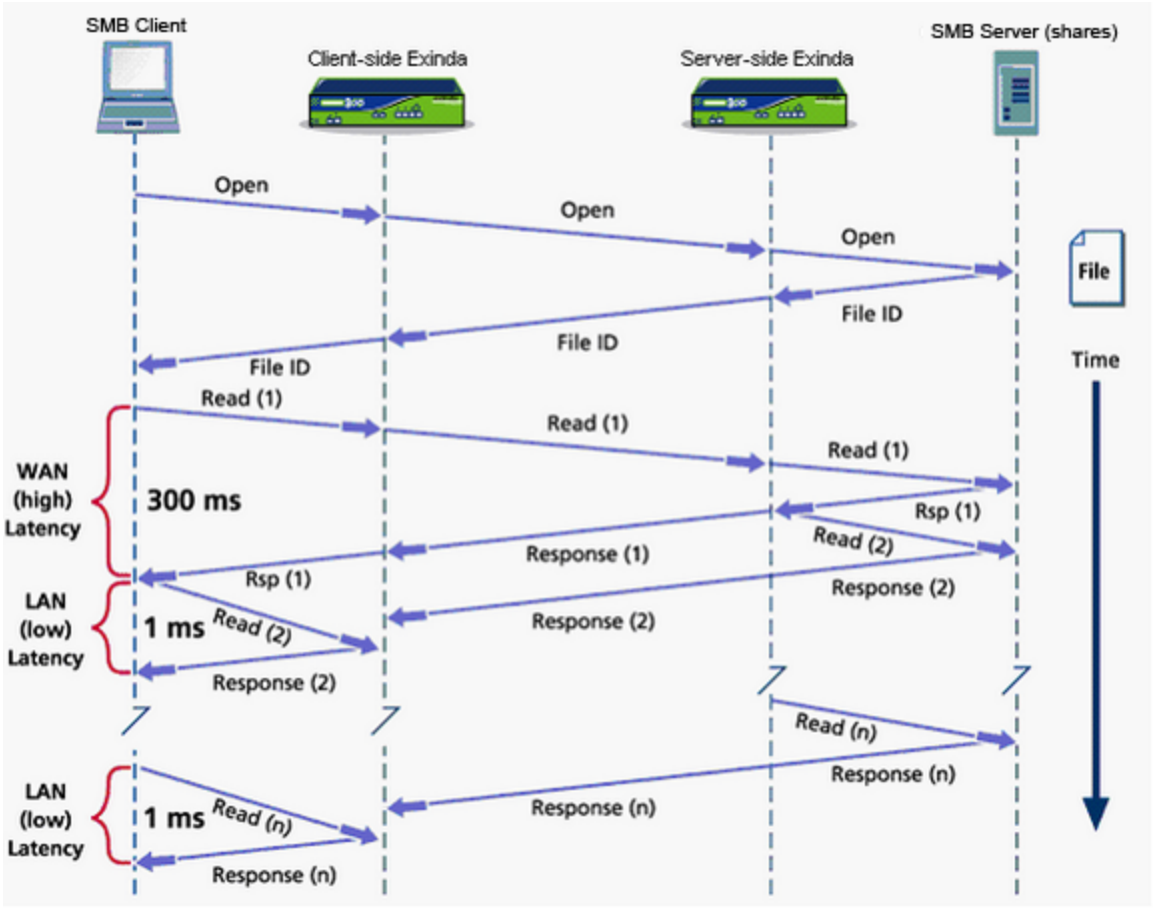
Chapter 1: Accelerating CIFS/SMB File Transfers

How SMB/CIFS (File Transfer) Acceleration Works

SMB1 and SMB2 are remote file access protocols that form the basis for Windows file sharing. Each time you browse or access files on a Windows server using Windows Explorer, Windows uses the SMB protocols to transport information (files or directory information) back and forth between your computer and the server.

In addition to file sharing, SMB is also used as a transport protocol for various higher level Microsoft communications protocols, as well as for network printing, resource location services, remote management/administration, network authentication (secure establishment services), and RPC (Remote Procedure Calls). SMB operates very poorly over a high latency WAN link because by design SMB sends a large number of back and forth transactions to complete a request.

The primary goal of Exinda SMB acceleration is to reduce the overall accumulated latency introduced by the "chattiness" of the SMB protocols. Each Exinda appliance can act on behalf of an SMB client and server to make the interaction between the two computers more efficient. Exinda maintains a state machine and database of SMB behaviors that it relies upon to optimize future SMB related transactions. When Exinda determines that a certain SMB transaction is likely to occur, it pre-fetches data and temporarily stores it in the appliance memory for future reference. Once the pre-fetched data is referenced, the data is deleted from the memory. See the following figure.



SMB acceleration works seamlessly for TCP Acceleration, WAN Memory, and Compression, and benefits from the ability of the WAN memory to reduce data traversing the WAN, just as with other applications such as FTP, HTTP, or email.

To deal with the inefficiencies of the SMB protocol Exinda has developed several optimizations to improve the performance of applications using this protocol. Each version of SMB handles file transfer optimizations in different ways, and may include reading ahead of the data stream, writing behind the data stream, and caching meta data about files and folders. In addition to this, the Exinda appliance ensures that data is efficiently compressed and deduplicated.

SMB1

With SMB1 there are several opportunities to provide optimizations: object caching, read ahead and write behind of data, and meta-data caching.

- **Object Cache**

  This refers to the saving of files to an internal file storage area on the appliance. When a client reads a file, it is cached on both the client side and server side appliances. This significantly improves

response time for successive reads of the same file as it occurs at LAN speed instead of WAN speed. When a client writes a file, the object cache is updated which allows successive reads of the file to be served as efficiently as possible without having to use the WAN.

- **Read Ahead**

  Reading ahead of the data stream is an optimization by which the appliance pre-fetches the contents of a file ahead of the client that is attempting to read it. When the Exinda appliance detects a client attempting to perform a sequential bulk read of a file, the appliance fabricates read requests to the server on behalf of the client. The end result is that the appliance is effectively sending the reads to the server and pre-populating both the client side and server side cache. Since SMB1 clients perform reads serially, this dramatically improves cold pass read performance and helps to populate the object cache quickly.

- **Write Behind**

  Writing behind the data stream is an optimization by which the Exinda appliance immediately responds to the client when it is trying to write a file. When the appliance detects a client attempting to perform a bulk write to a file, it immediately responds to the client from the client side appliance. The end result is that the Exinda appliance is effectively sending the write requests to the server so the conversation between the client and client side appliance is occurring at LAN speed. Since SMB1 clients perform writes serially, the immediate response by the appliance allows the client write requests to fill the connection, making it appear to be asynchronous and significantly improving write performance.

- **Meta-data Caching**

  Meta-data caching is an optimization by which the Exinda appliance caches the properties related to files and folders on both the client side and server side appliances. When a client queries the properties of a file or folder, it is served from cache which eliminates the need to go across the WAN. This occurs quite frequently when browsing a file share location that has a larger number of file and folder entries. Similar to the object cache, change notifications are registered to ensure that the meta-data cache does not serve stale information.

SMB2

With the addition of SMB2, most of the optimizations that were implemented for SMB1 no longer apply. Below is a rationale for each of these and why they are no longer needed.

- **Read Ahead and Write Behind**

  In SMB2, read ahead and write behind requests are built in to the client, effectively stacking the requests one on top of the other in an asynchronous manner without any gaps between them. As a result, there is no accumulation of latency and therefore no need for the appliance to attempt to perform any sort of read prefetching or immediate write response.

- **Meta-data Caching**

In SMB2, meta-data caching is performed by the client. This eliminates the need for the appliance to do any caching in the middle as the client very quickly caches its own copy of the file and folder meta-data locally and uses that for the duration of the session.

Compression and Deduplication

Aside from the protocol specific optimizations that are provided by the appliance, the Exinda SMB acceleration framework also provides some significant downstream optimization benefits, primarily in the areas of compression and deduplication. The SMB acceleration framework is reconstructing the SMB messages in their entirety before processing them. This means that for large data centric operations like reading and writing a file, the appliance is actually operating on large blocks of data as opposed to individual packets of fragmented data. In doing so, Exinda passes off these large blocks of data to our WAN memory framework. This allows the WAN memory framework to heavily optimize for compression and deduplication.

Configure file acceleration

SMB Acceleration is the file transfer specific component of the Exinda Application Acceleration Technology. To deal with inefficiencies in the SMB protocol, the Exinda appliance has several optimizations to improve the performance of applications using this protocol, including reading ahead of the data stream, writing behind the data stream, and caching meta data on files and folders.

SMB acceleration makes the following scenarios more efficient:

- **File Download (Read)** – The SMB client is reading a file from an SMB server. The server-side Exinda proactively requests future read events and passes the read information to the client-side Exinda so that it is available locally and immediately to the SMB client.
- **File Upload (Write)** – Similar to the read scenario, the Exinda appliance proactively transfers write data to the other Exinda. The client-side Exinda responds locally to write requests from the SMB client and passes the data to the server-side Exinda at WAN link speed to complete the write operation.
- **Remote Access of Microsoft Office Files** – Microsoft office files (Word, PowerPoint, Excel, etc.) which reside on a remote SMB server are often opened from a SMB client. The Exinda SMB Acceleration addresses slow downloads by pre-fetching the file data and populating it on the client side Exinda. Consequently, all SMB client requests for the file data are served from the client side Exinda at LAN speeds.
- **Directory Browsing** – When browsing a remote file system using Windows Explorer, the SMB protocol transfers various bits of information about the files you are browsing. This metadata is transferred in special SMB instructions called transactions. The Exinda appliance also caches these transactions such that they can be served locally, from the client-side Exinda appliance. This significantly improves the performance of directory browsing using the SMB protocol.

Related Topics

How SMB/CIFS (File Transfer) Acceleration Works (page 8)

Acceleration Diagnostics (page 44)

Manage optimization services (page 15)

Configure Exinda Appliance Community

A group of Exinda appliances in a network is referred to as a community. Exinda appliances that are part of the same community can accelerate to and from each other. Generally, Exinda appliances automatically discover each other when attempting application acceleration, however, if an appliance is not automatically discovered, you can manually add the Exinda appliance to the community. When the IP address of a manually added Exinda appliance changes, the community node must be updated as well.

Community Peers

Hostname	Host ID	IP Address(es)	Firmware Version	Status
exinda7	00900b2695b4	10.100.0.7	7.0.0.2070	ONLINE
exinda-tor-op	b8ac6f863261	10.20.0.205	7.0.0.2014	ONLINE
ex-beta1-wan	b8ac6f874f7c	10.10.10.11	7.0.0.2069	ONLINE
ex-beta1-lan	b8ac6f879c8f	10.10.10.10	7.0.0.2069	ONLINE
exinda-tor-op2	bc305bd6c2ea	10.20.0.206	6.4.3.2784	ONLINE
weber-exinda	d4ae528e15a5	10.0.0.10	6.4.3.2784	ONLINE

Figure - List of automatically discovered Exinda appliances

NOTE

The Community service uses port 8017 to communicate between Exinda Appliances. Please ensure this port is open for proper functionality.

Version Info:

- In a pre-6.4 version, by default, the community was larger than it needed to be, which caused some inefficiencies. In this case, user-defined community groups allow you to create multiple separate smaller Exinda Communities in the same network.
- In 6.4 and later versions, appliances automatically join the community of appliances with which they are accelerating. If you want your 6.4 or later appliance to belong to a community of pre-6.4 appliances, you need to configure the community settings to match your pre-6.4 appliances.

Related Task

Exinda Communities: adding, editing, and removing appliances (page 13)

Exinda Communities: adding, editing, and removing appliances

Use the following sets of instructions to edit the listing of Exinda community members. For appliances with firmware versions v6.4.0 or later, you do not need to manage communities unless you want such an appliance to join a community created for a pre-6.4.0 appliance group.

NOTE

An Exinda appliance can belong to multiple community groups. By default, all appliances belong to the community group with Group ID 0. As a security measure, the Community Group ID can be used like a PIN to restrict access to any other Exinda appliance from joining your community.

Manually adding an Exinda appliance to the community

1. Go to **Configuration > System > Optimization > Community**.
2. In the **Manually Add New Community Node** area, type a **Name** and the **IP Address** for the Exinda appliance.

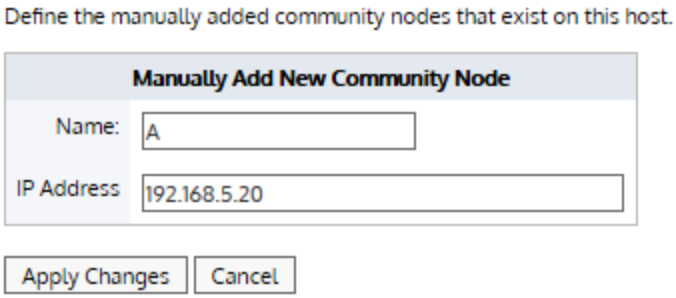
3. Click **Apply Changes**.

   The appliance is added to the list of manually added community nodes.

Editing manually added communities

1. Go to **Configuration > System > Optimization > Community**.
2. On the **Manually Added Community Nodes** panel, for the particular appliance, click **Edit** .

The edit screen opens.



3. Modify the name or IP address of the appliance.
4. Click **Apply Changes**.

Removing manually added Exinda appliances from the community

1. Go to **Configuration > System > Optimization > Community**.
2. To remove individual appliances, on the **Manually Added Community Nodes** panel, find the appliance and click the **Delete** button next to its entry.
3. To remove all appliances from the community, click **Remove all community peers from system**.

Manage optimization services

The Exinda optimization technology enables applications to run faster over the WAN. Latency in the network affects user productivity and satisfaction with their applications and network. Latency can be due to the sheer volume of data that must be returned for the given application as well as contention for the available bandwidth, the distance that the data must travel while the user is waiting for the data to be retrieved, including the number of back-and-forth communications of "chatty" applications, and failures of the data delivery requiring the data to be retransmitted .

The Network Orchestrator appliance uses a variety of techniques to address these issues. The appliance can reduce the amount of data transmitted over the WAN by using deduplication, compression, and caching techniques. The appliance can minimize delays associated with waiting for the data to be returned by reducing the chattiness of particular protocols and by anticipating requests for data and pre-fetching the data. The appliance can also reduce the frequency of data delivery failures so that data does not have to be retransmitted.

Related Topics

Universal Acceleration Service (page 15)

Protocol-specific Acceleration (page 16)

Data caching (page 17)

Configuring the Optimization Services (page 17)

Universal Acceleration Service

- **Exinda Community** – Provides appliance auto-discovery and acceleration capability services between all Exinda appliances in the WAN. To learn more, read How Appliance Discovery Works

(page 18).

- **WAN Memory** – Provides data reduction using deduplication and compression technology.

Protocol-specific Acceleration

- **TCP Acceleration** – Provides layer 4 (TCP) protocol optimization.

  The TCP protocol can be optimized by establishing a protocol tunnel to avoid subsequent 3-way TCP handshake chattiness and ensuring that the tunnel is kept alive. TCP Acceleration also allows the administrator to set the TCP receive window size to optimize the amount of data in flight given the environment characteristics and to set congestion control algorithms to best match the environment. TCP Acceleration will also reduce chattiness and the amount of data on the wire by acknowledging the receipt of packets in batches instead of acknowledging each packet individually. TCP Acceleration also notifies ECN-aware (Explicit Congestion Notification) routers without dropping packets.

- **SSL Acceleration** – Provides acceleration for SSL encrypted connections.

  SSL Acceleration provides acceleration of SSL encrypted TCP sessions by intercepting SSL connections to configured servers and decrypting them, performing acceleration techniques, then re-encrypting them again. Only traffic to servers that are explicitly configured is SSL accelerated. Any SSL traffic that the Exinda appliance sees that does not belong to a configured server is ignored.

- **SMB Acceleration** – Provides layer 7 SMB1 and SMB2 (Windows File Sharing) protocol optimization.

  SMB (Server Message Block),operates as an application-layer network protocol used for providing shared access to files, printers, serial ports, and miscellaneous communications between nodes on a network. May also be known as CIFS (Common Internet File System), where CIFS is a dialect of the SMB protocol.

  SMB Acceleration is the file transfer specific component of the Exinda Application Acceleration Technology. To deal with inefficiencies in the SMB protocol, the Exinda appliance has several optimizations to improve the performance of applications using this protocol, including reading ahead of the data stream, writing behind the data stream, and caching meta data on files and folders.

- **NCP Acceleration** – Provides layer 7 NCP (NetWare Core Protocol over TCP port 524) protocol optimization.

  NCP is used in some products from Novell. NCP is used to access file, print, directory, clock synchronization, messaging, remove command execution, and other network service functions in these Novell products.

Data caching

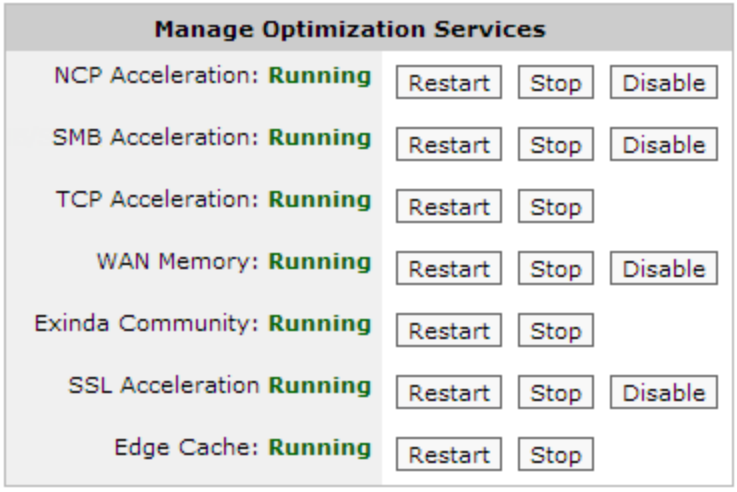
Edge Cache – Provides acceleration of static web content such as HTML, GIF, JPEG, ZIP, RAR, ISO as well as dynamic content including YouTube, Google Video, Vimeo.

NOTE

The Acceleration feature (including universal & protocol-specific acceleration) is licensed separately. Edge Cache is also licensed separately. Please contact your local Exinda representative if you wish to enable either of these features.

Configuring the Optimization Services

The Manage Optimization Services dialog allows you to start, stop, and disable the optimization services running on the Exinda appliance. Ensure that the service that you need is running. To find the Management Optimization Services controls, go to **Configuration > System > Optimization > Services**.

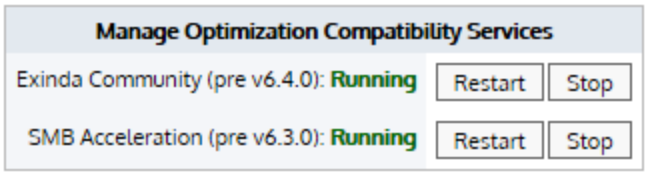


CAUTION

If a service is disabled, any concurrently accelerated connections remain untouched, that is acceleration continues, whereas any new connections are not be able to use the service. When a service is stopped, all accelerated connections (new and concurrent) stop using the service immediately. Stopping services like SMB, TCP, and WAN Memory might cause a failure in currently accelerated connections requiring them to be re-established.

Managing Optimization Compatibility

To enable compatibility with Exinda appliances that are running older firmware, you can manage the services that interact with these appliances. Go to **Configuration > System > Optimization > Services**. At the bottom of the page you can start, restart, and stop the Exinda Community service (for pre v6.4.0 appliances) and the SMB Acceleration service (for pre v6.3.0 appliances).



How Appliance Discovery Works

For the most part, acceleration requires two appliances: one to accelerate (such as compressing, or deduplicating data) and one to decelerate (such as recomposing the traffic from the compressed deduplicated traffic). Therefore each appliance must know of the other appliances with which it can accelerate. To find other appliances, the appliances have an auto-discovery process. It is used for two purposes:

1. The discovery of which connections can be accelerated.
2. The discovery of new Exinda appliances on the network.

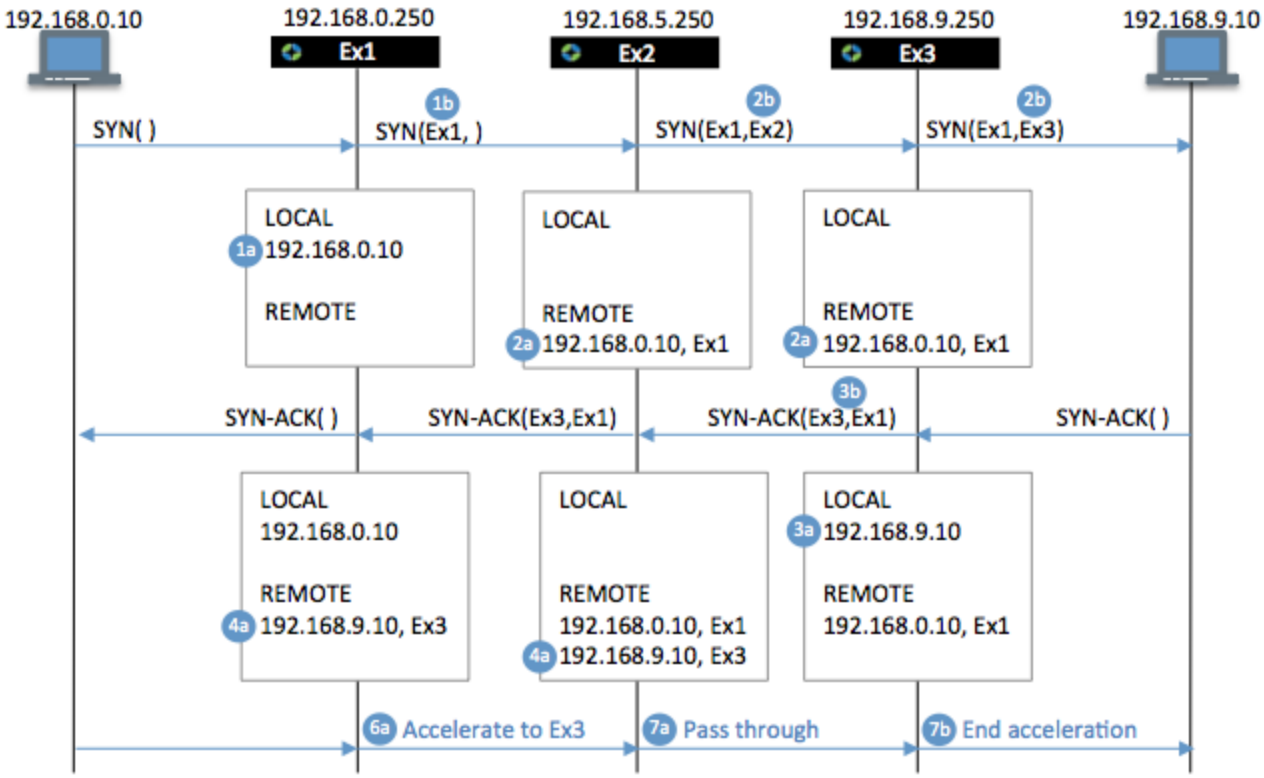
Appliances that can participate in accelerated communications are discovered by detecting extra information in the flow that is required during acceleration of a flow. The appliance adds the following information to the TCP option of SYN, SYN-ACK, and the first ACK packets of each new connection:

1. Source Appliance ID
2. Destination Appliance ID
3. Acceleration Module Map

Optionally an IP address corresponding to one of the appliances can be sent. In addition to this, each appliance must keep a list of the host IP/appliance ID pairs, which indicates which Exinda appliance terminates the acceleration for conversations with a given host IP.

Discovery Process

The connection discovery process is as follows:



1. When an appliance receives a packet SYN from a client:
   a. It adds the client IP to its local list.
      E.g., adding 192.168.0.10 to the Ex1 local list.
   b. It adds the auto-discovery option to the packet, filling out the source details.
      E.g., adding Ex1 as the source of the SYN when leaving Ex1.
   c. If the server exists in the appliance remote list, then the destination field is filled out with the appliance details, otherwise the destination is left blank.
2. When an appliance receives a SYN packet containing the auto-discovery option:
   a. It records the client IP address and source appliance ID to its remote list.
      E.g., adding 192.168.0.10, Ex1 to the local lists of Ex2 and Ex3.

   b. It fills out the destination details and forwards the packet on.
   E.g., adding Ex2 as the destination of the SYN when leaving Ex2 and replacing the destination of the SYN with Ex3 when leaving Ex3.

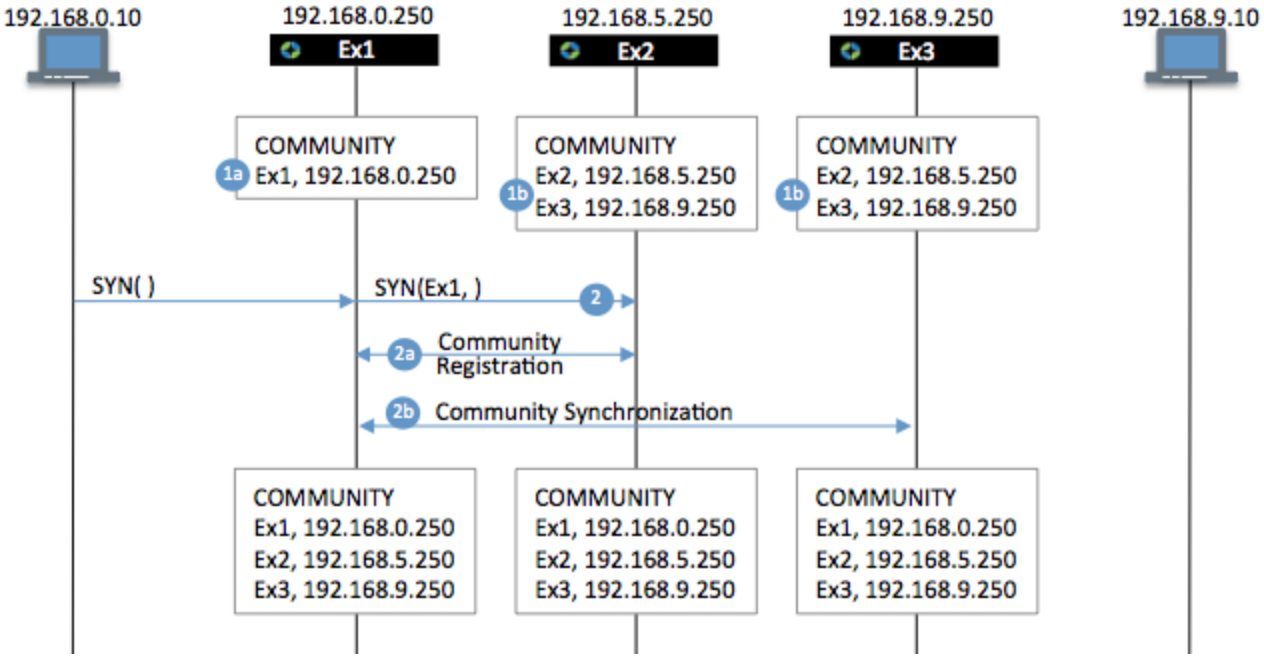
3. When an appliance receives a SYN-ACK from the server without any auto-discovery option:
   a. It adds the server IP to its local list.
   E.g. adding 192.168.9.10 to the local list of Ex3.
   b. It adds an auto-discovery option with both the source and destination details filled out.
   E.g., adding Ex3 as the source and Ex1 as the destination in the SYN-ACK.
4. When an appliance receives the SYN-ACK containing the auto-discovery option:
   a. It adds the server IP address and source appliance ID to the remote list.
   For example, adding 192.168.9.10, Ex3 to the remote list of both Ex1 and Ex2.
5. After the SYN-ACK has passed through, both end appliances know which client or server that they are accelerating for and which other appliance they are accelerating with.
6. When an appliance receives a packet destined for a server, if it finds the source IP address of the packet in its local list and the destination IP address is in its remote list, then it performs acceleration techniques on the packet.
7. When an appliance receives a packet that has been accelerated:
   a. If it finds that the destination does not refer to itself, then it will ignore all further packets that are part of that connection.
   b. If it finds that the destination does refer to itself, then it will end the acceleration and forward the unaccelerated packets to the server.

Exinda Community

A group of Exinda appliances in a network is referred to as a community. Exinda appliances that are part of the same community can accelerate to and from each other. The community is generally those Exinda appliances that were automatically discovered.

NOTE

If an appliance is not automatically discovered, you can manually add the Exinda appliance to the community. To learn how to manually add an appliance to the community, read Configure Exinda Appliance Community (page 12).



When an appliance receives an auto-discovery option from a source that the Exinda community does not know about, it can notify the community which will establish a connection to that appliance, and add it to the community.

1. The appliances may have established communities already.
   a. One appliance may not yet belong to the community.
   b. Other appliances may belong to the same community.
2. When an appliance receives an auto-discovery option from a source the Exinda community does not know about,
   a. It establishes a connection to that appliance and adds it to the community.
   b. It notifies other members of the community.

This may also cause two existing communities to join together.

The Auto Discovery process is very lightweight - it adds negligible latency/delay to packets as they pass through the Exinda appliance.

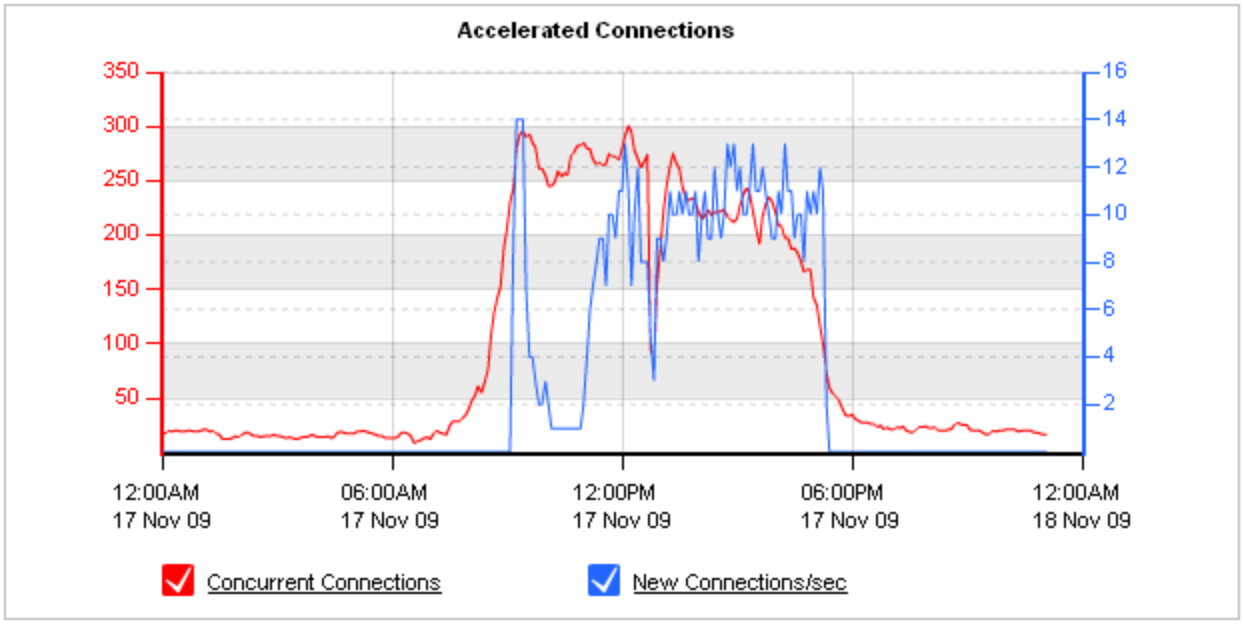
Accelerated Connections Report

The Accelerated Connections Report shows the number of concurrent accelerated connections as well as the connection establishment rate over time for the selected time period. It also shows the number of connections for each application acceleration type (SSL, SMB1, SMB2, NCP). This chart can answer questions such as:

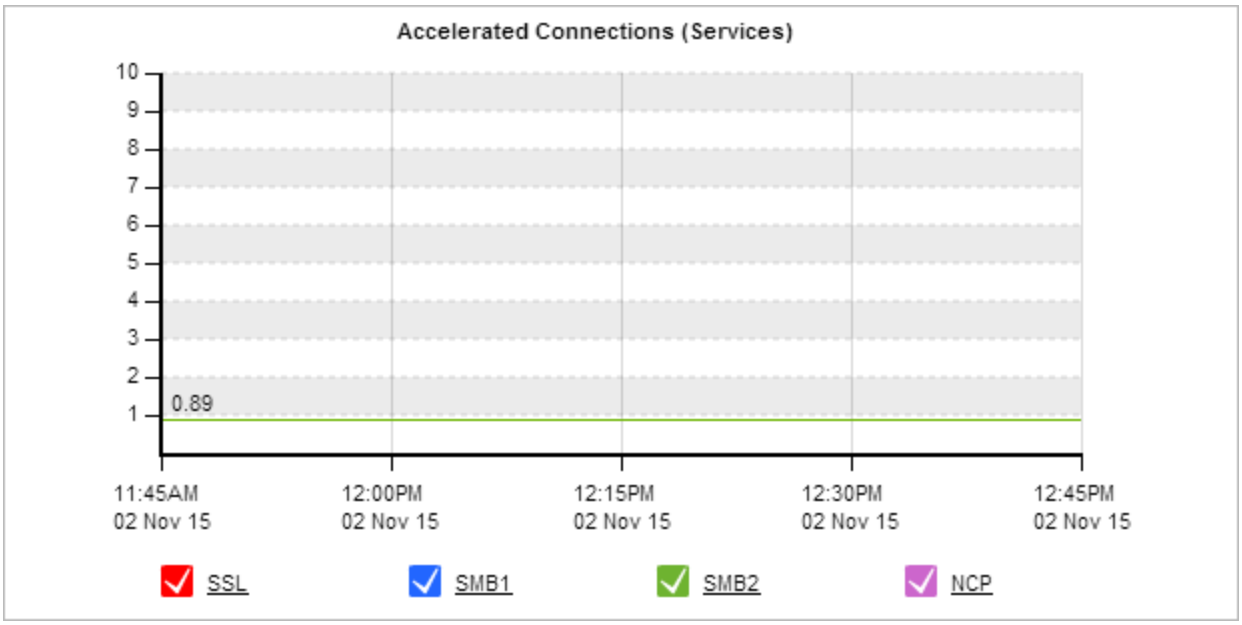
- Is there an unusual number of accelerated connections or is the connection rate particularly high or low?
- Is my traffic being accelerated as I expect?
- Am I close to or have I exceeded my licensed maximum number of accelerated connections?"

Connections over the licensed limit pass through the appliance without acceleration. If you are concerned about exceeding your licensed maximum, you can set an alert so that you will be emailed or so that the appliance will send an SNMP trap when the number of connections exceed your licensed limit.

To find the report, go to **Monitor > System > Accelerated Connections**.



The second chart shows accelerated connections for each type of accelerated traffic: SSL, SMB1, SMB2, and NCP.



How do I know what my licensed accelerated connections limit is?

You can view the details of your license.

1. Go to **Configuration > System > Setup > License**.
2. The **Max AA Connections** field in the current system license status reports your licensed limit.

How do I set an alert or send an SNMP trap when the number of accelerated connections has exceeded my licensed limit?

1. Go to **Configuration > System > Setup > Alerts**.
2. Ensure the appropriate check boxes are selected for **Max Accelerated Connections Exceeded**.

NOTE

The appliance must already be configured for email or SNMP.

Related Topics

Alerts (page 26)

Email Configuration (page 37)

Email Configuration (page 37)

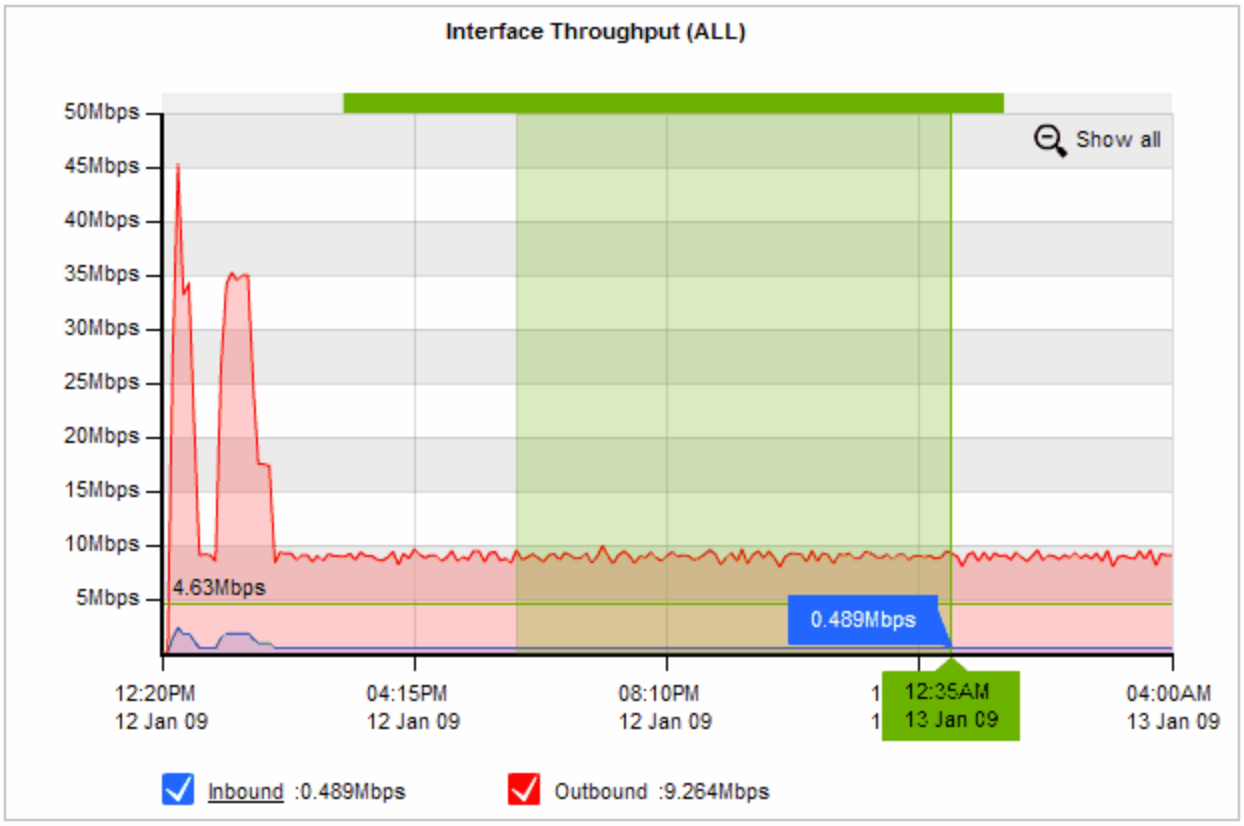
How do I interact with the interactive flash time graphs?

- To understand how to get a better look at traffic patterns and to remove clutter on the time graph, see Using Interactive Time Graphs.
- To understand how to set the desired time range for a chart, see Setting the Time Range.
- To understand how to print the report or schedule the report, see Printing and Scheduling Reports.

Using Interactive Time Graphs

If you want to get a better look at a traffic pattern or if the chart is too cluttered, you can zoom in to a custom time range and remove time series lines that you are not interested in on the time graphs.

To zoom into a custom time range, click and drag your mouse on the chart to select the desired time range. To return to the initial time range click the 'Show all' magnifying glass icon. Any data displayed below these interactive graphs will automatically be updated with the data for the selected time range.



To remove a time series line, click on the check in the graph legend or in some cases the table below the chart to toggle off the display of that line.

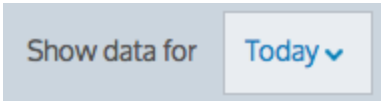
NOTE

The interactive feature is only applicable to Flash generated graphs. To change the graph display option navigate to Configuration > System > Setup > Monitoring.

Setting the Time Range

For each chart, you can set the time range that is reported in the chart.

At the upper-right of the report, select the desired date range from the drop down list. Custom time ranges are not supported.



After the date range is select, the graphs and charts are immediately updated.

Printing and Scheduling Reports

Monitoring reports can be exported as a PDF document, saved as a scheduled report, or can be printed directly from the Web UI. The following icons appear on the top-right of the interface:

- **Print**: Clicking on the Printer icon will open a new browser window and format the current report suitable for printing. It will then prompt you to select a printer.

NOTE

The print option is not available from the new application, subnet, and virtual circuit monitoring pages.

- **Schedule PDF**: Clicking on the schedule icon will save the report configuration to the scheduled reports. It will prompt you for a report name, the scheduled frequency, the email addresses to send it to, and optionally a password if you choose to password protect the PDF.
- **PDF**: Clicking on the PDF icon will render the current report as a PDF document and prompt you to save or open the PDF file once complete.

NOTE

Printed report and PDF reports may appear slightly different from the reports displayed on the Web UI.

Alerts

Alerts will notify you when there are issues or potential issues with either the Exinda appliance system (such as CPU utilization and memory paging) or with your traffic (such as an application performance score dropped).The alerts can either be sent by email or by SNMP traps. Use the alerts to ensure the system and your network is operating the way you need it to.

NOTE

To email alerts, valid SMTP and email settings are required. See Email Configuration (page 37). Recipients of the email alerts are configured where SMTP is configured.

To send SNMP traps, valid SNMP settings are required. See SNMP Configuration (page 30).

Name	Enable	Send Email	Send SNMP Trap	Trigger Threshold	Clear Threshold
CPU Utilization	☑	☑ Enable	☑ Enable	95 % Busy	80 % Busy
Disk Usage	☑	☑ Enable	☑ Enable	7 % Free	10 % Free
Memory Paging	☑	☑ Enable	☑ Enable		
NIC Collisions	☑	☑ Enable	☑ Enable	1 %	1 %
NIC Link Negotiation	☑	☑ Enable	☑ Enable		
NIC Dropped Packets	☑	☑ Enable	☑ Enable		
NIC Problems - RX	☑	☑ Enable	☑ Enable		
NIC Problems - TX	☑	☑ Enable	☑ Enable		
Bridge Link	☑	☑ Enable	☑ Enable		
Bridge Direction	☑	☑ Enable	☑ Enable		
System Startup	☐	☑ Enable	☐ Enable		
SMB Signed Connections	☑	☑ Enable	☑ Enable		
SLA Latency		☑ Enable	☑ Enable		
SLA Loss		☑ Enable	☑ Enable		
APS		☑ Enable	☑ Enable		
APM		☑ Enable	☑ Enable		
Redundant Power	☑	☑ Enable	☑ Enable		
Redundant Storage	☑	☑ Enable	☑ Enable		
Connection Limiting		☑ Enable	☑ Enable		
Max Accelerated Connections Exceeded	☐	☑ Enable	☑ Enable		
Asymmetric Route Detection	☑	☑ Enable	☑ Enable		
MAPI Encrypted Connections	☑	☑ Enable	☑ Enable		

Apply Changes

Some alerts are enabled with no option to disable, but for all alerts you need to decide if you want email notifications and/or SNMP traps. For some alerts, you can specify operational thresholds to trigger or clear the alerts.

Specified Thresholds Exceeded

- **SLA Latency** – Alert raised when the specified latency for an SLA object is exceeded.
- **SLA Loss** – Alert raised when there is loss for a SLA.
- **APS** – Alert raised when the defined threshold for an APS object is exceeded.

- **APM** – Alert raised when the defined threshold for an APM object is exceeded.
- **Connection Limiting** – Alert raised when one or more Virtual Circuits has connection limits enabled, and the threshold was reached.
- **Max Accelerated Connections Exceeded** – Alert raised when the number of accelerated connections exceeds the licensed limit. Connections over the licensed limit pass through the appliance and are not accelerated.

Particular Traffic Patterns Detected

- **Asymmetric Route Detection** – Alert raised when traffic from a single connection comes in to the network through one interface or node, and goes out through another interface or node.
- **SMB signed connections** – Alert raised when SMB signed connections are present.
- **MAPI Encrypted Connections** – Alert raised when encrypted MAPI traffic to a Microsoft Exchange server is detected on an Exinda appliance. Encrypted MAPI traffic cannot be accelerated.

Appliance Issues

- **CPU Utilization** – Alert raised when the CPU utilization threshold is reached. The defaults are 95% and 80% busy respectively.
- **Disk Usage** – Alert raised when the used disk space threshold is reached. The defaults are 7% and 10% free respectively.
- **Memory Paging** – Alert for memory use and paging.
- **NIC Collisions** – Alert raised when collisions are present on the interfaces. The defaults are 20 and 1 per 30 sec respectively.
- **NIC Link Negotiation** – Alert raised when the speed/duplex on an interface is set to auto, but it is negotiating at half duplex and/or 10Mbps.
- **NIC Dropped packets** – Alert raised when dropped packets are present on the interfaces.
- **NIC Problems - RX** – Alert raised when RX errors are present on the interfaces.
- **NIC Problems - TX** - Alert raised when TX errors are present on the interfaces.
- **System Startup** – Alert raised when the Exinda appliance boots up.
- **Bridge Link** – Alert raised when one of the links on an enabled bridge is down.
- **Bridge Direction** – Alert raised when the appliance cabling is incorrect. In most cases, it indicates the Exinda WAN interface has been incorrectly plugged into the LAN and vice versa.
- **Redundant Power** – Alert raised when one of the power supplies fails (only available on platforms with power redundancy).
- **Redundant Storage** – Alert raised when one of the hard disks fails (only available on platforms with storage redundancy).

Related Task

Enabling System Alerts (page 29)

Enabling System Alerts

Use the following instructions to enable the system alerts.

Before you begin…

Read through Alerts (page 26) for an understanding of what each of the alerts does.

To enable alerts

1. Go to **Configuration > System > Setup > Alerts**.
2. For each of the listed alerts, decide upon which you need **Enabled**.
3. For each of the enabled alerts, select the types of notification to receive: **Send Email**, **Send SNMP Trap**, or both.
4. If selecting **CPU Utilization**, **Disk Usage**, or **NIC Collisions** alerts, specify the **Trigger Threshold** and **Clear Threshold** levels that cause the notifications to be sent.

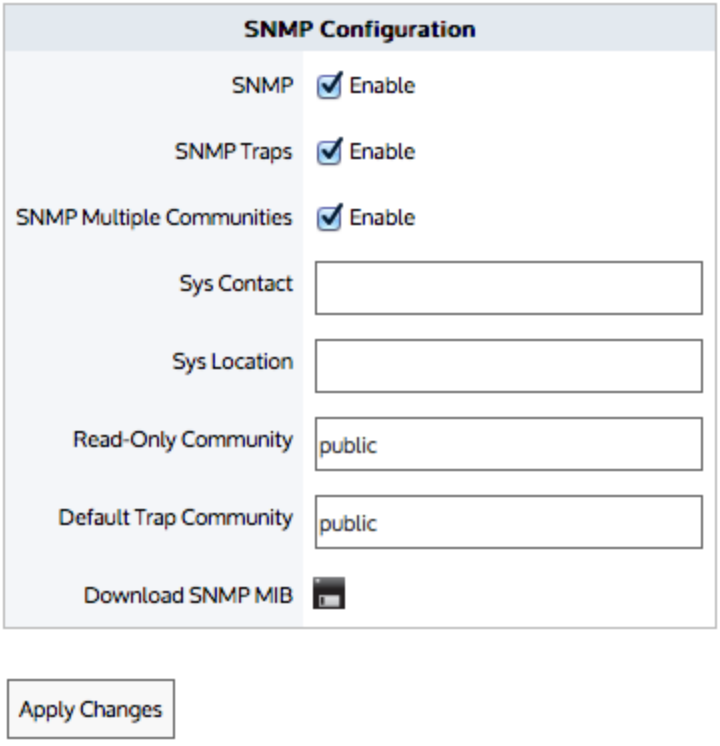
NOTE

When the Trigger Threshold is reached, an alert notification is sent to the administrator. When the Clear Threshold values are reached, the notifications stop being sent.

5. Click **Apply Changes**.

Chapter 2: SNMP Configuration

The Exinda appliance allows data export to SNMP systems. Configure the SNMP settings or download the Exinda SNMP MIB.



NOTE

To disable or enable SNMP traps for system alerts, see Alerts (page 26).

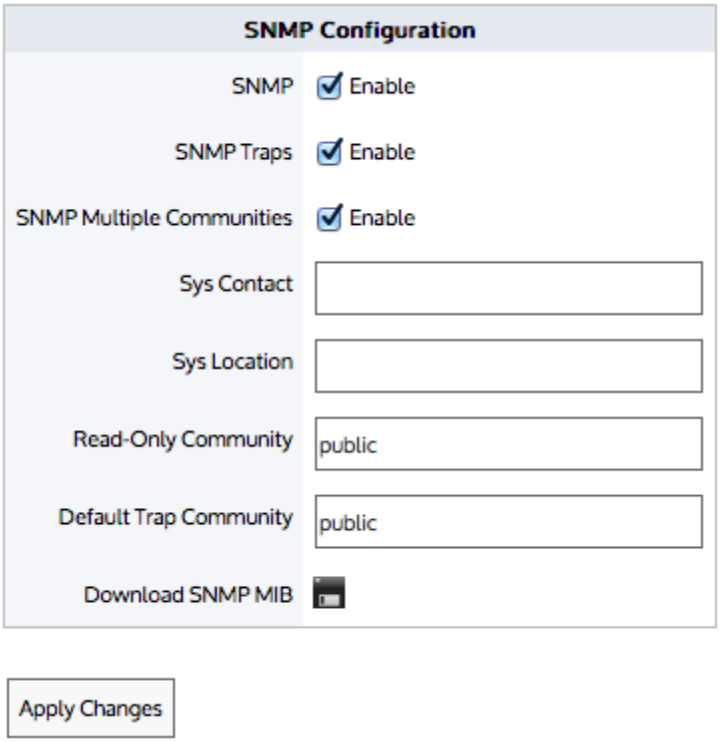
See the following for more information:

Configuring SNMP

Use the following instructions to configure SNMP.

Procedure

1. Go to **Configuration > System > Network > SNMP > SNMP Configuration**.



2. Enable the following, as needed:
   - **SNMP**
   - **SNMP Traps**
   - **SNMP Multiple Communities**

   NOTE: *When the Multiple Communities option is disabled, the Community list area does not appear.*
3. In the **Sys Contact** field, specify the syscontact variable in MIB-II.
4. In the **Sys Location** field, specify the syslocation variable in MIB-II.

5. Type the **Read-only** and **Default Trap** community string.

   NOTE: *When the Read-only community is changed to have a value that does not match an existing community, a new SNMP community is added to the list.*

6. Click **Apply Changes**.

Removing an unwanted SNMP Community

Use the following instructions to remove an unwanted SNMP community.

Procedure

1. Go to **Configuration > System > Network > SNMP > List of configured SNMP Communities**.

2. In the list of **SNMP Communities** area, select the checkbox next to community entry and click **Remove Selected**.

Downloading the SNMP MIB file

Use the following instructions to download the SNMP MIB file. The file contains additional monitoring information.

Procedure

1. Go to **Configuration > System > Network > SNMP**.

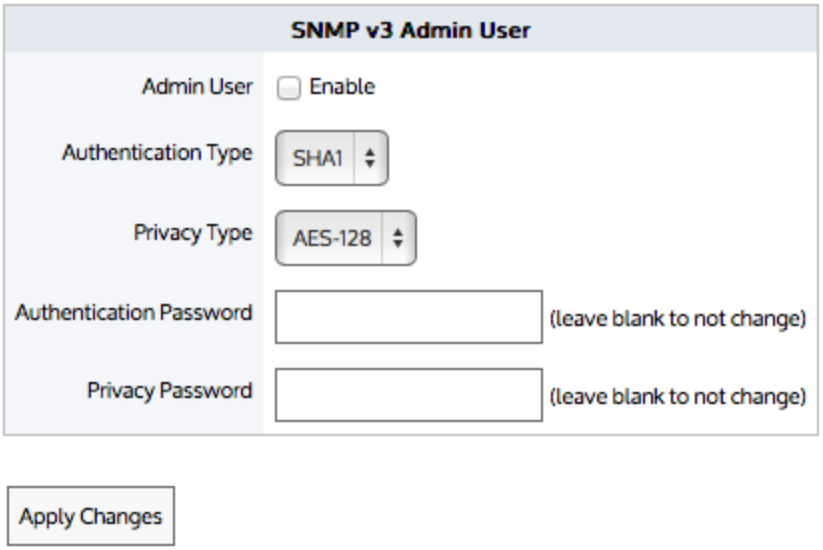
2. Under **SNMP Configuration**, click **Download SNMP MIB**.
   The `EXINDA-MIB.txt` file downloads to the location you specify.

Changing SNMP authentication for Admin user

Use the following instructions to change the SNMP authentication for the Admin user.

Procedure

1. Go to **Configuration > System > Network > SNMP > SNMP v3 Admin User**.

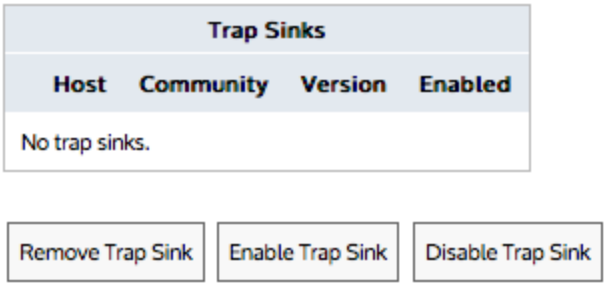


2. If you need to enable **Admin User**, select the checkbox.
3. From the **Authentication Type** spin-box, select either SHA1 or MD5.
4. From the **Privacy Type** spin-box, select either AES-128 or DES.
5. If necessary, change the **Authentication Password** by typing the new password.
6. If necessary, change the **Privacy Password** by typing the new password.
7. Click **Apply Changes**.

Temporarily stopping the sending of SNMP traps

Use the following instructions to disable the sending of SNMP traps to the sink server.

Procedure



1. Go to **Configuration > System > Network > SNMP > Trap Sinks**.
2. In the list, select the checkbox for server and click **Disable Trap Sink**.
3. To re-enable the server, select the server from the list and click or **Enable Trap Sink**.

Removing Trap Sink servers

Use the following instruction to remove a trap sink server.

Procedure

1. Go to **Configuration > System > Network > SNMP**.

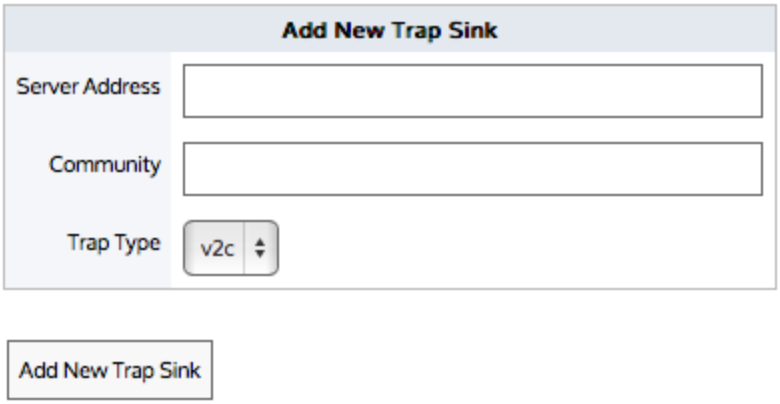
2. In the **Trap Sinks** area, select the server from the list and click **Remove Server**.

Defining SNMP trap destinations

Use the following instructions to define where SNMP traps are sent.

Procedure

1. Go to **Configuration > System > Network > SNMP**.



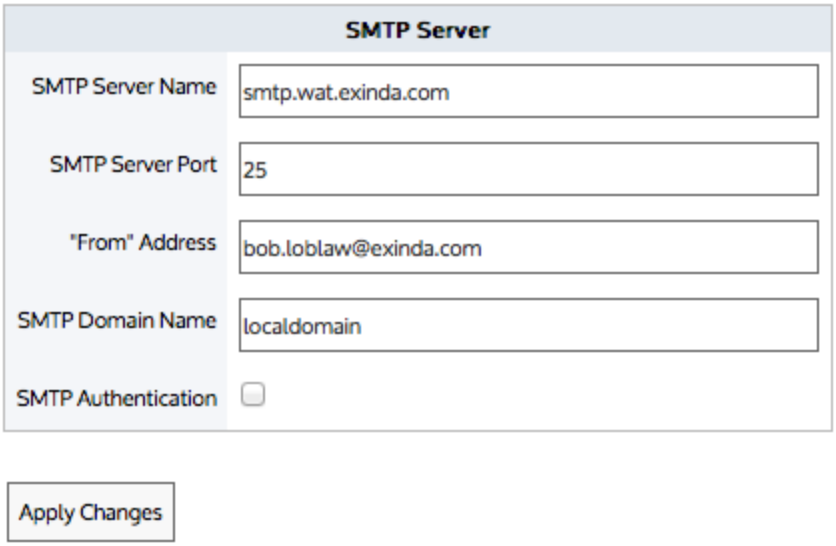
2. In the **Add New Trap Sink** area, specify the hostname or IP address of the SNMP trap sink server.

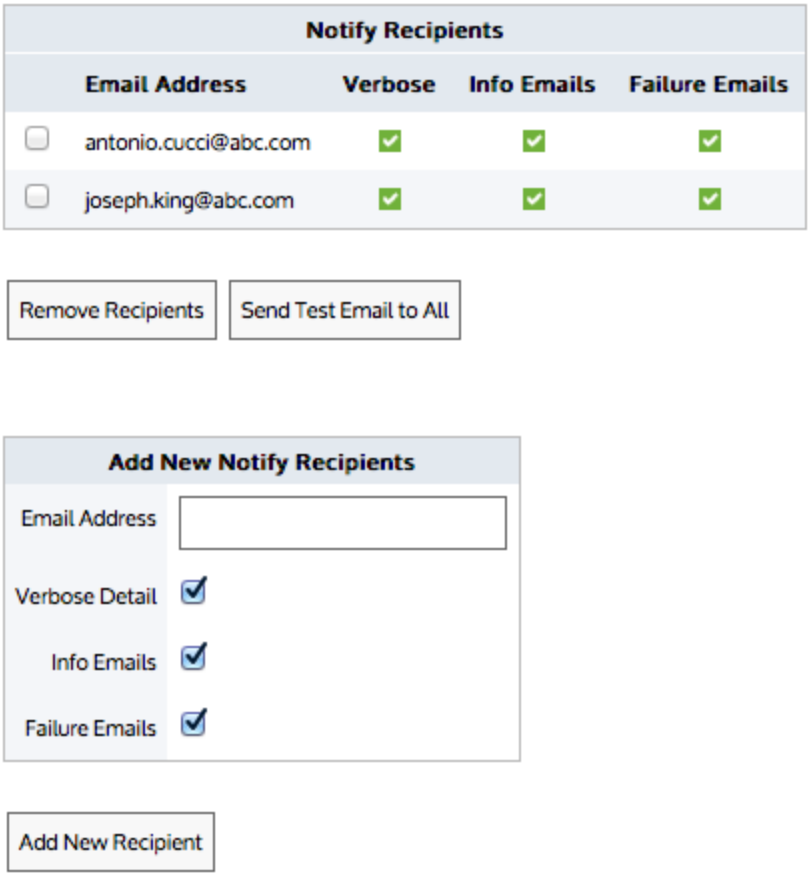
   TIP: You can specify IPv4 or IPv6 addresses, or a hostname.

3. Type the **Community** string for the SNMP trap sink server.
4. Select the appropriate SNMP trap type to send to the sink server.
5. Click **Add New Trap Sink**.

Chapter 3: Email Configuration

An SMTP server is required for sending email from the Exinda appliance. The appliance can email scheduled reports, system alerts, and auto-support notifications. Initially, you must configure the connection to the SMTP server, and then manage the users who receive the system notifications.





See the following for more information:

Configuring SMTP Server settings

Use the following instruction to configure the SMTP server settings.

Procedure

1. Go to **Configuration > System > Network > Email > SMTP Server**.
2. In the **SMTP Server Name** field, type the name.

   TIP: *You can use IPv4 or IPv6 addresses, or DNS names.*
3. In the **SMTP Server Port** field, type the port number.

   NOTE: *The default port number is 25.*
4. In the **"From" Address** field, type the email address from which the system alerts and report notifications should be sent.
5. If authentication is required, select the **SMTP Authentication** checkbox, and provide the **Username** and **Password**.
6. If necessary, select the **Use Secure Sockets Layer (SSL)** checkbox.
7. Click **Apply Changes**.

Adding notification email recipients

Use the following instructions to add new notification email recipients.

Procedure

1. Go to **Configuration > System > Network > Email > Add New Notify Recipients**.
2. In the **Email Address** field, type the email address.
3. Select the types of notifications the user should receive:
   - **Verbose Detail**—Send detailed event emails to the user.
   - **Info Emails**—Send informational emails to the user.
   - **Failure Emails**—Send failure emails to the recipient.
4. Click **Add New Recipient**.
   The new recipients are added to the Notify Recipients list above.

NOTE

The types of emails being received by a user cannot be modified. To change which emails a user receives, you must first delete the user, and then add the email address again with the appropriate types of notifications selected.

Related Tasks

Testing the SMTP configuration (page 40)

Removing notification email recipients (page 40)

Testing the SMTP configuration

Use the following instructions to test the SMTP configuration.

Procedure

1. Go to **Configuration > System > Network > Email > Add New Notify Recipients**.
2. Add your own email address and click **Add New Recipient**.
   The list in the "Notify Recipients" section above updates.
3. In the **Notify Recipients** section, click **Send Test Email to All**.

Related Tasks

Adding notification email recipients (page 39)

Removing notification email recipients (page 40)

Removing notification email recipients

Use the following instructions to remove users from the list of notification email recipients.

Procedure

1. Go to **Configuration > System > Network > Email > Notify Recipients**.
2. In the list, select the user to be deleted.
3. Click **Remove Recipients**.
   The user is removed from the list, and will no longer receive email notifications.

Related Tasks

Testing the SMTP configuration (page 40)

Adding notification email recipients (page 39)

Chapter 4: Troubleshooting CIFS

Troubleshoot issues with SMB file acceleration

If you are experiencing issues with SMB file acceleration, the following are possible troubleshooting options to consider:

- Ensure that the traffic is being processed by the expected policy.

  Go to **Monitor > Real Time Conversations**, and select the Show Policies option. This groups the traffic by the virtual circuit and policy. Look for the desired traffic in expected policy. If the traffic is being accelerated by TCP, the background colour is yellow. If the traffic is being processed by CIFS acceleration the CIFS acceleration icon is shown.

- If a client had already established a connection with the server when the SMB acceleration service was restarted, file transfers over that connection cannot take advantage of the acceleration.

  There are two options for terminating the connection between the client computer and the server: Restart the client computer or on a MS Windows client computer, navigate to **Control Panel > Administrative Tools > Services**, and restart the Workstation service.

- Any of the Troubleshoot issues with TCP acceleration (page 43) considerations may be applicable.

You can also attempt to diagnose the issue by viewing the system log or the system diagnostics information.

- The system diagnostics for acceleration can be filtered for SMB acceleration, WAN memory, or TCP acceleration. See Acceleration Diagnostics (page 44).
- The system log file can be filtered for SMB acceleration (smbad), WAN memory (wmd), TCP acceleration (tcpad), or community (communityd). See Viewing System Log Files (page 48).

Troubleshoot issues with TCP acceleration

If you are experiencing issues with acceleration, the following are possible troubleshooting options to consider:

- Ensure that the traffic is processed by the expected policy.

  Go to the Real Time Conversations monitor and check the Show Policies option, which groups the traffic by the virtual circuit and policy. Look for the desired traffic in the expected policy. If the traffic is being accelerated by TCP, the background colour will be yellow.

- If you have a mix of 7.4, 7.0, 6.4.3, and pre-6.4.3 appliances, perhaps the Acceleration TCP Option Mode is not set correctly. Exinda had used option 30 to indicate acceleration but needed to change this when option 30 was assigned to indicate multi-path TCP. A number of choices were added to

ensure compatibility with earlier appliances. Ensure that you believe your choice is correct for your situation or choose another selection.

- If you have the Multi-Path TCP Acceleration Bypass setting enabled and and Acceleration TCP Option Mode is set to liberally use option 30, then when option 30 is encountered it will be interpreted as being multi-path TCP rather than Exinda acceleration and thus will not be accelerated. Ensure these settings are set correctly.
- If you have a backhaul scenario and you have not enabled the Dual Bridge Bypass setting, then acceleration will not work properly when the SYN from the client is not processed on the same bridge as the SYN/ACK from the server.

You can also attempt to diagnose the issue by viewing the system log or the system diagnostics information.

- The system diagnostics for acceleration can be filtered for SMB acceleration, WAN memory, or TCP acceleration. See Acceleration Diagnostics (page 44).
- The system log file can be filtered for SMB acceleration (smbad), WAN memory (wmd), TCP acceleration (tcpad), or community (communityd). See Viewing System Log Files (page 48).

Acceleration Diagnostics

Acceleration diagnostics aid in troubleshooting TCP Acceleration, SMB Acceleration and WAN Memory issues by displaying the current configuration for those areas.

- The TCP Acceleration diagnostics display the current TCP configuration settings as well as the number of new and concurrent accelerated connections and reduction statistics.
- The SMB Acceleration diagnostics display the current SMB configuration settings. If SMB signed connections are present, the total number of signed connections is also displayed.
- The WAN memory Acceleration diagnostics display the current configuration settings as well as reduction statistics for the individual hosts.

Related Tasks

Viewing TCP Acceleration Configuration and Statistics (page 44)

Viewing WAN Configuration and Statistics (page 45)

Viewing SMB Acceleration Configuration and Statistics (page 46)

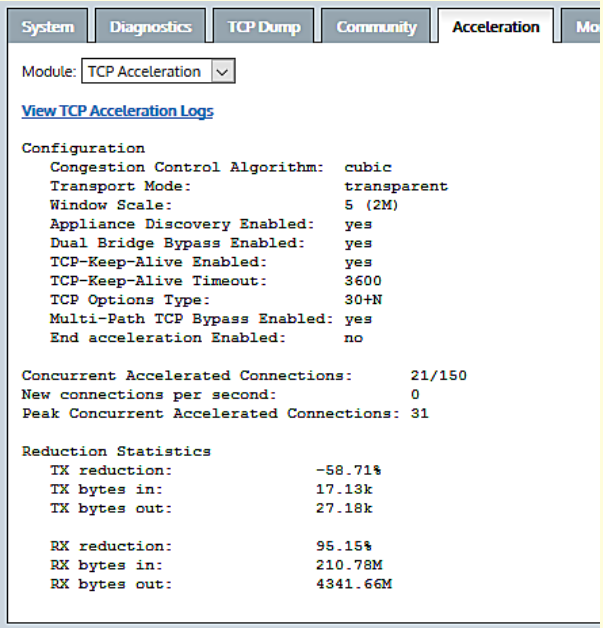
Viewing TCP Acceleration Configuration and Statistics

Use the following instructions to view the TCP acceleration configuration and current statistics.

To view TCP acceleration details

1. Go to **Configuration > System > Diagnostics > Acceleration**.
2. From the **Module** drop-down, select **TCP Acceleration**.
   The configuration settings and statistics for TCP acceleration appear.

EXAMPLE



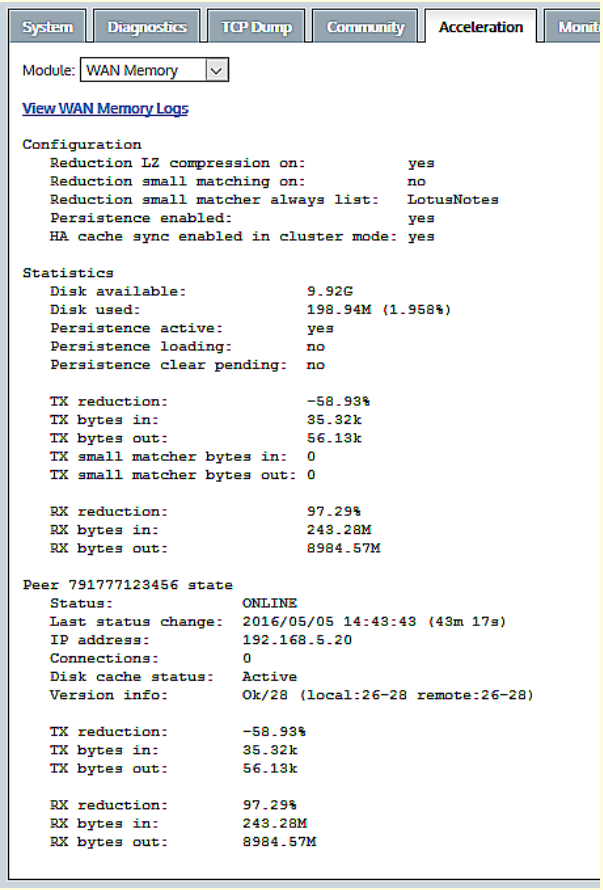
Viewing WAN Configuration and Statistics

Use the following instructions to view the WAN configuration and operational statistics.

To view the WAN memory configuration

1. Go to **Configuration > System > Diagnostics > Acceleration**.
2. From the **Module** drop-down, select **WAN Memory**
   . *The configuration settings for WAN memory acceleration appear.*

EXAMPLE



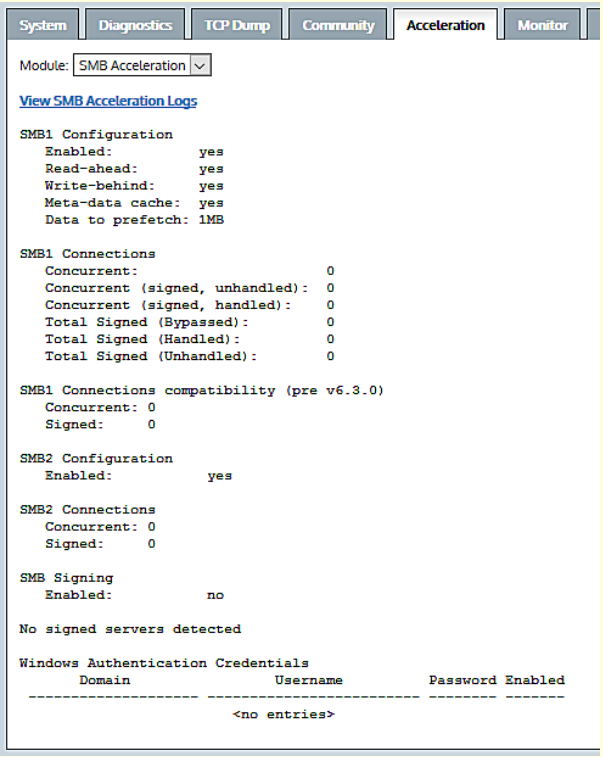
Viewing SMB Acceleration Configuration and Statistics

Use the following instructions to view the SMB acceleration configuration and the current statistics.

To view the SMB details

1. Go to **Configuration > System > Diagnostics > Acceleration**.
2. From the **Module** drop-down, select **SMB Acceleration**
   . *The configuration settings for SMB1 and SMB2 appear.*

EXAMPLE



The connections statistics are grouped into two categories:

- `Concurrent` — All signed connections from the file sharing servers that are currently connected.
- `Total Signed` — All signed connections since the SMB Acceleration service was last started, including those recorded as Concurrent.

As signed connections are processed, there are three possible results:

- `Bypassed` — The number of connections that bypass acceleration because the first time an attempt to validate the domain credentials failed, which resulted in the connection being identified as signed, but is not accelerated. All subsequent attempts to validate credentials of a signed connection against the IP address of the server are marked as `Unhandled`.
- `Handled` — The number of connections that are known to be signed and accelerated.
- `Unhandled` — The number of connections that, following a bypass state, had subsequent attempts to validate credentials of a signed connection against the IP address of the server.

Viewing System Log Files

The View Log Files page allows you to view the system log files and filter out various log messages. Log files provide an inside into the Exinda appliance's operation and aid in troubleshooting.

The following can be used to filter for particular messages:

- WAN memory — `wmd`
- TCP acceleration — `tcpad`
- SMB acceleration — `smbad`
- Community — `communityd`

To filter and navigate within the log file

1. Go to **Configuration > System > Logging > View**.
2. Select the log file to view. By default, the **Current Log** is displayed.

   The Exinda appliance periodically archives log files. These archived log files can also be viewed by selecting them from the Logfile list.
3. To filter the contents of the log file, type the criteria to filter by and click **Apply**.

   The following are examples of common filters thar reduce the reported log lines to a single type:

   - WAN memory — `wmd`
   - TCP acceleration — `tcpad`
   - SMB acceleration — `smbad`
   - Community — `communityd`
4. If there are multiple pages of log entries, to navigate to a specific page, type the page number in the **Go to Page** field and click **Go**.