


# New Search

(host="si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com" source="ids.log" sourcetype="IDS")  NOT port )

All time

✓ **260 events** (11/27/23 7:11:59.000 PM to 11/28/23 4:09:19.000 AM)

standard\_perf (search default)

No Event Sampling

Events (260)

Format Timeline

1 hour per column



## SELECTED FIELDS

*a* host 1  
*a* source 1  
*a* sourcetype 1

## INTERESTING FIELDS

# date\_hour 1  
# date\_mday 1  
# date\_minute 2  
*a* date\_month 1  
# date\_second 2  
*a* date\_wday 1  
# date\_year 1  
*a* date\_zone 1  
*a* index 1  
# linecount 2  
*a* punct 1  
*a* splunk\_server 1  
# timeendpos 1  
# timestartpos 1

+ Extract New Fields (/en-US/app  
/search  
/field\_extractor?sid=1701144559.4999)

Time

Event

Time	Event
11/27/23 7:12:00.421 PM	<p>2023-11-27 19:12:00,421 - Non-IP packet: Packet (Length: 60)</p> <p>Layer ETH</p> <p>: Destination: 08:00:27:35:44:dd Address: 08:00:27:35:44:dd .... ..0. .... = LG bit: Globally unique address (factory default)</p> <p>Show all 22 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = ids.log sourcetype = IDS</p>
11/27/23 7:12:00.420 PM	<p>2023-11-27 19:12:00,420 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = ids.log sourcetype = IDS</p>
11/27/23 7:12:00.420 PM	<p>2023-11-27 19:12:00,420 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = ids.log sourcetype = IDS</p>

Time	Event
11/27/23 7:12:00.419 PM	<p>2023-11-27 19:12:00,419 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.418 PM	<p>2023-11-27 19:12:00,418 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.418 PM	<p>2023-11-27 19:12:00,418 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>

Time	Event
11/27/23 7:12:00.417 PM	<p>2023-11-27 19:12:00,417 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.416 PM	<p>2023-11-27 19:12:00,416 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.416 PM	<p>2023-11-27 19:12:00,416 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>

Time	Event
11/27/23 7:12:00.415 PM	<p>2023-11-27 19:12:00,415 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.414 PM	<p>2023-11-27 19:12:00,414 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.414 PM	<p>2023-11-27 19:12:00,414 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>

Time	Event
11/27/23 7:12:00.413 PM	<p>2023-11-27 19:12:00,413 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.412 PM	<p>2023-11-27 19:12:00,412 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.411 PM	<p>2023-11-27 19:12:00,411 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>

Time	Event
11/27/23 7:12:00.410 PM	<p>2023-11-27 19:12:00,410 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.409 PM	<p>2023-11-27 19:12:00,409 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.409 PM	<p>2023-11-27 19:12:00,409 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>

Time	Event
11/27/23 7:12:00.408 PM	<p>2023-11-27 19:12:00,408 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>
11/27/23 7:12:00.407 PM	<p>2023-11-27 19:12:00,407 - Non-IP packet: Packet (Length: 42)</p> <p>Layer ETH</p> <p>: Destination: ff:ff:ff:ff:ff:ff Address: ff:ff:ff:ff:ff:ff .... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)</p> <p>Show all 21 lines</p> <p>host =</p> <div>si-i-071ac4b49eedf6ab8.prd-p-3gaqk.splunkcloud.com</div> <p>source = <code>ids.log</code> sourcetype = <code>IDS</code></p>