Splunk® Common Information Model Add-on Common Information Model Add-on Manual 5.3.2

Network Sessions

Generated: 6/03/2024 6:55 pm

Network Sessions

The fields in the Network Sessions data model describe Dynamic Host Configuration Protocol (DHCP) and Virtual Private Network (VPN) traffic, whether server:server or client:server, and network infrastructure inventory and topology.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Network Session event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Sessions	network
	session
|____ Session_Start	start
|____ Session_End	end
|____ DHCP	dhcp
|____ VPN	vpn

Fields for Network Sessions event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Sessions	`action`	string	The action taken by the reporting device.	Required for pytest-splunk-addon Prescribed values are:

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				• started (for VPN session starts, and DHCP lease starts) • ended (for VPN session teardowns, and DHCP lease ends) • blocked (for the VPN session disallowed start attempts, or failed DHCP leases)
All_Sessions	dest_bunit	string	The business unit of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	dest_category	string	The category of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	dest_dns	string	The domain name system address of the destination for a network session event.	recommended
All_Sessions	dest_ip	string	The internal IP address allocated to the client initializing a network session. For DHCP and VPN events, this is the IP address leased to the client.	• recommended • required for pytest-splunk-addon
All_Sessions	dest_mac	string	The internal MAC address of the network session client. For DHCP events, this is the MAC address of the client acquiring an IP address lease. For VPN events, this is the MAC address of the client initializing a network session. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	• recommended • required for pytest-splunk-addon
All_Sessions	dest_nt_host	string	The NetBIOS name of the client initializing a network session.	recommended
All_Sessions	dest_priority	string	The priority of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	duration	number	The amount of time for the completion of the network session event, in seconds.	
All_Sessions	response_time	number	The amount of time it took to receive a response in the network session event, if applicable.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Sessions	signature	string	An indication of the type of network session event.	required for pytest-splunk-addon For example: DHCPACK, DHCPNAK, DHCPRELEASE, WebVPN session started, etc2.
All_Sessions	signature_id	string	The unique identifier or event code of the event signature.	
All_Sessions	src_bunit	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	src_category	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	src_dns	string	The external domain name of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_ip	string	The IP address of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_mac	string	The MAC address of the client initializing a network session. Not applicable for DHCP events. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Sessions	src_nt_host	string	The NetBIOS name of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_priority	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
All_Sessions	user	string	The user in a network session event, where applicable. For example, a VPN session or an authenticated DHCP event.	• recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				• required for pytest-splunk-addon
All_Sessions	user_bunit	string	The business unit associated with the user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	user_category	string	The category of the user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	user_priority	string	The priority of the user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	vendor_product	string	The full name of the DHCP or DNS server involved in this event, including vendor and product name. For example, Microsoft DHCP or ISC BIND. Create this field by combining the values of the vendor and product fields, if present in the events.	recommended
DHCP	lease_duration	number	The duration of the DHCP lease, in seconds.	
DHCP	lease_scope	string	The consecutive range of possible IP addresses that the DHCP server can lease to clients on a subnet. A lease_scope typically defines a single physical subnet on your network to which DHCP services are offered.	required for pytest-splunk-addon