Vendor - Citrix

Product - Netscaler ADC

Ref	Link
Splunk Add-on	https://splunkbase.splunk.com/app/2770/
Product Manual	https://docs.citrix.com/en-us/citrix-adc/current-release/system/audit-logging-configuration-logging.html

Sourcetypes

sourcetype	notes
citrix:netscaler:syslog	None

Sourcetype and Index Configuration

key	sourcetype	index	notes
citrix_netscaler	citrix:netscaler:syslog	netfw	None

Filter type

MSG Parse: This filter parses message content

Setup and Configuration

1. Install the Splunk Add-on on the search heads) for the user communities interfaced on this data source. If CC4S is exclusively used the addon is not required on the indexer.

2. Review and update the splunk_index.csv file and set the index and sourcetype as required for this data source.

3. Follow vendor configuration steps per Product Manual above. Ensure the data format selected is [DDMYYYY]

Options

Variable	default	description
SC4S_LISTEN_CITRIX_NETSCALER_SLN_UK_TCP_PORT	empty string	Enable a TCP port for this specific vendor product using the port specific port assigned number defined
SC4S_LISTEN_CITRIX_NETSCALER_SLN_UU_UDP_PORT	empty string	Enable a UDP port for this specific vendor product using the port specific port assigned number defined
SC4S_ARCHIVE_CITRIX_NETSCALER_SLN	no	Enable archive to disk for this