

系统状态

- 审核日志, on page 1
- •系统日志, on page 3

审核日志

审核日志包含用户执行的操作的详细信息。这包括(但不限于)配置文件、规则、网关的登录/注销 活动、创建、删除、更新、启用、禁用等操作或与多云防御解决方案的配置和操作相关的任何用户 活动。

时间格式

日志可以采用 UTC(协调世界时)或本地时间格式显示。本地是指配置的用户所在的时区,例如美国/太平洋。日志的日期和时间将以 ISO 8601 格式显示(完整日期加上小时、分钟、秒和小数秒 - YYYY-MM-DD T HH:MM:SS:S)。示例: 2020-11-22T10:58:46.820

要选择或切换不同的时间格式,请点击单选按钮,如图所示:

iters and Sear	ch	Switch to Advanced	d Search	
Local 🗸	La	ast 1 Hour 🔍 🗸		
Time Format				
UTC				
			0	-

时间框架

日志可以以 15 分钟到 30 天的增量选项或自定义时间段显示。要选择或切换时间范围,请点击下拉列表并选择时间范围,如图所示:

Audit Logs

	F					
Local 🗸	Last 15 Mins	~				
	Select Time Fran	ne				
	Last 15 Mins					
Date and Time	Last 1 Hour	Last 15 Mins	Resource N	User	Role	Source
2023-07-26T14:43	Last 1 Day				ROLE_SU	
	Last 7 Days					
	Last 30 Days					
	Custom					

对于自定义时间范围,点击日历对象,然后点击保存,选择自定义、开始和结束日期或时间。

搜索过滤器

可以使用搜索功能和审核日志字段过滤日志。审核日志字段为操作类型源 IP用户网关 CSP 账户角色要过滤一个或多个字段的审核日志,请执行以下操作:

步骤1 在搜索字段中点击鼠标左键以访问下拉菜单。

Audit Logs Filters and Search Switch to Quick Filters Q Action Type Source IP **CSP** Account Gateway I User Gateway 20 (CSP Account Role . .

- 步骤2选择一个字段,例如操作。
- 步骤3 键入所需的搜索字符串,例如 DELETE。
- 步骤4根据需要向搜索条件添加其他字段。

系统日志

系统日志包含多云防御解决方案执行的操作的详细信息。这包括但不限于系统消息、网关事件、实例创建/删除以及多云防御解决方案(系统)的其他配置和操作修改。

示例:对于 Actions = "DELETE"并由用户执行且字符串包含 "steve"的过滤器,过滤条件和结果中将显示该操作。

时间格式

日志可以采用 UTC(协调世界时)或本地时间格式显示。本地是指配置的用户所在的时区,例如美国/太平洋。日志的日期和时间将以 ISO 8601 格式显示(完整日期加上小时、分钟、秒和小数秒 - YYYY-MM-DD T HH:MM:SS:S)。示例: 2020-11-22T10:58:46.820

要选择或切换不同的时间格式,请点击单选按钮,如图所示:

System Logs			
Filters and Search	Switch to Advanced	d Search	
ртс 🗸 L	ast 15 Mins 🔍 🗸		
Time Format			
итс			
Local	CSP Account	Gateway	Sev

时间框架

日志可以以 15 分钟到 30 天的增量选项或自定义时间段显示。 要选择或切换时间范围,请点击下拉列表并选择时间范围,如图所示:



对于自定义时间范围,点击日历对象,然后点击保存,选择自定义、开始和结束日期或时间。

搜索过滤器

可以使用搜索功能和系统日志字段过滤日志。

系统日志字段为 网关 CSP 账户 消息

要过滤一个或多个字段的系统日志,请执行以下操作:

步骤1 在搜索字段中点击鼠标左键以访问下拉菜单。

Filters and Search				
	Switch to Quick Filt	ers		
Q Gateway				
CSP Account Message Severity	CSP Account	Gateway	Severity	Sub Type

步骤2 选择一个字段,例如 网关。

步骤3键入所需的搜索字符串,例如 ingress。

步骤4 根据需要向搜索条件添加其他字段。

示例: 过滤网关 = "ingress" 的邮件和包含 "created" 的邮件将显示在过滤条件和结果中。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意,翻译版本仅供参考,如有任何不 一致之处,以本内容的英文版本为准。