

Table of Contents

Table of Contents	1
Приложения	2
Требования к сетевому окружению	3
Описание форматов журналов	5

Требования к сетевому окружению

Documentation: ☒

Product: UGMC

Version: 6.1.9

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (до веб-консоли UserGate Management Center)	Доступ к веб-интерфейсу управления устройством.
	TCP	8300	Входящий (до веб-консоли UserGate NGFW, подключённого к UGMC)	Доступ к веб-интерфейсу управления UG NGFW, подключённого к UGMC.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: 93.91.171.46; 178.154.221.222; - ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (от UserGate до DNS-сервера)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.entensys.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера static.entensys.com.
Репликация настроек	TCP	4369	Входящий (с первого узла кластера на второй и последующие узлы)	Сервис, необходимый для работы кластера конфигурации. Установка управляющего соединения.
		9000-9100	Входящий (приём конфигурации от первого узла кластера)	Передача информации об изменении конфигурации кластера (реплика настроек)
Сервис UserGate Management Center	TCP	9712	Входящий (к UGMC от NGFW)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств и сервера UserGate Management Center.
		2022	Входящий (к UGMC от NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Контроль конечных устройств (начиная с версии 7.1.0)	TCP	9712	Входящий (к UGMC от UG Client)	Первоначальная установка связи и обмен ключами шифрования управляемых устройств UserGate Client и сервера UserGate Management Center.
		4045	Входящий (к UGMC от UG Client)	Построение SSL-туннеля для обмена данными с помощью ключей, полученных при установке связи.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
		22000-22711	Входящий (к UGMC от UG Client)	Передача журналов и телеметрии с UG Client на UG LogAn транзитом через UGMC.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
SNMP	UDP	161	Входящий (до UserGate)	Доступ к серверу UserGate по протоколу SNMP.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.
FTP (экспорт журналов) (начиная с версии 7.1.0)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов) (начиная с версии 7.1.0)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов) (начиная с версии 7.1.0)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.
Ручная проверка сайтов по категориям	TCP	80/443	Исходящий (до updates.usergate.com)	Ручная проверка сайтов по категориям.

Documentation: ☒
Product: UGMC
Version: 6.1.9

Формат журнала событий

CEF

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 0 — информационные. • 6 — предупреждения. • 8 — ошибки. • 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einsonstal
	suser	Имя пользователя.	Administrator (Admin)
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	administrator_login
	src	IPv4-адрес источника.	192.168.117.254
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"login":"ex_admin","realm_id":"31d8fcb6-e51d-4e3f-b799-181d31a45b06"}

JSON

Название поля	Описание	Пример значения
user	Имя пользователя.	Admin

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4-адрес источника события.	192.168.174.134
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einsonstal
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth

