SP5000 «Антифрод»

Руководство администратора

АО «Искра Технологии»
2023 г.

Документ выпущен компанией

АО «Искра Технологии»

РФ, 620066 Екатеринбург, ул. Комвузовская, 9-а

Т +7 343 210 69 51
Ф +7 343 341 52 40

Оглавление

1. О документе

В настоящем руководстве описаны основные действия и возможности настройки системы пользователями, обладающих ролью Администратора SP5000 «Антифрод».

Перед началом эксплуатации Системы пользователю необходимо ознакомиться с настоящим руководством.

1. Процесс настройки продукта

1.1. Проверка состояния сервиса

После установки пакета можно проверить состояние сервиса УВр:

```
sysadmin@deb10dvd1:~$ systemctl status aa6511
● aa6511.service - AA6511AX Network Element service
   Loaded: loaded (/etc/systemd/system/aa6511.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2023-07-19 10:28:36 +05; 3h 5min ago
 Main PID: 446 (aa6511_cfc)
    Tasks: 6 (limit: 4698)
   Memory: 17.6M
   CGroup: /system.slice/aa6511.service
           └─446 /opt/aa6511/bin/aa6511_cfc
```

Если был получен корректный ответ о состоянии сервиса (пример выше), переходим к пункту 1.2 текущего документа.

1.2. Внесение изменений в основной файл конфигурации УВр

После проверки состояния сервиса УВр необходимо внести изменения в основной файл конфигурации. Файлы конфигурации расположены в /etc/aa6511.

config.json - основной файл конфигурации.

```
{
  "log_params" : { // Настройки логирования
    "log_level": "VRB",
    "log_file_limits" : {
      "max_file_cnt": 1000,
      "max_line_cnt": 100000
    }
  },
  "sn" : [{ // Список станций
    "sn_id" : 199,
    "sn_name" : "iutce199",
    "sn_li_ip_addr" : "192.168.101.199",
    "sn_li_port" : 9907,
    "sn_timeout_s" : 400,
    "dicon_log_mode" : 0 // 0 - separate log off, 1 - separate log on with all
conversions, 2 - separate log on with only unsuccessful conversions
  }],
  "sn_phase_dicon": [  // Список диконов
     {
       "sn_id": 199,
       "rules": [
```

```
          {"sn_pfx": "34320222", "sn_nr_type": 4, "mc_pfx": "900", "mc_nr_type": 1}
        ]
     }
  ],
  "antifraud_in_trunk": [ // Список входящих транков вызова с которых нужно
верифицировать
    {
      "sn_id" : 199,
      "tgrp_id" : 229,
      "src_operator_id" : 10229, // Идентификатор оператора с которого приходят вызова в
данном транке
      "dst_operator_id" : 10199  // Идентификатор нашего оператора (оператора к которому
принадлежит данный sn_id)
    }
  ],
  "antifraud_out_trunk": [ // Список исходящих транков на вызова по которым к нам может
прийти запрос верификации
    {
      "sn_id" : 199,
      "tgrp_id" : 229,
      "src_operator_id" : 10199, // Идентификатор нашего оператора (оператора к которому
принадлежит данный sn_id)
      "dst_operator_id" : 10229 // Идентификатор оператора на которого уходят вызова в
данном транке
    }
  ]
}
```

1.3. Внесение изменений в файл конфигурации УВр для взаимодействия с другими компонентами ИС Антифрод

После внесения изменений в основной файл конфигурации необходимо откорректировать файл конфигурации для взаимодействия с другими компонентами ИС Антифрод.

vfn_config.json – в файле конфигурации задаются параметры взаимодействия с другими компонентами ИС Антифрод.

В этом конфигурационном файле нас интересуют параметры: **vfn:id** и **ccn:ipAddress, ccn:sft user**. Все остальное как правило менять не нужно.

```
{
    "vfn" : {
        "id": 199, // Здесь нужно указать идентификатор нашего узла верификации
        "privateKeyPath": "/opt/vfn/key/private512.pem"
    },
    "ccngw" : {
        "database" : {
            "numbers": "/opt/vfn/numbers",
```

```
        "nodes": "/opt/vfn/nodes",
        "pub": "/opt/vfn/pub",
        "connections": {
            "requests": "/opt/vfn/connections/requests",
            "responses": "/opt/vfn/connections/responses"
        }
    },
    "pm_jobs" : [
        "call_statistics"
    ]
},
"vfgw" : {
    "http" : {
        "local port" : "8081",
        "remote port" : "8081",
        "encrypted" : true,
        "connect timeout" : {
            "period" : {
                "unit" : "msec",
                "value" : 50
            }
        }
    }
},
"ccn" : {
    "ipAddress" : "192.168.143.203", // IP адрес SFTP сервера ЦУ
    "sftp user" : "node_199", // Имя пользователя имеет вид node_<vfn_id>
    "reports" : {
        "incidents" : "/incidents",
        "incidents_a" : "/incidents_a",
        "statistics" : "/statistics"
    },
    "database" : {
        "numbers" : "/numbers",
        "nodes" : "/nodes",
        "pub" : "/pub",
        "connections" : {
            "requests" : "/requests",
            "responses" : "/responses"
        }
    }
},
"timers" : {
    "getIncidentReq" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        }
```

```
    },
    "getIncidentAReq" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        }
    },
    "refreshNumbersInfo" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        }
    },
    "refreshNodesInfo" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        }
    },
    "refreshCallInfoRequests" : {
        "period" : {
            "unit" : "sec",
            "value" : 60
        }
    },
    "refreshPublicKeys" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        }
    }
},
"pm_jobs" : {
    "call_statistics" : {
        "period" : {
            "unit" : "sec",
            "value" : 900
        },
        "counters" : [
            [
                "ATTMS",
                "all"
            ],
            [
                "TBVRF",
                "all"
            ],
            [
```

```
                "RJCTS",
                "all"
            ],
            [
                "ERR1",
                "all"
            ],
            [
                "ERR2",
                "all"
            ]
        ]
    }
  }
}
```

1.4. Подключение к SFTP Центрального Узла ИС Антифрод

После внесения изменений в файлы конфигурации необходимо организовать подключение к SFTP Центрального Узла ИС Антифрод.

Для того чтобы работало подключение к SFTP Центрального Узла ИС Антифрод, необходимо добавить публичный ключ **/home/aa6511/.ssh/id_rsa.pub** в список разрешенных на SFTP сервер. Обычно это файл **/home/sftp-user/.ssh/authorized_keys**

После этого проверяем соединение с SFTP с помощью команды:

```
sysadmin@deb10dvd5:~$ sudo su
[sudo] password for sysadmin:
root@deb10dvd5:/home/sysadmin# su aa6511 -s /bin/bash
aa6511@deb10dvd5:/home/sysadmin$ sftp node_107@10.99.2.24
Connected to node_107@10.99.2.24.
sftp>
```

ВАЖНО!

После установки пакета УВр будет автоматически сгенерирован ключ шифрования для соединений с другими УВз и УВр. Он находится в **/opt/vfn/key**. Публичный ключ (**public512.crt**) нужно положить в папку **pub** на SFTP но с именем вида **node-<vfn:id> -key.pub**