

# Product Architecture

## Conteúdos

Introdução .....	2
<b>Ambiente</b> .....	2
Redes de Trabalho .....	2
Configurações .....	2
Políticas .....	2
Servidores .....	2
<b>Componentes</b> .....	2
Agente .....	2
Servidor .....	3
Base de Dados .....	3
Console .....	3
<b>Comunicação</b> .....	4
Console – Servidor .....	4
Console – Base de Dados .....	4
Servidor – Base de Dados .....	4
Servidor principal – Servidor secundário .....	4
Servidor – Agente .....	4
<b>Políticas de gerenciamento</b> .....	4
Administração .....	4
Armazenamento .....	5
Distribuição .....	5
Aplicação .....	5
<b>Gerenciamento de Cadastro</b> .....	5
<b>Segurança</b> .....	5
Agente de segurança .....	5
Segurança de Comunicação .....	5
Segurança de Administração .....	5
Balanceamento de Carga e Disponibilidade .....	5
<b>Atualizações</b> .....	6
Consumo e dimensão dos Recursos .....	6
Agentes .....	6
Servidores .....	6
Arquitetura para um único servidor .....	6
Arquitetura para muitos servidores .....	6
Maquinas virtuais .....	6
Bases de Dados .....	7
<b>Integração com software de terceiros</b> .....	7
Distribuição .....	7
Administração .....	7
Relatórios .....	7
<b>Apêndice – Consumo de Banda para os Principais Operadores</b> .....	8

**Aranda 360 ENDPOINT SECURITY** é uma solução complementar as aplicações de antivírus existentes na atualidade. A360 é uma ferramenta de tipo modular de distribuição (enterprise grade architecture solution) e oferece as características de software de segurança requeridas por qualquer organização, bloqueando os diferentes tipos de ataques ou atividades suspeitas, que um antivírus normal não pode deter.

## Ambiente

Para compreender a arquitetura desta aplicação, você deve conhecer o conceito de “ambiente”. Em Aranda 360 ENDPOINT SECURITY um ambiente é o conjunto de redes de trabalho, configurações, políticas e servidores.

### Redes de Trabalho

Las redes de trabalho têm grupos de estações de trabalho, que são homogêneas para o uso de políticas de segurança. As redes de trabalho estão definidas por parâmetros, como o nome da máquina, sub-redes, endereços IP, ou uma unidade do diretório ativo da organização. Estas podem ser associadas a diferentes políticas, baseadas num contexto específico.

### Configurações

As configurações de agentes fazem possível a definição de três aspectos principais:

- Agentes que se conectam num servidor (este processo se desenvolve usando testes).
- Decisão de ativar ou não o modo de advertência (este notifica violação de regras sem bloqueio do sistema)
- Configuração e aprendizagem de parâmetros usados para analisar o comportamento das estações de trabalho.

### Políticas

As políticas são parâmetros que definem o nível de segurança para todos os aspectos das estações de trabalho. As políticas são implementadas de forma dinâmica por os agentes, dependendo do uso real da estação de trabalho.

### Servidores

Os servidores de Aranda 360 ENDPOINT SECURITY permitem o gerenciamento das redes de trabalho e de suas políticas associadas.

## Componentes

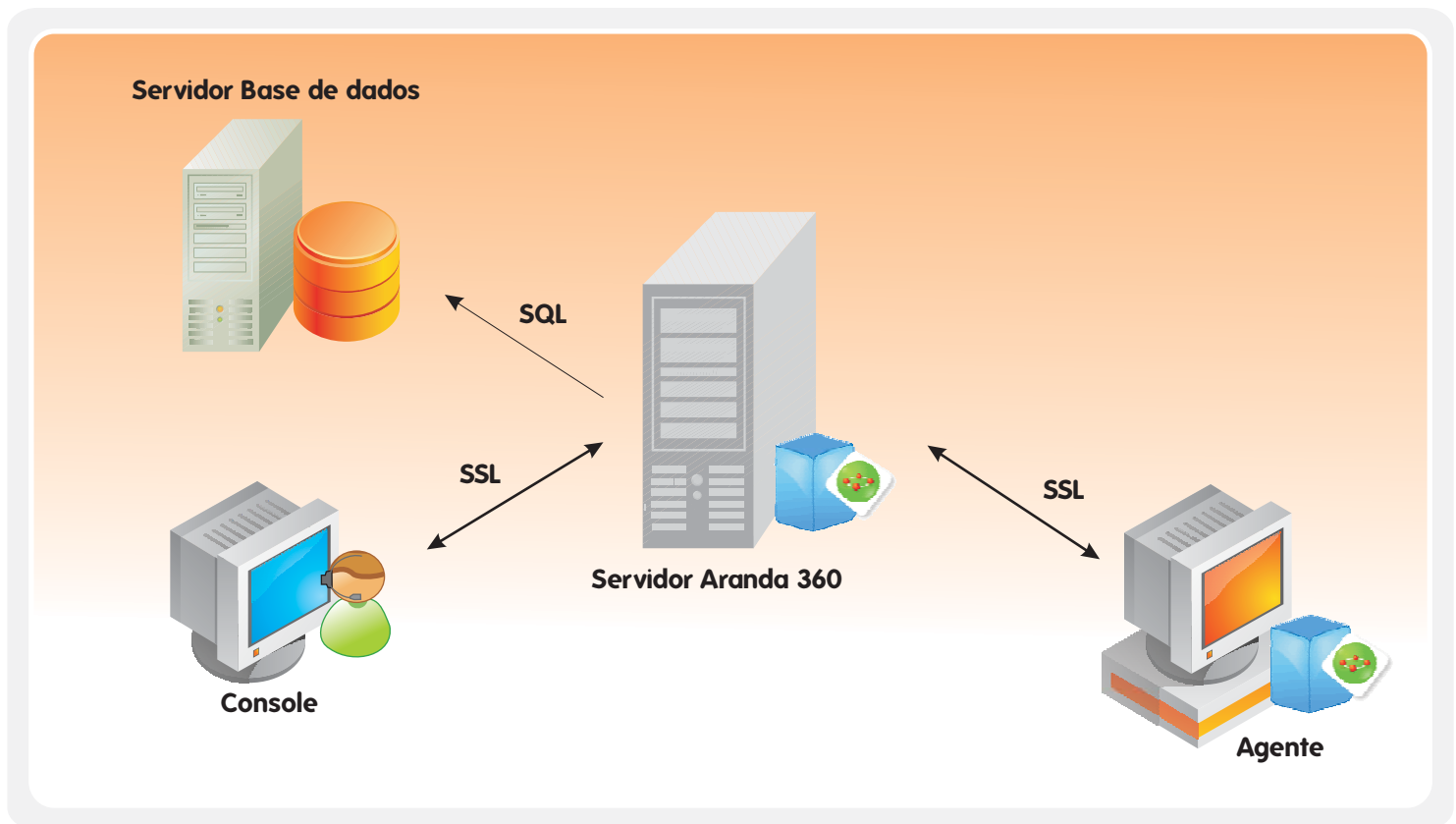
Aranda 360 ENDPOINT SECURITY é constituído por agentes instalados nas estações de trabalho, um ou mais servidores que administram os agentes, uma ou mais consoles de administração e uma base de dados que armazena os eventos de registro dos agentes, assim como a informação que Aranda 360 ENDPOINT SECURITY necessita executar.

### Agente

O agente reside na estação de trabalho e é um componente fundamental de Aranda 360 ENDPOINT SECURITY; o agente se carrega na memória, quando o Sistema Operacional Windows se inicia. A função do agente consiste na recuperação e armazenamento local de suas políticas quando está conectado ao servidor. De igual maneira, se encarrega de implementar as políticas de acordo com os resultados dos testes independentemente de se o agente esta ou não conectado ao servidor.

O agente se encarrega de proteger a estação de trabalho considerando três aspectos fundamentais: aplicação, sistema e rede de trabalho. Quando um evento infringe as políticas de segurança, o agente reage imediatamente; desta maneira, bloqueia uma operação perigosa ou inclui um evento no registro. O registro é enviado ao servidor, se o agente este conectado á rede da sua companhia; em outro caso, o registro pode ser armazenado temporalmente e transmitido quando uma conexão se estabeleça.

O administrador pode escolher quais eventos específicos se converteram numa notificação de usuário. Essas notificações poderão se ver numa janela de ajuda automática (pop-up).



### Servidor

O servidor está no centro da arquitetura do Aranda 360 ENDPOINT SECURITY; sua função é ativar os ambientes previamente configurados na console de gestão. Por conseguinte se pode gerenciar a comunicação e supervisionar o agente; adicionalmente, o servidor recebe os registros de eventos provenientes dos agentes e armazená-los na base de dados. Aranda 360 ENDPOINT SECURITY requiere como mínimo um servidor Principal-mestre (master Server) para cada ambiente. No obstante, servidores Secundários-escravos (slave servers) podem ser usados, para proporcionar um balanceamento de carga e gerar maior acessibilidade.

O servidor mestre se comunica com a console de gestão; este compartilha a rede de trabalho e a informação sobre as políticas de segurança com os servidores escravos.

Finalmente, se deve dizer que vários servidores principais podem ser definidos para um ambiente, para distribuir a comunicação de agentes entre servidores específicos, baseados na topologia da rede corporativa.

### Base de Dados

As bases de dados do Aranda 360 ENDPOINT SECURITY estão no servidor da tecnologia Microsoft SQL. Embora o A360 se instale por padrão com o motor de Microsoft MSDE. Durante a implementação do Aranda 360 ENDPOINT SECURITY, Aranda Software recomenda utilizar uma versão comercial do servidor Microsoft SQL, porque este não tem limitações de tamanho e possuem elementos de administração completos que não estão disponíveis com MSDE. A base de dados armazena as configurações do agente e as políticas de segurança junto com os registros das estações de trabalho. O administrador, porém pode armazenar esta informação em bases de dados separadas.

### Console

A console de gestão é uma ferramenta de administração do Aranda 360 ENDPOINT SECURITY. Esta console está baseada em tecnologia .Net e pode ser usada em qualquer estação Windows (Win32). A console de gestão pode ser instalada na mesma máquina de instalação da ferramenta, ou pode ser usada nos modos monousuário ou multi-usuário.

## Comunicação

A comunicação entre os diferentes módulos de Aranda 360 ENDPOINT SECURITY permite compreender o funcionamento desta solução e também é uma aplicação confiável com baixo consumo de banda.

### Console – Servidor

A console se comunica com o servidor, quando necessita implementar as políticas de segurança, ou quando necessita consultar os servidores para verificar o estado dos agentes. A console se conecta com o servidor mediante um TCP criptografado, usando o protocolo SSL v3, da porta A16007.

### Console – Base de dados

Durante os processos de atualização ou eliminação de políticas de software, a console se comunica com a base de dados. Esta situação também se apresenta durante as consultas aos registros. A console se conecta à base de dados mediante uma conexão SQL TCP na porta 1433 (configurável).

### Servidor – Base de dados

O servidor Aranda 360 ENDPOINT SECURITY se conecta à base de dados para armazenar mensagens mediante uma conexão TCP na porta 1433 (configurável).

### Servidor Principal (mestre) – Servidor Secundário (escravo)

As conexões entre os servidores mestres e escravos permitem a sincronização do ambiente da ferramenta. Os servidores escravos se encontram em comunicação com o servidor mestre mediante uma conexão TCP na porta 16003.

### Servidor – Agente

Os agentes se comunicam com o servidor para receber suas configurações e as políticas de segurança associadas com as estações de trabalho, assim como para enviar os arquivos de registro para o servidor. O servidor e o agente se comunicam mediante uma conexão SSL v3 na porta 16005.

Para poder gerenciar conexões de muitos agentes sem necessidade de sobrecarregar a rede de trabalho, o servidor utiliza um sistema de tokens. Usando a porta 16006 para escutar os dois lados, este sistema permite o controle de vários agentes que estão conectados simultaneamente ao servidor. Se o agente não pode conectar-se ao servidor mestre, pode-se conectar a um outro servidor existente nesta configuração.

## Políticas de Gerenciamento

As políticas estão constituídas por parâmetros que definem o nível de segurança para todos os aspectos da estação de trabalho. As políticas se aplicam de forma dinâmica pelos agentes, e são geradas conforme ao contexto de uso de cada estação.

### Administração

As políticas se definem com a ajuda do editor de políticas da console. As políticas podem ser definidas para um ambiente especial, ou podem ser compartilhadas por todos os ambientes. As políticas se aplicam as redes, quer dizer, um grupo de agentes; porém, sua implementação pode ser impactada por o estado do ponto final (endpoint), o ambiente da rede, ou a informação recuperada por o diretório ativo.

Ejemplos:

- Aplicações autorizadas para abrir um tipo de arquivo, assim como para criar ou modificar arquivos num diretório específico.
- Aplicações implementadas, somente se o ponto final está conectado a rede de trabalho corporativa.
- Conexões Wifi (wireless fidelity) limitadas aos pontos de acesso específico, ou com acesso aos pontos que usam sistemas de criptografia muito fortes, como o WPA.
- Dispositivos de armazenamento removíveis como o USB, ou o Firmware, limitados aos modelos específicos, às senhas específicas ou aos números de serial.

## Armazenamento

As políticas são armazenadas junto com o ambiente na base de dados. Por isso, as políticas são comuns aos servidores que têm o mesmo ambiente. No agente as políticas são armazenadas localmente em arquivos protegidos por Aranda 360 ENDPOINT SECURITY e por isso não são acessíveis pelo usuário.

## Distribuição

As políticas são distribuídas pelos servidores aos agentes. Os servidores também se encarregam de verificar o estado dos agentes antes de descarregar neles as políticas. Após isso, o servidor volta à sua política de estado ativo, e ao mesmo tempo o agente carrega a política que vai ser implementada.

## Aplicação

As políticas aplicadas pelo agente não podem ser modificadas pelo usuário, independentemente de seus privilégios de administrador local.

## Gerenciamento de Cadastro

Toda vez que o agente detecta um evento, gera automaticamente um registro. Se a estação de trabalho não é conectada à rede, os eventos são armazenados localmente pelo agente. Quando o agente é conectado à rede, os eventos se enviarão ao servidor, e este se encarregará de armazenar-los na base de dados de cadastro.

A console de gestão de Aranda 360 ENDPOINT SECURITY permite o acesso aos registros de eventos, assim como ao sistema por filtro, reportando os eventos de acordo com sua urgência e severidade.

## Segurança

Aranda 360 ENDPOINT SECURITY protege o sistema contra ataques, usos desfavoráveis, ou tentativas de desativar esta ferramenta. O servidor de A360 se conecta num serviço automático de descrição certificada, hospedado neste servidor (na porta HTTPS), cuja função é certificar aos agentes durante a implementação. Desta forma, as conexões futuras entre os agentes e o servidor estarão sujeitas num estrito procedimento de autenticação para atingir a proteção do sistema.

### Agente de segurança

O administrador define as ações que o usuário pode implementar sobre o agente. Neste caso se pode definir se o usuário é ou não autorizado para deter o agente, e se este pode ou não desinstalar o serviço de A360, independentemente de seus privilégios locais ou administrativos para uma estação de trabalho.

O agente pode ser parado temporariamente por o usuário somente se tem uma autorização do administrador; para esse caso, o administrador proporciona ao usuário uma senha para ser usada uma vez (depois de trocar as senhas de autenticação off line). Posteriormente, o agente protege automaticamente seus arquivos. Quando A360 é instalado numa estação de trabalho, esta aplicação não pode ser modificada ou eliminada do sistema.

### Segurança de Comunicação

As comunicações entre servidores, agentes e consoles estão baseadas no protocolo SSL v3. Cada componente tem seu certificado X509 v3. Cada agente tem um único certificado que permite a identificação da máquina, eliminando a possibilidade de fraude ou clonagem. O agente é conectado à companhia com base neste certificado. Isto significa que o agente Aranda 360 ENDPOINT SECURITY da companhia "X" não pode ser conectado num servidor da companhia "Y" e por isso não poderá carregar nem implementar suas políticas.

### Segurança de Administração

Os direitos de administração de Aranda 360 ENDPOINT SECURITY podem-se gerenciar considerando o ambiente e os conceitos de função desta ferramenta. Cada administrador é associado com uma função, que tem operações autorizadas, assim como por um ou mais ambientes onde o administrador tem o direito de executar estas operações.

Por exemplo, um administrador pode ter direito de atribuir políticas num ambiente, sem a necessidade de modificar-las.

### Balanceamento de Carga e Disponibilidade

Aranda 360 ENDPOINT SECURITY tem uma arquitetura modular (enterprise grade architecture) com capacidade de expansão de acordo com os requerimentos do momento. A solução gerencia grande número de agentes da mesma organização.

Para garantir o desempenho e disponibilidade desta aplicação, os servidores desta solução oferecem as seguintes características:

- Balanceamento de carga: no caso de sobrecarga do servidor, outro servidor se encarrega de gerenciar seus agentes.
- Disponibilidade: no caso de falhas no servidor mestre, um servidor escravo pode assumir a responsabilidade de suas funções. Os agentes podem se conectar a qualquer outro servidor configurado no ambiente, se o servidor mestre não estiver disponível.

## Atualizações

As atualizações de produtos se fazem para renovar arquivos num repertório acessível pelos servidores de A360. É possível estabelecer parâmetros, de tal maneira que as atualizações se programem automaticamente, que é útil para uma arquitetura de muitos servidores.

Normalmente o servidor verifica as atualizações. O administrador pode definir uma frequência de verificação, assim como a implementação de um modo de recuperação específica (ftp, http, manual). Depois que os arquivos são recuperados, e o servidor é atualizado, se inicia a atualização automática do agente. Os intercâmbios com os agentes da versão n-1 serão mantidos até que a atualização esteja completa.

Quando uma nova versão de Aranda 360 ENDPOINT SECURITY está disponível, o servidor notifica os agentes. Os arquivos são baixados e armazenados localmente, enquanto isso, os agentes continuam funcionando. Para economizar o consumo de banda, as atualizações se abaixam usando fluxos de dados.

A versão atualizada estará vigente a partir do seguinte reinício do agente. Se a atualização tem uma versão anterior o agente atualizado continuará usando a mesma política. Contudo, se a atualização é uma versão atual, o agente carregará a política mais recente desde o servidor.

O administrador atualiza a console de gestão usando o comando "Procurar Atualizações". Se uma atualização da base de dados esquemática necessita ser aplicada, o administrador pode aplicar o serviço empregado para instalar a base de dados (acessível desde a console da estação).

## Consumo e dimensionamento dos Recursos

### Agentes

O agente de Aranda 360 ENDPOINT SECURITY necessita poucos recursos do equipamento. Num processador Pentium II 400 MHz, esta aplicação usa menos de 1% em condições normais, e um 2% no máximo, se for requerido. Adicionalmente, A360 requiere menos de 20 MB de memória para leitura e escritura.

### Servidores

#### Arquitetura para um único servidor

Esta arquitetura é desenhada para companhias pequenas ou de tamanho meio. O servidor de Aranda 360 ENDPOINT SECURITY se conecta num máximo de 300 agentes em sua "Standard Edition" e pode manejar milhes de agentes em sua "Enterprise Edition".

#### Arquitetura para muitos servidores

Para este tipo de arquitetura cada servidor Aranda 360 ENDPOINT SECURITY maneja milhes de agentes. Desta maneira se devem considerar os componentes e as funções do servidor: frequência de comunicação com os agentes, número de redes criadas, banda disponível, e quantidade de registros transmitidos.

A implementação de servidores escravos gera um balance de carga e facilita o desempenho e confiabilidade da ferramenta.

### **Máquinas virtuais**

Os servidores Aranda 360 ENDPOINT SECURITY podem ser instalados em Windows ou em máquinas virtuais.

### **Bases de Dados**

Para começar a base de dados requer 2 MB de espaço em disco para armazenar os dados do Aranda 360 ENDPOINT SECURITY, além do espaço adicional para o armazenamento dos registros. Este espaço pode variar de acordo ao número de agentes e os registros que serão armazenados.

## **Integração com software de terceiros**

Devido a sua arquitetura aberta, e ao uso de tecnologias padrão tais como .Net e SQL. Aranda 360 ENDPOINT SECURITY integra-se com ambientes administrativos previamente criados e configurados, sem a necessidade de criar trabalho adicional para as equipes técnicas das organizações.

### **Distribuição**

A distribuição do agente Aranda 360 ENDPOINT SECURITY se desenvolve com as ferramentas de distribuição de software comuns, como qualquer aplicação de Windows, sem necessidade da intervenção do usuário. Também, o agente pode ser instalado numa imagem principal (master image).

Depois de sua distribuição, o agente entra em vigor a partir do seguinte reinício da estação de trabalho. Após este processo o agente conecte-se ao servidor de autenticação incluso no servidor do A360, para obter seu certificado. O agente não operará até que não tenha uma permissão.

### **Administração**

O Aranda 360 ENDPOINT SECURITY tem uma interface de verificação de registros, mas pode transmitir os registros do agente para sistemas Syslogtype. O servidor A360 pode filtrar eventos do cadastro, para transferir os eventos de alta prioridade. Estas interações combinadas com as políticas de segurança sincronizadas, não permitirão a sobrecarga das operações.

### **Relatórios**

A base de dados de Aranda 360 ENDPOINT SECURITY utiliza tecnologia Microsoft SQL. Os modelos de dados e diagramas de informação estão disponíveis e podem ser aproveitados para tomar decisões de terceiros, como por exemplo: objetos de negócios ou software SAS para processos de análise e relatórios.

## Apêndice – Utilização de Banda para os Principais Operadores

<p><b>Envio de Política desde a Console de Administração até o Servidor Mestre</b> Medido desde o Ponto de Vista do Servidor</p> <p>Servidor configurado com cinco redes, cada uma delas com política de teste e uma configuração contextual de teste.</p>	<p><b>Duração</b></p> <p>1.5 a 2s</p>	<p><b>Média de Tráfego</b></p> <p>~ 100 Kbytes/s</p>
--	---------------------------------------	--

<p><b>Comunicação entre o servidor e os agentes</b> Medido desde o Ponto de Vista do Servidor</p> <p>Intercâmbio de Tokens entre o agente e o servidor (intervalo de 120s) A média de tráfego é armazenada</p> <p>Envio de política vazia desde o servidor para os agentes.</p> <p>Envio de registros do agente para o servidor mestre A média de tráfego é armazenada</p>	<p><b>Duração</b></p> <p>1.5 a 2s</p> <p>~2,5s</p> <p>&lt;1s</p>	<p><b>Tráfego Entrante</b></p> <p>~1 Kbytes 8.8 o/s</p> <p>~10 Kbytes</p> <p>~1 Kbytes ~8.5 o/s</p>	<p><b>Tráfego Saindo</b></p> <p>~1 Kbytes 8.65 o/s</p> <p>~9 Kbytes</p> <p>~1 Kbytes ~8.5 o/s</p>
--	--	---	---

<p><b>Comunicação entre o Servidor e a Base de Dados</b> Medido desde o Ponto de Vista do Servidor</p> <p>Envio de registros desde o Servidor para a Base de Dados A média de tráfego é armazenada</p>	<p><b>Duração</b></p> <p>&gt;3s</p>	<p><b>Tráfego Saindo</b></p> <p>~500 Kbytes * 4 Kbytes /s</p>
--	-------------------------------------	---

\* Resultados conseguidos, enquanto se geram entre 5 e 10 alarmes por segundo.

<p><b>Sincronização entre os Servidores Mestre e Escravo</b> Medido desde o ponto de vista do Servidor Escravo</p> <p>Sincronização entre os servidores mestre e escravo (intervalo de 30s)</p> <p>A média de tráfego é armazenada</p> <p>Atualização do servidor escravo</p>	<p><b>Duração</b></p> <p>1s a 3s</p> <p>&gt; 1s</p>	<p><b>Tráfego Entrante</b></p> <p>~180</p> <p>6 o/s</p> <p>~214 Kbytes</p>	<p><b>Tráfego Saindo</b></p> <p>165 o</p> <p>5,5 o/s</p> <p>~19 Kbytes</p>
---	---	--	--

<p><b>Comunicação entre a Console e a Base de dados</b> Medido desde o ponto de vista da Console de gerenciamento</p> <p>Conexão da console de gerenciamento á base de dados, para visualizar os registros.</p>	<p><b>Duração</b></p> <p>&gt; 1s</p>	<p><b>Tráfego Entrante</b></p> <p>~ 26 Kbytes por 65000 alertas</p>	<p><b>Tráfego Saindo</b></p> <p>~1.4 Kbytes</p>
---	--------------------------------------	---	---

<b>Verificação de Agentes desde a Console de Gerenciamento</b> Medido desde o ponto de vista da Console	<b>Duração</b>	<b>Tráfego Entrante</b>	<b>Tráfego Saindo</b>
Verificação do agente (intervalo de 30s)  A média de tráfego é armazenada	~1s	~3.2Kbytes  0.11Kbytes /s	~2.1Kbytes  .07 Kbytes /s
Verificação dos agentes (intervalo de 30s)  A média de tráfego é armazenada	~1s  <1s	~3.5 Kbytes  0.11 Kbytes /s	~2.1 Kbytes  0.07 Kbytes /s