McAfee Agent Handler

McAfee®

Contents

Introducing Agent Handlers

The ePolicy Orchestrator (ePO) 4.5 server separated out the services of the server dealing with agent requests, and added management logic to allow deployment of instances of these services. This new component of the ePO infrastructure has been termed an **Agent Handler**.

In ePO 4.0 and previous, there was a single ePO server that agents could connect to and receive policy and task updates. Since the ePO server was responsible for handling every agent connecting to it, there was a limitation on the deployment size an ePO server could handle. The only option to increase the scalability of a single ePO server was by moving the database out. Otherwise the ePO server could be scaled vertically (through bigger and faster hardware) instead of horizontally (through more servers to distribute the load). The introduction of Agent Handlers in 4.5 gives customers the ability to grow their logical ePO infrastructure horizontally adding multiple Agent Handlers to scale agent connectivity.

Contents

ePO architecture overview

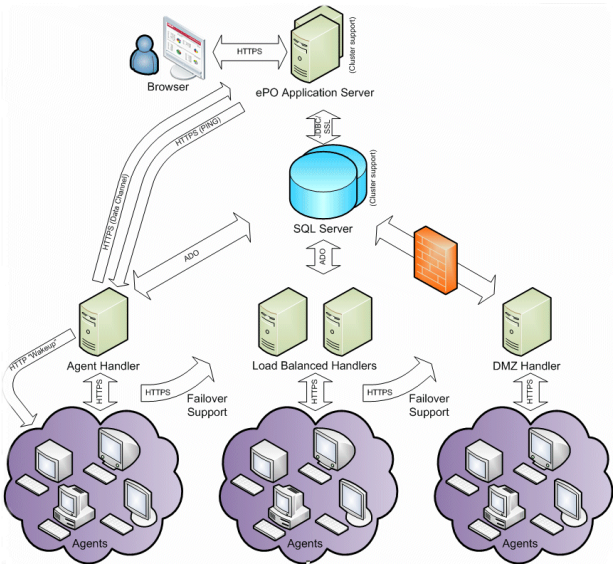

Figure 1: An ePO 4.5 deployment

A mid-range server hardware is cheaper than high-end servers. The use of Agent Handlers helps to scale more cost effectively to larger ePO installations without breaking an organization up and using multiple ePO servers.

Since Agent Handlers can be added as needed, they allow the ePO deployment to grow with the company.

Reasons for choosing to deploy multiple Agent Handlers include:

- Scalability — if your ePO server is overloaded handling your agent request volume.
- Failover — if you want to allow agents to fail over between multiple physical devices, and do not want to cluster the ePO server.
- Topology — if you need to manage systems behind a NAT, or in an external network, so long as the agent handler can continue to have a high bandwidth connection to the central database.

The introduction of Agent Handlers in conjunction with the new version of the McAfee Agent (4.5) allows fault tolerance of the overall ePO infrastructure to the loss of one or more Agent Handlers. McAfee Agent 4.5 can be configured with a fallback list of agent handlers. If the highest priority handler is not reachable, the agent will fail back through its prioritized list until it is able to contact an Agent Handler.

This white paper will describe Agent Handlers and some considerations when planning to deploy multiple agent handlers.

Agent Handler basics

Agent Handlers co-ordinate work between themselves, and the application server communicates with remote agent handlers. A work queue in the database is used as the primary communication mechanism. Agent handlers check the work queue frequently (approximately every ten seconds) and perform the requested action. Typical actions include agent wake-ups, deployments, and data channel messages. This is one of the reasons that each agent handler needs a relatively high speed, low latency connection to the database.

Services

There are three services running in any ePO 4.0 installation. These can be located at **Start** | **Run** | **Services.msc**:

- Application Server (MCAFEETOMCATSRV)
- Apache Server (MCAFEEAPACHESRV)
- Event Parser (MCAFEEEVENTPARSERSRV)

The Apache Server and Event Parser are responsible for communicating with McAfee Agent. These two services work in conjunction to receive updated events and properties from the agents, and send updated policies and tasks as assigned by administrators in the ePO console.

The Application Server (Tomcat) hosts the UI and server task scheduler.

Install Types

In ePO 4.5, the primary ePO server installation includes all three services, for example both Apache and Tomcat. There is only one primary ePO server in a logical ePO server.

An Agent Handler installation includes only the Server (Apache) and Event Parser services. A small number of Agent Handlers can be deployed on separate hardware and co-exist within a single logical ePO infrastructure.

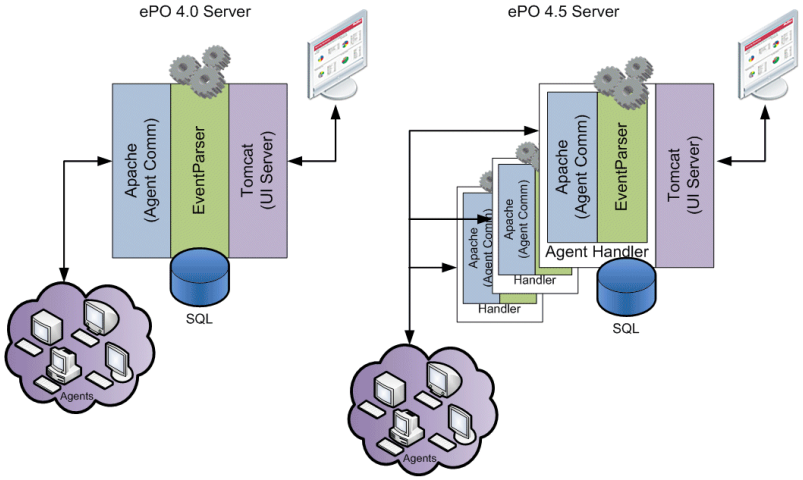

Figure 2: Breaking out the Agent Handler

An agent handler is installed as a part of the primary ePO server. This will be sufficient for many small ePO installations; in such cases an additional agent handler is not required.

To install additional agent handlers, a second installer is available as part of the ePO 4.5 server that allows an administrator to install an agent handler on a separate server, and connect the agent handler to the primary ePO server. Once installed, the additional agent handler is automatically configured to work with the primary ePO server to distribute the incoming agent requests. ePO console can be used to configure Handler Assignment rules to support more complex scenarios, such as an Agent Handler in the DMZ or behind a firewall.

Administrators can override the default behavior by creating rules specific to their environment. See *Agent Handler Management*.

Purpose of Agent Handler

Introduction of agent handlers is designed to provide a solution for the following, prioritized issues:

1. Scalability
2. Failover
3. Network topology

Scalability

The ePO server is the central management solution for McAfee products and with the introduction of SIA program the integration SDKs are available to third party partners as well. As the number of products integrated with ePO increases, attempt to receive policy or send events to ePO increases with the increase in load on the server. An ePO deployment that manages only Virus Scan Enterprise may be able to manage around 200K systems with a single server. But as additional products are deployed and managed by the same server, the increased load decreases

the maximum number of systems manageable with the same hardware. The introduction of agent handlers provides the ability to scale an ePO infrastructure horizontally by adding additional servers to manage an equivalent or larger number of agents with a single logical ePO deployment.

Failover

With ePO 4.0 and previous versions, ePO server unavailability (for example due to upgrade, network, and so on) prevented agents from receiving policy and task updates and reporting events and properties. Once multiple agent handlers are deployed, they can be made available to agents as failover candidates. This allows the application server and any number of agent handlers to either fail or be taken offline while still enabling agents to receive updated tasks or policy from the online agent handler(s). As long as the agent handler is connected to the database it can continue serving agents, including any policy or task modifications that result from agent properties or from user modifications prior to the application server being taken offline.

Failover is only available with the McAfee Agent 4.5. Whereas ePO 4.0 and previous versions of the agent only understand a single server location. The configuration file shared with McAfee Agent 4.5 contains a configurable fallback list of Agent Handlers. McAfee Agent 4.5 will fail down through the list of agent handlers until the list ends or it is able to contact a valid, enabled Agent Handler.

One of the issue using multiple agent handlers for failover is that since McAfee Agent 4.0 only know about a single server, adding agent handlers does not help with providing failover or load balancing for pre McAfee Agents 4.5. Virtual agent handlers (see *Figure 6: Grouping and Virtual Agent Handlers*) can be used with software or hardware load balancers to allow multiple agent handlers to exist behind a single IP address and hostname.

Network Topology

Agent handlers enable support for several network topologies that were not supported in ePO 4.0 and previous versions.

NATted Regions

In ePO 4.0, if agent was within a NAT, they could be managed, but they could not be directly addressed by the ePO server. Administrators were unable to perform direct manipulation of those systems. The agents could not be woken up by the server, so all communication had to be initiated at the agent, which increased latency for certain user-initiated operations. With ePO 4.5, an agent handler can be placed inside a NAT, and will be able to address systems within the NATted region for wake-up, data channel access, and so on.

External Systems

Installation of an Agent Handler in a DMZ will allow external systems to receive their appropriate policies and tasks. For more information, see *Agent Handlers in the DMZ*.

Roaming

Many organizations have a subset of users who roam between sites. By supporting and configuring multiple agent handlers, a roaming user can connect to their nearest agent handler. This is possible only if the agent handlers from all locations have been configured in the agent's

failover list. If the administrator chooses, policy and system sorting can be modified so that the roaming system can receive a different policy in each location.

Backward Compatibility

An important aspect of the agent handler implementation was to ensure seamless backwards compatibility with McAfee Agent 3.6 and 4.0 versions. These versions of the agent had no concept of multiple agent handlers, so only a single entry for the ePO server is available. Consequently, even if multiple agent handlers are configured for failover, only the first handler in the list is sent to 3.6 and 4.0 agents. Hence, the failover from the agent side is not available to legacy agents. However, if agent handlers are arranged in a virtual group, using either software or hardware based load balancers, the single group entry will be sent to these agents. This allows a measured ability to provide load balancing and failover even to legacy agents.

Repository Cache

McAfee Agent by default uses the primary ePO server (same server as Tomcat) as the master repository. This means that agents will fail back to the Agent Handler if they are unable to communicate with their configured repository to pull content and product updates. Since the agent handler may not be running on the same machine as the true master repository (on the ePO application server), it needs to handle these requests. Agent handlers transparently handle requests for software and cache the required files after downloading from the master repository. No configuration is necessary.

Agent Handler Management

All agent handler management is performed under **Menu** | **Configuration** | **Agent Handlers**. Handler Assignment rules are configured in this page.

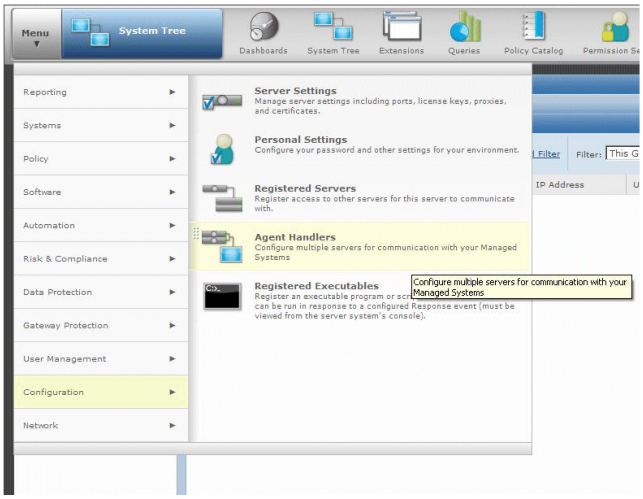

Figure 3: Agent Handler Menu Item

Once an agent handler is installed, it will appear in the list of available agent handlers, which is retrieved from the top left element on the agent handler management page.

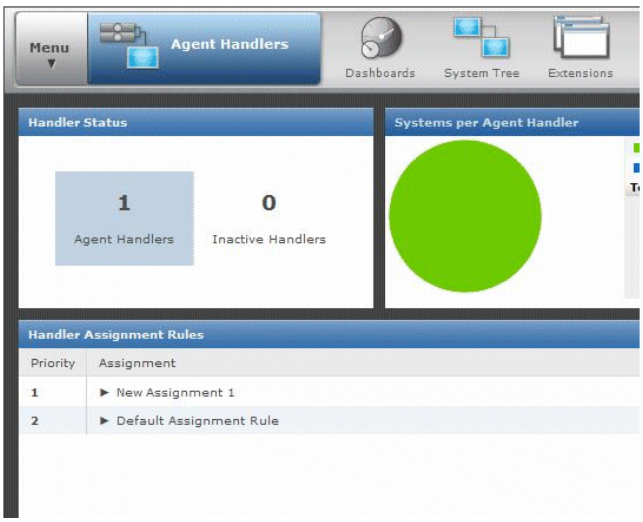

Figure 4: Agent Handler Management Page

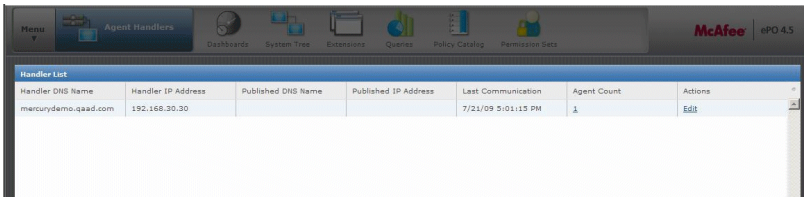

Figure 5: List of Agent Handlers

Agent handlers can be bundled together into Handler Groups for assignment as a single unit in handler assignment rules. Alternatively, if using a load balancer, or if your agent handler can be known by different IP addresses on more than one network segment, you can create virtual agent handlers for use in assignment rules. Type the Virtual DNS name and IP address on the Group page, and the virtual agent handler will be available for assignment.

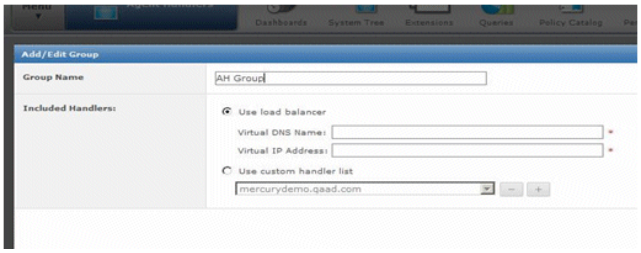

Figure 6: Grouping and Virtual Agent Handlers

An administrator can create handler assignment rules to specify the agent handler and their order for each system. This allows administrators to set primary and fallback agent handlers differently for different areas of the tree.

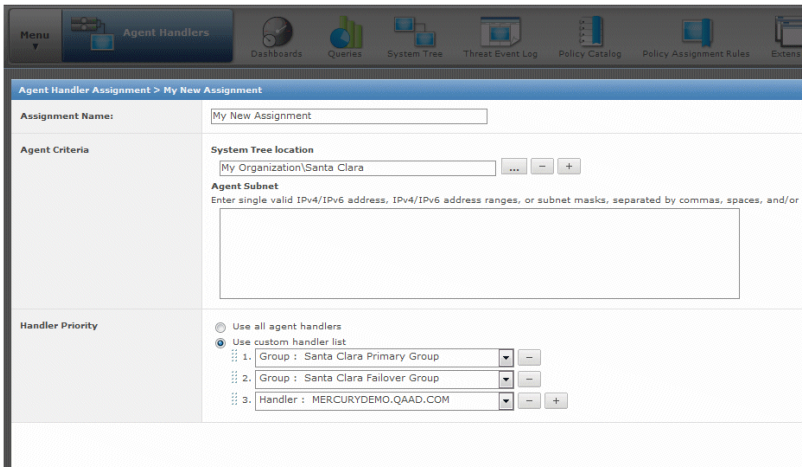

Figure 7: Agent Handler Assignment Rules

Agent Handler Deployment Considerations

A loaded Agent Handler has approximately the same hardware and database requirements as a full ePO 3.6 or 4.0 server. When determining how many agent handlers are required for a given deployment, the first thing to examine is the database usage. If the database serving your 3.6 or 4.0 server is under heavy load, then adding agent handlers will not help. You will need to upgrade your SQL server hardware to take advantage of multiple agent handlers. If the database is currently running at a moderate to low load, then additional agent handlers can allow you to expand your logical ePO infrastructure.

Internal scale testing at McAfee has shown good benefit for additional agent handlers up to 70% database CPU load. As each agent handler adds some overhead (DB connections and management queries to the database) adding agent handlers beyond this point results benefit in performance.

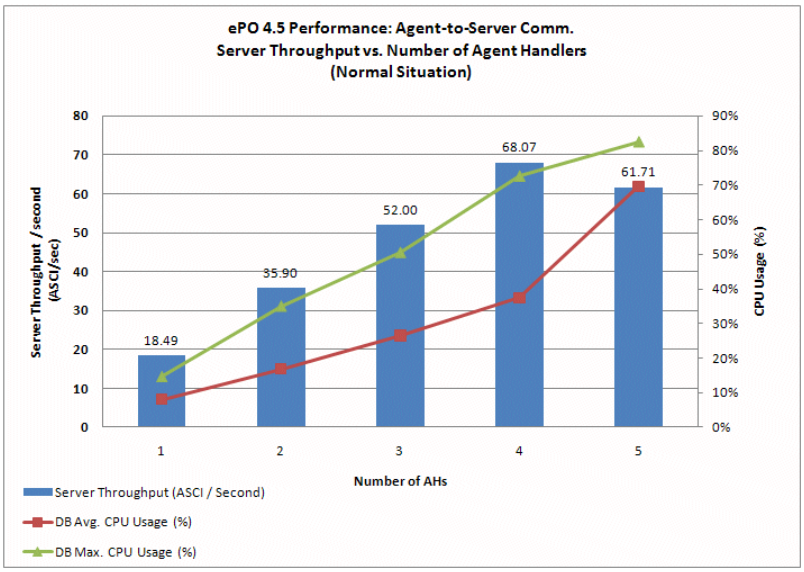

Figure 8: Performance & Load

Figure 8 assumes equal, heavy load across each of the agent handlers.

NOTE: Server, database, and Agent Handler configuration include:

- ePO Server: 8 CPU Xeon 2.0 GHZ; 8GB RAM; Windows 2003 Server Enterprise SP2
- SQL Server: 16 CPU Xeon 3.0 GHZ; 16GB RAM; Windows 2003 Server Enterprise SP2
- Agent Handlers: one CPU Intel 2.66 Dual Core; 4GB RAM; Windows 2003 Server Enterprise SP2

Each agent request includes incremental props from ASE, VSE, GSE, HIPS, SAE, and an event package of 10 events — two from each product.

▸ Failover

Failover

Failover between Agent Handlers can be configured in one of two ways. In a simplest deployment (see *Figure 9*), two agent handlers can be deployed as primary and secondary. In this approach, all agents will initiate communications with the primary agent handler, and will only use the secondary agent handler if primary agent handler is unavailable. This deployment can make sense if the primary agent handler has better hardware, and is capable of handling the entire load of the infrastructure.

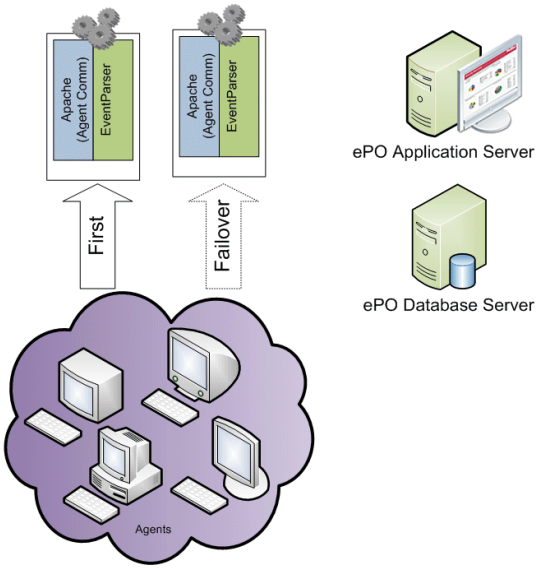

Figure 9: Two Agent Handlers in Failover

The second deployment combines failover with load balancing. Here, multiple agent handlers are all put in the same agent group, and the ePO server will insert each agent handlers in the group into the list of agent handlers at the same order level. McAfee Agent 4.5 will randomize agent handlers at the same order level, which should result in an equal load across all agent handlers in a particular group.

Agents will fail over between all handlers in a group before failing through to the next handler in the assignment list. This means that using agent handler groups results in both load balancing and failover benefits.

Scalability

The default behavior of agent handlers within ePO 4.0 is for scalability. Enabling an additional agent handler requires a user install and an additional agent handler. All agent handlers will be used at the same order level until custom assignment rules are created. This results in equal load across all agent handlers.

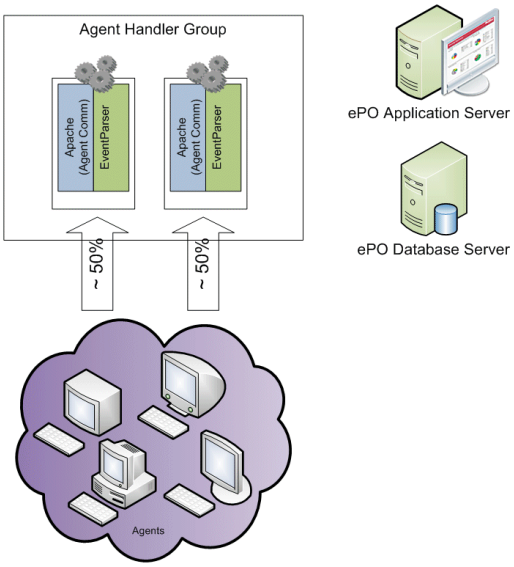

Figure 10: Two Agent Handlers Configured as a Group

Agent Handlers in the DMZ

One of the most requested deployment scenarios is to be able to have an agent handler in a DMZ. This enables management and updating of external clients. This is possible, although the agent handler requires access to both the common database and the application server, some firewall rules are necessary for this.

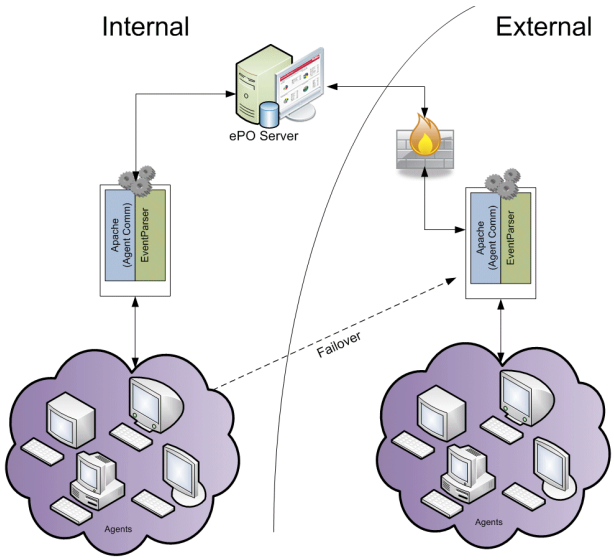

Figure 11: Agent Handler in a DMZ

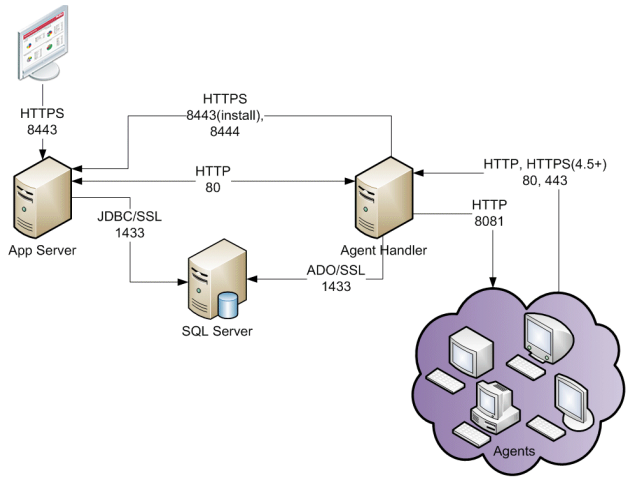

Figure 12: Default Ports in Use

Agent Handlers versus Multiple ePO Server

Inevitably the question of whether it is more appropriate to add an additional agent handler or deploy another ePO server will arise. As a general response, Agent Handlers should be used when:

- The existing ePO infrastructure needs to be expanded to handle more agents, more products, or a higher load due to more frequent ASCI communication.
- The customer wants to ensure agents continue to dial in and receive policy/task/product updates even if the application server is unavailable.
- The customer wants to expand ePO management into disconnected network segments, where there is still a relatively high bandwidth link to the ePO database.

Agent Handler should not be installed to:

- Replace distributed repositories. Distributed repositories exist to distribute large files throughout an organization, and do not contain any logic.
- Connect a disconnected network segment where there is limited or irregular connectivity to the ePO database.

In most cases it is preferable to add a new Agent Handler rather than a new ePO server. Only when separate IT infrastructures, separate administrative groups, or test environments a new ePO server is the best choice.

Frequently Asked Questions

- What ports do I need to open in my firewall to allow the Agent Handler?

  See *Figure 12: Default Ports in Use*

- What data is sent to ePO Server and what is sent to the database?

  One of the additional features of ePO 4.5 is an API extension for McAfee products integration called the Data Channel. It is a mechanism for McAfee products to exchange messages between their endpoint plugins and their management extensions. This will be the majority of data sent from the Agent Handler to the application server. Although there is limited use by McAfee products yet, it is used internally by ePO for agent deployment and wake-up progress messaging. Other functions such as agent properties, tagging, and policy computation is performed directly against the database.

- If the ePO server is not defined in my repository list will replication still occur?

  Yes, if the agent contacts the Agent Handler for software packages, the Agent Handler will retrieve them from the real master repository.

- How much bandwidth will be used for communication between the database and the ePO server?

  Bandwidth between the Agent Handler and the database will vary based on the number of agents connecting to that Agent Handler. However, each Agent Handler will place a fixed load on the database server for its heartbeat (updated every minute), checking the work queue (every 10 seconds), and by its pool of database connections held open to the database (2xCPU for EventParser + 4xCPU for Apache).

- What versions of the McAfee Agent will work with Agent Handlers?

  McAfee Agent 3.6.x, 4.0.x, and 4.5.x are supported. To McAfee Agent 3.6.x and 4.0.x agents, the Agent Handlers appears to be the ePO server. The sitelist sent to these agents includes a single entry for the server location. Hence, these agents cannot take advantage of the existence of multiple handlers for failover or load balancing. Agents version 4.5 and above are multiple-agent-handler aware.

- Is the communication between the agent and Agent Handler encrypted?

  Yes. All traffic between Agents and the Handler are signed and verified with public/private DSA key pairs for authenticity. Agents prior to 4.5 use the legacy 3DES encryption for channel encryption. McAfee Agent 4.5 and later use TLS by default.

- How many agents does one Agent Handler support?

  Agent Handlers for scalability is not required until a deployment reaches 100K nodes. Agent Handlers for topology or failover may be required at any stage. A good rule would be one Agent Handler per 50K nodes.

- What kind of hardware/Operating System is required to install an Agent Handler on?

  The Operating System should be a Microsoft Server Operating System (2003 server or 2008 server), as the non-server Operating System versions have severe (~10) limits set on the

number of incoming network connections. More information on scaling is available in the ePO 4.5 Hardware Sizing Guide.