DOWNLOAD PDF EPO 4.6 AGENT HANDLER WHITE PAPER.

Chapter 1 : McAfee QUICKCLEAN Setup guide | blog.quintoapp.com

blog.quintoapp.com Handler Deployment Considerations A loaded Agent Handler has approximately the same hardware and database requirements as a full ePO or server. 4GB RAM. heavy load across each of the agent handlers.6 or 4.

Supported deployment methods Deploy software to your managed systems. Before deploying any software, review the associated product install guide to ensure the target system meets the minimum requirements. Configure product update tasks for your managed systems. Master Repository and Management Extensions The master repository stores the installers, updates, hotfixes, and content updates that deploy to managed systems. Checking in software to the master repository is necessary if you plan to use McAfee ePO to deploy products. The master repository is divided into three separate branches: Current, Evaluation, and Previous. The intention of the branches is to aid with product lifecycle management. The product version that has been tested and approved by your company for release. Used to store new releases for internal testing on a limited set of systems before release to the entire organization. Used to save and store prior. DAT and engine files before adding the new ones to the Current branch. If you experience an issue with new. DAT or engine files in your environment, you have a copy of a previous version that you can use to roll back the. DAT on your systems if necessary. Each point product you plan to manage with McAfee ePO also includes one or more management extensions. The extensions add controls for that point product, such as policies and client tasks. If a management extension is removed, the corresponding policies and tasks you created for that product are also removed. The optional server setting Policy and Task Retention can be enabled to save policies and client task data if you remove the extension. System Tree Building the System Tree involves two main objectives: Creating and organizing groups and sub-groups 2. Adding systems As part of the planning process, consider the best way to organize systems into groups before building the System Tree. Grouping systems with similar properties or requirements into these units allows you to manage policies and tasks for systems in one place, rather than setting policies for each system individually. There are many methods to populate the System Tree. The Lost and Found Group: This group cannot be deleted or renamed. The sorting criteria cannot be changed from being a catchall group, although you can provide sorting criteria for any subgroups created in it. If no such group exists, one is created. Creating Policies and Setting Assignments When a product management extension is checked in, the policy catalog is updated with the policies for the corresponding point product. Review the Product Guide for corresponding product information about the policy settings you are working with. When a policy has been created, it can be assigned to any group, subgroup, or individual node in the System Tree. All child subgroups in the System Tree hierarchy inherit policies set at their parent groups. These inheritance rules simplify policy and task administration. For details review the Enforcing Policies section of the Product Guide. Policies set at the My Organization level of the System Tree apply to all groups. Policies assigned to a group apply to all subgroups or individual systems in that group. Inheritance can be broken if you need to assign a unique policy to an individual subgroup or node. During the agent-server communication interval, system properties and product events are collected and sent to McAfee ePO. The list of assigned client tasks is then downloaded and added to the agent scheduler, and assigned policies are enforced. This process is repeated at every agent-server communication interval ASCI. McAfee ePO updates an existing System Tree record with the new properties received or adds a new record to the System Tree, if there is not already an entry present for the system. For additional details on working with the System Tree, see the System Tree section. Deployment tasks should be completed in a phased rollout to install products to groups of systems at a time. The same task can have multiple assignments throughout the System Tree, and each assignment defines the schedule for the task. Avoid creating task schedules that will repeat the task too frequently or run the task on too many nodes simultaneously because this could potentially overload the McAfee ePO server. When a client task is assigned to a group or node in the System Tree, the agent downloads the task settings during its next communication interval and invokes the task according to the schedule defined. When the client task is invoked, the agent downloads the components defined from the McAfee ePO server Master Repository. Additional Distributed Repositories can be configured to help split up the load. As you deploy products to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems. Product Update Product updates are a type of client task that are used to apply content updates to products already installed on managed systems. Content updates include antivirus definitions. DATs , version updates, and hotfixes. This task downloads the latest. DAT to the managed systems: This defines which branch the managed system pulls the. The default is set to use the Current Branch. Provide a meaningful name for the task and enable the option for. Assign the newly created task to the groups, subgroups, or individual systems you wish to update the. Typically, the schedule for this task should be set to run at least once per day. This is desirable when, instead of upgrading an older McAfee ePO server, the administrator chooses to build a new environment. The alternative, redeploying the McAfee Agent to all managed endpoints, can be unwieldy in larger environments. There are minimal limitations regarding McAfee ePO server versions when transferring systems. There are several critical factors to consider when transferring systems: System transfer does not include System Tree structure, policies, or policy assignments, only the systems themselves. A general workflow for exporting and importing policies and system structure is included in KB McAfee Drive Encryption introduces several complicating factors such as user assignments or token data. A step-by-step guide to configuring system transfer is detailed in KB A basic walkthrough of the migration process is included in KB , including step-by-step instructions for implementing the basic workflow: This process may be necessary if the SQL server runs out of disk space. Those older workflows are still an option, but with the advent of the Disaster Recovery Snapshot , the recovery and migration has been consolidated into one easy process. Considerations for the Disaster Recovery Snapshot: This is due to the SQL Express 10GB file size limitation and how much data is stored within the database inside the snapshot table. If all three methods of communication are different, the endpoints have no way of routing their traffic to the new server outside of a DNS redirect. If McAfee ePO 5. If the McAfee ePO server is upgraded from a previous version, it is necessary to use the new functionality made possible by the Certificate Manager. It is critical that the certificate migration process described in KB is not finalized before an accepted number of client machines have communicated and received the new agent-server communication certificates. Internal tracking is available within the Certificate Manager to provide for complete visibility. A failure to follow instructions during this step will result in a complete failure for all client machines that have yet to receive the new certificate to communicate with McAfee ePO â€”meaning that redeployment of the McAfee Agent will be the only solution. See KB login required. Because the SQL database for McAfee ePO is highly transactional in nature, the execution speed of those transactions directly relates to how fast the product is able to operate. The Recommended Maintenance Plan login required for the McAfee ePO database focuses primarily on several configuration options and a regularly scheduled maintenance plan that consists of three tasks. The full recovery model introduces additional overhead backing up the transaction log and requires a great deal more space on the SQL server for the ever-growing transaction log. Shrinking the database causes database fragmentation, which reduces performance. The option to shrink the data file can be taken in situations such as when an uncharacteristically large flood of unexpected events is generated and stored within the SQL database. A large number of events might occur after a malware outbreak. To configure a regularly scheduled SQL maintenance plan: Back up the SQL database.

Chapter 2 : Agent Handler server requirements - McAfee ePolicy Orchestrator

Hi Guys, I wonder ifyou could help, have experience or point me in right direction to implement ePO infrastructure. Wecurrently use ePO Patch 7 and this server manages clients at 66 blog.quintoapp.com of the sites have at least 2mbits connection to the server over WAN link.

Here are ten things you need to know â€" directly from our ePO Support engineers. See KB â€" Description and primary log locations for the ePO services for the primary log locations. In order for this process to complete, it is necessary to first verify that all environmental requirements are met. For more information, check KB â€" Environmental requirements for agent deployment from the ePO 4. KB â€" ePO server backup and disaster recovery procedure. If your Disaster Recovery Snapshot Server Task is running regularly recommended nightly it is only necessary to schedule database backups, cutting your work in half. The Event Parser service is particularly sensitive to database connectivity issues. If you find that the Event Parser service has stopped and is unable to start, it is most likely that the database connection has been broken. From here, it is important to input your database connection credentials and information and test the connection before saving the changes and restarting the ePO services. Wrong password in account used to log on to SQL 5. See KB â€" Deployment tasks configured to "Run at every policy enforcement" lead to max connections in ePO Agent to server communication fails for additional information. Hardware Sizing and Bandwidth McAfee has performed tests on different server-class systems to help users determine the hardware requirements for ePO. PD â€" ePO Hardware Sizing and Bandwidth Usage Guide has information on how to calculate hardware requirements, bandwidth usage, and database sizing. However, this can cause a variety of issues including not reporting back to ePO server the correct point product information, point product events from that client failing to be parsed, and newly created client tasks for point products failing to invoke on the client. Almost always, point product extensions are backwards compatible with the point product package version on the client so there is typically no impact on the client side by upgrading your server side extension. As with any change on the server side, please be sure to take a backup of your ePO server and database before making a change to your extensions see Must Know 1. Please read the product documentation including the Release Notes as well before upgrading your extension. For more information, see p. Keep performance in mind when configuring Automatic Responses Configuring your Automatic Responses correctly is vital to maintaining good ePO server performance. If your Automatic Response is configured to trigger on every event â€" without aggregation for an Event ID that you typically already have many of in ePO, Application Server Service Tomcat will be overwhelmed with trying to process all the automatic responses. This can lead to unresponsiveness, out of memory errors in your ePO server, or just very slow console GUI responsiveness. Please see the ePO Product Guide for more information. Once this is in place, the MAC address will still be reported to ePO, however MACs matching the one inserted will no longer be used for matching purposes. These can be found on the McAfee ServicePortal.

Chapter 3 : Explanation of Agent Handler assignment priority

McAfee Agent (MA) 5.x, 4.x McAfee ePolicy Orchestrator (ePO) 5.x, x. Engagement Team To help track customer impact, do the following in Insight: In the Documented Solution field, add the Knowledge Base article number, without the KB prefix.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. License Attributions Refer to the product Release Notes. This new component of the ePO infrastructure has been termed an Agent Handler. 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. 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: 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. These can be located at Start Run Services. 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. Install Types In ePO 4. There is only one primary ePO server in a logical ePO server. A small number of Agent Handlers can be deployed on separate hardware and co-exist within a single logical ePO infrastructure. 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. Once installed, the additional agent handler is automatically configured to work with the primary ePO server to distribute the incoming agent requests. 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: 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 K systems with a single server. But as additional products are deployed and managed by the same server, the increased load decreases 6 McAfee Agent Handlers Introducing Agent Handlers Purpose of Agent Handler 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. 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. The configuration file shared with

McAfee Agent 4. One of the issue using multiple agent handlers for failover is that since McAfee Agent 4. 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. 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. External Systems Installation of an Agent Handler in a DMZ will allow external systems to receive their appropriate policies and tasks. 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. 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. 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. 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. 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. Handler Assignment rules are configured in this page. 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. 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. 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. 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. 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. 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. Server, database, and Agent Handler configuration include: 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. 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. 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. 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. 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. As a general response, Agent Handlers should be used when: Agent Handler should not be installed to: Distributed repositories exist to distribute large files throughout an organization, and do not contain any logic. 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. One of the additional features of ePO 4. 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. Yes, if the agent contacts the Agent Handler for software packages, the Agent Handler will retrieve them from the real master repository. Bandwidth between the Agent Handler and the database will vary based on the number of agents connecting to that Agent Handler. To McAfee Agent 3.

Chapter 4 : Red Hat NETSCAPE MANAGEMENT SYSTEM - AGENT GUIDE Installation guide | blog.quint

Mcafee Antivirus VSE not getting installed when deployed from ePO When deploying the Mcafee Antivirus VSE from ePO , we wer How to uninstall Host Data Loss Prevention agent without using a challenge code.

Do not copy without permission. Other names and brands may be claimed as the property of others. It measures compliance by comparing the actual configuration of a system to the desired state of a system. This guide provides system requirements for McAfee Policy Auditor software, and information about installing it as a managed product, as well as modifying, repairing, removing, and reinstalling the software. Contents Product components Audience Conventions Finding product documentation Product components McAfee Policy Auditor software consists of several components that are used to create benchmarks, audit systems, and display results. These are the McAfee Policy Auditor components as they appear in the user interface: Each audit must contain at least one benchmark. Ideally, audits should contain only one benchmark. The information in this guide is intended primarily for: Conventions This guide uses the following typographical conventions. Book title or Emphasis Title of a book, chapter, or topic; introduction of a new term; emphasis. Bold Text that is strongly emphasized. User input or Path Commands and other text that the user types; the path of a folder or program. Code A code sample. User interface Words in the user interface including options, menus, buttons, and dialog boxes. Hypertext blue A live link to a topic or to a website. Note Additional information, like an alternate method of accessing an option. Tip Suggestions and recommendations. Warning Critical advice to prevent bodily harm when using a hardware product. Finding product documentation McAfee provides the information you need during each phase of product implementation, from installing to using and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase. User Documentation 1 Click Product Documentation. McAfee Policy Auditor 6. This section presents information to help plan and prepare your system before installing the software. Contents Preparation for installing the software System requirements Database considerations and support Preparation for installing the software Complete these tasks before installing the McAfee Policy Auditor software. Refer to System requirements for details. The license is not automatically upgraded from an evaluation version. System requirements Verify that your server and systems to be audited meet these system requirements before you start the installation process. Unless otherwise specified, these are minimum requirements and are not optimal for performance. They apply only to McAfee Policy Auditor. You must also consider system requirements for any other products you are installing, such as McAfee Vulnerability Manager. Server requirements This section contains information you need to know before installing the McAfee Policy Auditor software, including hardware and software requirements. For instructions, see the Microsoft product documentation. Supported operating systems McAfee Policy Auditor is installed as an extension of ePolicy Orchestrator software and runs on operating systems supported by that product. For the most current information about supported operating systems, see this article in the McAfee KnowledgeBase: Browsers supported ePolicy Orchestrator software runs on the most commonly-used browsers and can be accessed from anywhere on the network. For the most current information about ePolicy Orchestrator software virtual infrastructure support, see this article on the McAfee KnowledgeBase: Ports needed by ePolicy Orchestrator software for communication through a firewall ePolicy Orchestrator software uses ports to communicate with web browsers, SQL Server, managed systems, the network, and other portions of the software. For the most current information about ports use by ePolicy Orchestrator software, see this article in the McAfee KnowledgeBase: This table shows the ports needed by ePolicy Orchestrator software for communication through a firewall. Port Default Description Traffic direction Agent to server communication port 80 TCP port opened by the ePolicy Orchestrator software server service to receive requests from agents. Agent communicating over SSL 4. TCP port opened to replicate repository content to a SuperAgent repository. Outbound connection from the SuperAgents. Inbound connection to the ePolicy Orchestrator software server. Outbound connection from remote Agent Handlers. Note from the ePolicy that this port cannot be changed. This port is specified or determined automatically during the setup process. Supported virtual infrastructure software ePolicy Orchestrator software runs on the most commonly-used virtual infrastructure software. Virtual software ePO 4. Consider using distributed repositories and strategically placing them throughout your network to ensure that managed systems are updated and to minimize network traffic. As you update your master repository, the ePolicy Orchestrator software software replicates the contents to the distributed repositories. For more information on distributed repositories, see your appropriate ePolicy Orchestrator software product guides. Component Requirement Free disk space MB on the drive where the repository is stored. Memory MB minimum. The available features depend upon the agent version and the ePolicy Orchestrator software version. Some of the new features of ePolicy Orchestrator software version 4. Some of the new features of McAfee Agent4. Free disk space for agent plug-in MB. Free disk space for other McAfee components Sufficient disk space on client computers for each McAfee product that you plan to deploy. For more information, see the corresponding product documentation. Network environment Microsoft or Novell NetWare networks. Network interface card NIC 10 Mbps or higher. Agentless audit support Agentless audits allow you to audit systems that do not have the McAfee Policy Auditor agent plug-in installed. McAfee Vulnerability Manager versions 7. To perform agentless audits, you must have a McAfee Vulnerability Manager server that is accessible over your network. Database considerations and support McAfee Policy Auditor software, which requires a database, uses the ePolicy Orchestrator software server database by default. Using McAfee Policy Auditor software with a database Any of the following databases, if previously installed, meet the requirements for the software. If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you might have a problem installing or starting the ePolicy Orchestrator software. These tables provide additional information about your database choices and other software requirements. Dedicated server and network connection Needed if managing more than 5, systems. Local database server If the database and McAfee Policy Auditor server are on the same system, McAfee recommends configuring your server to use a using a fixed virtual memory size that is approximately two-thirds of the total memory allotted for SQL Server. If the minimum number of SQL Server licenses is not available, you might have difficulty installing or starting the ePolicy Orchestrator software server. Available in bit and bit versions. SQL Server bit is supported only if it is installed on a separate system from the ePolicy Orchestrator software server. You must acquire and install. Microsoft updates Update the ePolicy Orchestrator software server and the database server with the most current updates and patches. Database storage requirements When determining hardware needs for your organization, it is important to estimate the amount of database storage required to use McAfee Policy Auditor software. McAfee has designed the software so that audit results consume the minimum amount of disk space. The amount of database storage you require depends on these factors: The tables used to calculate server and database requirements are based on tests of the software in the following distributed environment: The differential audits feature causes the increase in database size to decrease significantly after the first audit. The Index Configuration server setting also affects the size of the database. If you use the Minimal Indexing option, the database will be smaller than if you use one of the other options. The ultimate database size cannot be calculated accurately prior to deploying McAfee Policy Auditor, but can be estimated approximately 3 months after beginning a phased rollout. Use the database storage sizing estimates to determine the initial database size for new systems and new audits. Estimating database storage requirements You can estimate the average amount of hard disk space needed to store new McAfee audit results. For example, 20 audits once per quarter, 5 audits once per month, or one audit once per week. The sum is equal to the size of the database required to store the audit results for one year. For example, if you intend to store the audit results for McAfee Policy Auditor 6. If you intend to store the audit results for six months, divide the database size by two. Database storage example and requirements table The requirements table for database sizing can help you calculate the the approximate disk space needed for your McAfee Policy Auditor database. Requirements table for database sizing Use this table to estimate the required size of your database. These estimates are based upon the average size of benchmark audit results. Your needs may vary. The table does not include this value, so we approximate this to two audits per week running on 2, systems. The table does not include this value, but it is equivalent to three yearly audits on 50, systems. Calculate the approximate database size: When a file changes, the McAfee Policy Auditor agent plug-in notes the change and sends an event back to the server.

Chapter 5 : Agent Handler details - McAfee ePolicy Orchestrator

If you really need to be on ePO instead of ePO please consider ramping it up to ePO patch 5. Significant improvements exist between patch 3 and patch 5, especially in respect to products heavy on the datachannel, such as endpoint encryption (eepc), data loss prevention (dlp) and policy auditor (pa).

We strongly recommend that you read the entire document. Release date â€” November 4, This release was developed for use with: This update must be applied immediately to avoid a potential security breach, and to maintain a viable and supported product. Resolved issues This hotfix resolves the following issues. For a list of issues fixed in earlier releases, see the Release Notes for the specific release. Issue Both of the vulnerabilities below involve denial of service attacks via memory leak. For more information, please visit the links provided below. There are separate installers for this hotfix: Use the appropriate installer for your McAfee ePO server and remote agent handlers. See below for more information. These updates will not install in FIPS mode. If, after this hotfix is installed, McAfee ePO is reinstalled, then you must reapply this hotfix. Later patch releases include this fix or include updated files. Install the software on McAfee ePO and remote agent handlers Follow these steps to install this hotfix. Install the software on McAfee ePO server clusters Follow these steps to install this hotfix in your cluster environment. Perform the installation on the node where the first installation of McAfee ePO was performed. The hotfix does not need to be installed on any other nodes. Although this is optional, we highly recommend this step to ensure that the installation is isolated to the active node. Tomcat Verify hotfix installation Follow these steps to ensure that the hotfix was installed correctly. McAfee ePO installation directory: Remote agent handler installation directory: Hotfix files should be applied only on the advice of McAfee Technical Support, and only when you are actually experiencing the issue being addressed by the hotfix. Hotfix files should not be proactively applied in order to prevent potential product issues. You are responsible for reading and following all instructions for preparation, configuration, and installation of hotfix files. Hotfix files are not a substitute or replacement for product Service Packs which may be released by McAfee, Inc. It is a violation of your software license agreement to distribute or share these files with any other person or entity without written permission from McAfee, Inc. Further, posting of McAfee hotfix files to publicly available Internet sites is prohibited. Find product documentation After a product is released, information about the product is entered into the McAfee online Knowledge Center. Do not copy without permission. Other names and brands may be claimed as the property of others.

Chapter 6 : McAfee ePolicy Orchestrator - ePO | McAfee Products

NOTE: All handlers, including the McAfee ePO server itself and all remote Agent Handlers, depend on a fast, consistent connection to the SQL database. Don't forget to update any remote handler's database configuration to point to the new database; otherwise, the handler will be nonfunctional and unable to process incoming Agent communications.

Chapter 7 : How To Setup McAfee Agent Handler ~ Information Security Blog

In this quick step guide, we have ePO patch 5 installed, so we would be installing agent handler from ePO L source binaries. Navigate to the Agent handler folder The agent handler folder is within the EPOL folder.

Chapter 8 : Ports needed by ePolicy Orchestrator for communication through a firewall

The Agent Handler can authenticate to the McAfee ePO SQL database using domain credentials. If Windows authentication is not possible, the account the Agent Handler uses to authenticate to the database must use SQL authentication.

Chapter 9 : Mcafee Agent Handler Installation â€“ TechMo'sâ€¦

DOWNLOAD PDF EPO 4.6 AGENT HANDLER WHITE PAPER.

The McAfee ePO console is also used to configure Agent Handler Assignment rules to support more complex scenarios. For example, an Agent Handler behind the DMZ, firewall, or using network address translation (NAT).