DDM Inventory 9.30: Securing the Database

Securing the Server

HP® Discovery and Dependency Mapping Inventory

Introduction

Because DDM Inventory collects sensitive information about the devices that are attached to a corporate network, security is a paramount concern. DDM Inventory version 9.30 provides security features that can protect the confidential data that it collects.

This document depicts the DDM Inventory application security model, explains the security features that DDM Inventory provides, and guides customers in implementing effective security measures.

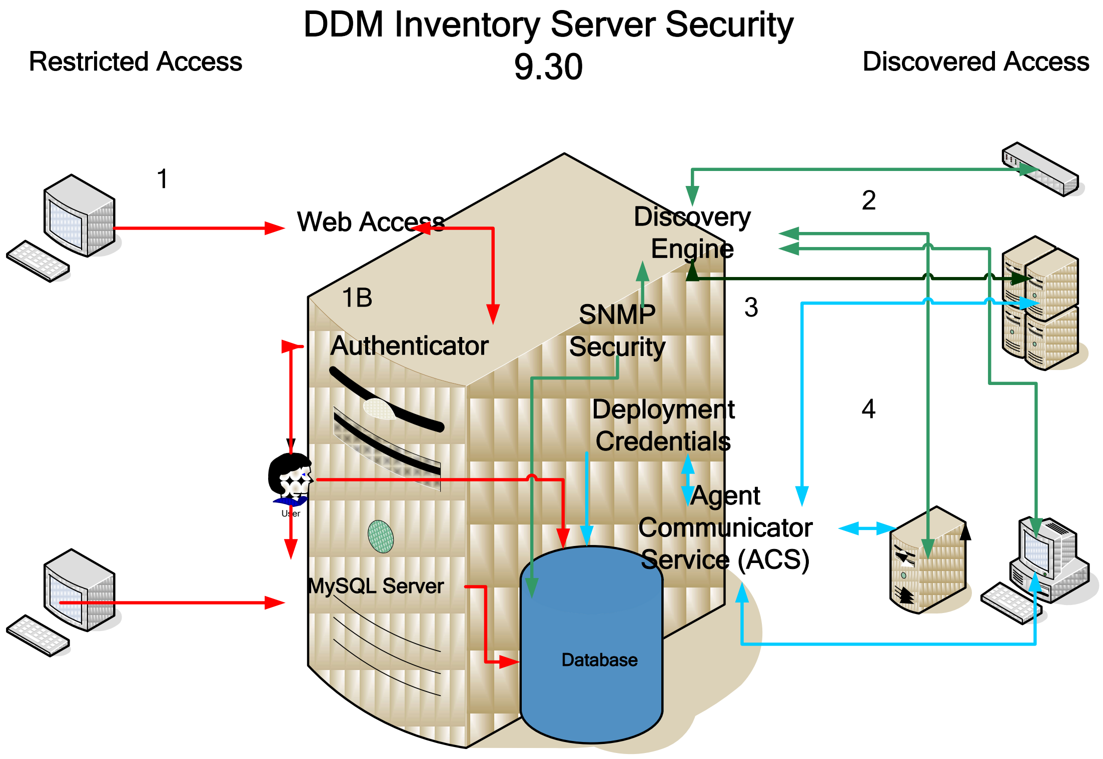
Note: Before attempting to implement security measures, read the *DDM Inventory Installation and Initial Setup Guide* in its entirety and make sure you understand it. The guide contains important additional information about securing your DDM Inventory server.

Overview of DDM Inventory security

Figure 1 displays an overview of security-related components and interfaces that are addressed in this document. The following diagram depicts security configuration on a single server:

- *Web client to web server communication, MySQL client to server communication (1)*
- *Additional DDM Inventory security settings (1b)*
- *SNMP, community strings, and DDM Inventory (2)*
- *VMware Discovery (3)*
- *Agent communication (4)*

Figure 1. Overview of DDM Inventory Security



In the scenario in Figure 1 the following steps occur to provide database security:

1. The Web client communicates with the Web server using an HTTPS/SSL connection. (HTTPS is an abbreviation of *HyperText Transfer Protocol Secure*. SSL is an abbreviation of *Secure Sockets Layer*.)
2. The Web server confirms the identity of the user with the Authenticator.
3. Once logged in, depending on the type of the user account, the user may be allowed to change the discovery settings IP Address, Community Strings, and Deployment Credentials. Only administrators of DDMI can make changes to the discovery configurations. For more information on user accounts please see the Configuration and Customization guide for Setting up accounts.
4. MySQL client communicates with MySQL server directly. The Discovery Engine will use SNMP Security to communicate with devices in the network while trying to collect information about them.
5. Additionally accounts to discover VMware Host and Virtual Centers/vCenters are then used during the discovery phase.
6. The Agent Communicator uses the Deployment credentials to start the initial deployment of the DDMI Agent and also uses deployment credentials for agentless scanning.
7. Both the MySQL server and the Web server are installed with DDM Inventory.

Web client to Web server communication (1)

The DDM Inventory installation wizard installs the Apache Web server as the default Web server. When using DDM Inventory, the embedded Apache web server cannot be used as a generic web server for any other purposes - it is dedicated to DDM Inventory. Data exchanged between the Web server and the Web client may contain critical information such as user passwords, information about assets, and details of the network topology. This information is encrypted when passed over the network using HTTPS.
Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than to the default Web port number, 80. For DDM Inventory, secure communications between the server and the client take place via the standard HTTPS port 443.

When you use the installation wizard to install DDM Inventory, one step in the wizard allows you to enter your own Fully Qualified Domain Name (FQDN) for your server in the network. This adds the information to the certificate that will be used in communications that originate from workstations. The certificate from DDM Inventory must be applied to each workstation. You can also obtain your own certificate (from a certificate provider such as Verisign, Inc) and add this to the DDM Inventory Server in place of the default certificate that is provided.

Note: For more information about this configuration see the *DDM Inventory 9.30 Release Notes* and Initial setup and installation guide.

Certificate files are located in the default location of the data directory, unless you have changed the default data path. The default path is usually

```
C:\Documents and Settings\All Users\Application Data\Hewlett Packard
\DDMI\cert\
```

Certificate file must be installed on each workstation that will access the DDM Inventory Server. This is automated by the browser you are communicating with. You should also be sure that a backup of this directory is stored in a secure location. In the event that the DDM Inventory server fails and it is necessary to re-install DDM Inventory server to recover the backup of this directory will ensure that a re-install of certificates is not needed across the client population. The files stored here have to be kept here.

Directory	File Name	Used for
..\DDMI\Cert	ACSKeyStore.bin	DDMI Agent Communication, Never Copied, DO NOT DISTRIBUTE
..\DDMI\Cert	acstrust.cert	DDMI Agent Communication, Never Copied, DO NOT DISTRIBUTE
..\ DDMI \Cert	agentca.pem	DDMI Agent Communication, Never Copied, DO NOT DISTRIBUTE

After you have completed the previous tasks, you access the server using the host name that was assigned to the server and added as the FQDN. For more information see the *DDM Inventory Installation and Initial Setup Guide*.

Communications between MySQL client and MySQL server (1)

You have the option of using the MySQL client to communicate with the MySQL server.

The DDM Inventory installation wizard installs MySQL server. The standard port that is used to connect to a MySQL server is TCP/IP port 3306. In DDM Inventory the port is changed to 8108. Access to the port can be disabled for each account that accesses the database, which allows data to be transferred out of DDM Inventory in a controlled manner.

Direct access to the tables and fields in the MySQL server is not controlled by the DDM Inventory Authenticator. Using a MySQL client to access the server enables you to connect to the combined information in the Discovery database, which is the only database that is visible in DDM Inventory. Using the security template included with DDM Inventory, the MySQL server can be configured with rights so that no user has visibility to it except the Windows Server administrator.

For tools that access the MySQL database in DDM Inventory, go to http://www.mysql.com. In addition, an ODBC driver named "MySQL Connector" is available at http://dev.mysql.com/downloads/connector/odbc. With this driver you can take information from the Discovery database and copy it to a third-party program such as Microsoft Access. You can then create customer reports on the data that has been populated into the Discovery database. To connect to the MySQL database, use version 5.1.8 of the MySQL ODBC driver.

Note: When you connect to the MySQL database on DDM Inventory, the database name is "aggregate," which is the original name given to the database many years ago. The *external* name of the database is “Discovery.” The name change was made so that the name is not confused with Aggregator.

Information sent via Connect-It is transferred using either a native MySQL driver, or using an ODBC connection that can be made to transfer the information into another application such as Asset Manager.

The Discovery database contains all the information that was collected during the Network Discovery process and later merged with the scan file information. The Discovery database has many tables of information from which SQL statements can be used to query the database.

Additional DDM Inventory security setting (1B)

For tighter control of the DDM Inventory Server you can enable additional security settings and activity logging.

Password management

Enabling password strength criteria enables you to set the following parameters:

- *Minimum number of lowercase letters*
- *Minimum number of uppercase letters*
- *Minimum number of digits*
- *Minimum number of symbols*
- *Minimum number of digits and symbols*
- *Minimum password length*
- *Maximum number of failed login attempts*

- *Password history*
- *Delete password history*

Activity logging

Security-minded organizations can log the actions performed by each user, and then research or troubleshoot problems that may be caused by changes made to DDM Inventory. By default this is disabled. This can be enabled by accessing the DDM Inventory server and selecting the Administration section. In here you will see the Server Configurations. The second to last option, "Log User Actions," is a Yes or No setting. To activate logging set the feature to yes.

Account types

In DDM Inventory there are five default accounts types, whose security is handled in Account Administration. Each account type has different permissions, and the principal difference between account types is the amount of administration authority that is permitted. The five default account types are:

- *Demo— The user has limited control, and is considered "safe" for demonstration and training purposes.*
- *IT Employee— The user can make specific, limited changes that affect what the user's own account can access. This account gives the user information before checking client systems.*
- *IT Manager— The user can make changes that affect the information that other accounts can see. Moreover, the IT Manager user can oversee the operation of DDM Inventory. This account type is not as powerful as the Administrator account.*
- *Administrator— The user can set up DDM Inventory and other accounts. This account type should be granted only to system administrators.*
- *Scanner— This account type is used when the scanners are deployed using Manual Deployment mode, when scanners are responsible for saving the off-site scan file directly onto the DDMI server. Used only in special circumstances, the Scanner account is reserved for devices where the user cannot install the Agent, which sends the scan file to the DDM Inventory server.*
- *Aggregator - The Aggregator account is used only to send data to an Aggregator server. Typically, an Aggregator server holds the data for multiple "remote" servers that are deployed throughout a large network. In order for an Aggregator server to obtain the data from the remote servers, it must have access to that server through an "Aggregator" user account. For more details, see the* Installation and Initial Setup Guide.

Server security template

A Windows security template should be applied to the DDM Inventory Server to protect critical components. This template is applied to any user account that can access the DDM Inventory server. The DDM Inventory server now supports Windows Server 2008 in addition to Windows Server 2003. Depending on the OS the path to the following information will be different. See the Compatibility Matrix for a complete list of supported Operating Systems.

The default Data folder for Windows Server 2003 installations is as follows:

C:\Documents and Settings\All Users\Application Data\Hewlett-Packard\DDMI

For Windows Server 2008 installations, the default Data folder is:

C:\ProgramData\Hewlett-Packard\DDMI

The location of the Data folder is represented by <*DataDir*> in this document. The <InstallDir> represents the location of the DDM Inventory program files.

The following table lists the rights that are applied and added to various folders on the server:

Folder Security

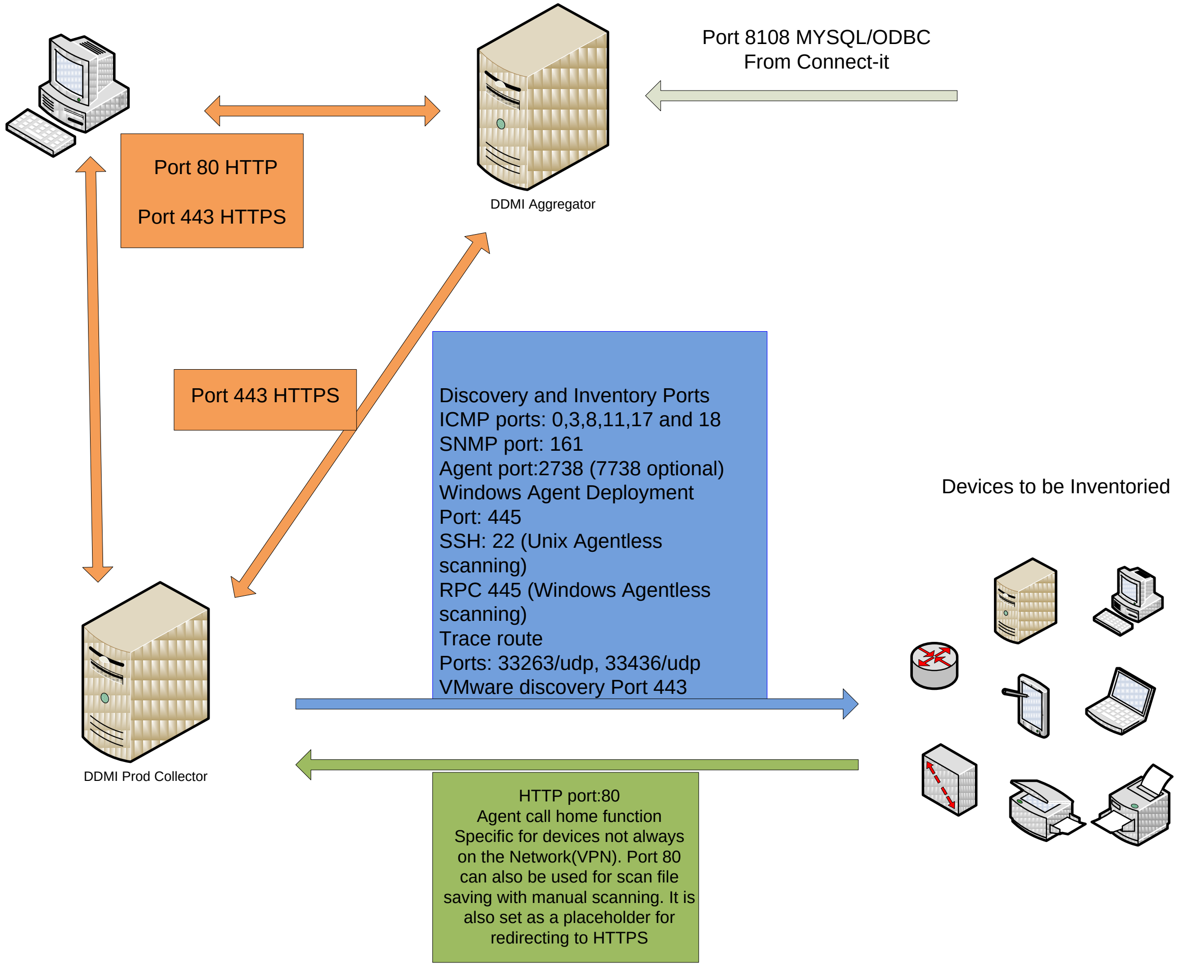
Folder	Security Measure
C:\Perl	Read-only access
<installDir>	Read-only access
<DataDir>\LiveAgents	No Visibility
<DataDir>\Scans	Read-only access
<DataDir>\Cert	No Visibility
<DataDir>\Database	No Visibility
<DataDir>\PrePostScripting	No Visibility
<DataDir>\AutoPass	No Visibility

Registry Key	Security Measure
HKLM\SOFTWARE\Hewlett-Packard\ED	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedAgentComm	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedApache	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedApacheSSL	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedAuth	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedDiscDB	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedDiscEng	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedEventMgr	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedLogger	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedSched	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedSysmon	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedSysStatus	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedTomcat	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedTplgConv	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedTplgEng	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedWatchdog	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedXmlEnricher	Read-only access
HKLM\SYSTEM\CurrentControlSet\Services\ovedXmlEnricher1	Read-only access

Open ports

When DDM Inventory cannot communicate over a WAN connection due to firewalls between the sites, HP recommends that you open the ports required by DDM Inventory. A complete list of ports can be found in the *Planning Guide*, a PDF version of which, planning.pdf, is available in the following folder. C:\Program Files\Hewlett-Packard\DDMI\<version Number>\Documents\ Addtionaly you can access these documents by selecting the DDMI program group from the start menu.

Figure 2: Overview of used TCP/UDP ports



Discovery and Inventory Ports
ICMP ports: 0,3,8,11,17 and 18
SNMP port: 161
Agent port:2738 (7738 optional)
Windows Agent Deployment
Port: 445
SSH: 22 (Unix Agentless scanning)
RPC 445 (Windows Agentless scanning)
Trace route
Ports: 33263/udp, 33436/udp
VMware discovery Port 443

HTTP port:80
Agent call home function
Specific for devices not always on the Network(VPN). Port 80 can also be used for scan file saving with manual scanning. It is also set as a placeholder for redirecting to HTTPS

In the figure above we display the TCP/UDP ports that are required to talk and communicate with devices in the network.

SNMP V1 and V2, community strings and DDM Inventory (2)

SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes. These processes report activity in each network device, such as a hub, router, or bridge, to the workstation console that is used to oversee the network. This process must be administered and controlled by the network administrator.

The agents return information contained in a MIB (Management Information Base). The MIB is the data structure that defines the information that is obtainable from the device, which determines those devices that can be remotely controlled. Originating in the UNIX community, SNMP has become widely used on all major platforms.

Securing the information contained in the MIB is done with a community string. The SNMP Read-only community string is similar to a user ID or password that allows access to a device's statistics. The

SNMP Read/Write community string is also similar to a user ID or password that allows you to set information on the device and change some of its options.

Warning: A device's community string is similar to an administrator's password and should be stored in a secure manner.

One reason why an organization may not enable SNMP in the network is the current Cert Advisory (http://www.cert.org/advisories/CA-2002-03.html). This advisory was issued for SNMP v1, which SNMP v2 uses. Each manufacturer identified in the cert has identified the issue and has offered patches for their products. These patches attempt to prevent the vulnerabilities identified by the advisory.

In DDM Inventory 9.30, HP uses the SNMP service from Microsoft, which was also affected by the vulnerability. Microsoft issued a Security Bulletin on February 12 2002 with an update on May 9, 2003 (http://www.microsoft.com/technet/security/bulletin/MS02-006.mspx).

DDM Inventory runs on either a Windows XP Professional Server or a Windows 2003 Enterprise Server. It will use the SNMP protocol for aiding in the modeling of devices in the network and will install the Microsoft SNMP services for discovery of DDM Inventory server itself.

HP relies on our customers to conform to the CERT Advisory board and apply patches and corrections to the network devices that are vulnerable.

SNMPv3 and DDM Inventory

With the support of SNMPv3 we can now have a more secure connection between DDMI and the devices using SNMPv3. SNMPv3 uses DES and AES encryption. DES has 56bit key length and AES comes with 128bit keys. DDMI uses net-snmp library v5.3 for access to the devices and works with a username/password rather then a community string. It is considered to be a more secure connection over it's pervious version. SNMP should be used to aid in the discovery of devices in the network.

VMware Communication and Credentials (3)

For VMware discovery DDMI is using VMware API calls. These are third party open source APIs designed to be faster and more efficient. The design information can be found at http://sourceforge.net/projects/vijava/ and future development for DDMI will be considered here.

Host servers did not really like agents to be installed and with the introduction of VMware ESXi this was locked down and DDMI Agent could not be installed. In the past DDMI would collect the data from VMware hosts using the agents. Now with the Java Based APIs DDMI can now access the host to collect hardware data about the server. Using only read only credentials DDMI will collect and store the hardware information without installing agent or running an inventory process. These credentials are stored at the DDMI Server and configured in the Virtualization Profile. A list of attributes can be seen in the below table.

DDMI		VMware
Table	Field	Object
hwCPUData	hwCPUCount	**HostCpuInfo**
hwCPUs	hwCPUType	**HostCpuPackage**
hwBusData	hwCardSummary	**HostPciDevice**
	hwSystemClockMHz	**HostCpuPackage**
hwCards	hwCardBus	**HostPciDevice**
hwBiosData	hwBiosSource	HostBIOSInfo
	hwBiosAssetTag	**OtherIdentifyingInfo**
		HostSystemInfo

hwMemoryData	hwMemTotalMB	**HostHardwareInfo**
hwOsData	hwHostOS	**AboutInfo**
	hwOSTimeZone	**HostDateTimeSystemTimeZone**
hwNetworkTcpip	hwTCPIPInstalled	
	hwIPHostName	**HostDnsConfig**
hwNetworkShares	hwNetworkShareName	**HostFileSystemMountInfo**
hwNICGateways	hwNICGateway	**HostIpRouteConfig**
hwNetworkCards	hwNICDescription	**PhysicalNic**
	hwNICUsesDHCP	**HostIpConfig**
	hwNICInterfaceName	**HostIpRouteConfig**
		PhysicalNicLinkInfo
		PhysicalNic
hwNetworkDNSServers	hwNetworkDNSServer	
hwNICIPAddresses	hwNICIPAddress	**HostIpConfig**
hwOSUserProfiles	hwOSUserProfileName	**UserSearchResult**
hwOSContainers	hwOSContainerName	**VirtualMachine**
	hwOSContainerRoot	**VirtualMachineConfigInfoDatastoreUrlPair**
	hwOSContainerStatus	**VirtualMachine**
hwOSContainerNetworkDevices	hwOSContainerNetworkDevice	**VirtualPCNet32**
	hwOSContainerNetworkDeviceAddress	**VirtualMachineGuestSummary**
hwOSClusterInfo	hwOSClusterState	**ComputeResourceSummary**
	hwOSClusterName	**ComputeResource**
hwOSClusterNodes	hwOSClusterNodeName	**HostSystem**
hwOSServices	hwOSServiceName	**HostService**
hwNetworkDNSServer	hwNetworkDNSServer	**DNSConfig**
hwMountPoint	hwMountPointVolumeName	**DatastoreInfo**
	hwMountPointVolumeType	**VolumeInfo**
	hwMountPointVolumeTotalSize	**HostFileSystemVolume**
	hwLocalMachineID	**SystemInfo**

Agent Communicator Service (ACS) (4)

- *In DDM Inventory you are able to deploy a scanner, run a scanner and retrieve a scan file from the scanner execution. This is done with the DDM Inventory Agent Communicator. The client that the agent is installed on is never able to request information from the DDM Inventory server. Communication is done using a 100% standard authentication/encryption method. This is identical to the one used to secure web servers. Communication is initiated by the DDM Inventory Server using a HTTPS 2048-bit RSA. (public / private key method) (Rivest-Shamir-Adleman) or RSA is a security method designed by RSA Security Inc in Bedford MA. It uses a two-part key. The private key is kept by the owner; the public key is published. Data are encrypted by using the recipient's public key, which can only be decrypted by the recipient's private key.*
- *Line encryption, to all clients, is using 128-bit 3xDES (Data Encryption Standard). Server and the Agent have both a pair of keys and a public cert in a X509 format.*
- *When the agent is being installed in a Windows environment it requires administrator-level rights to install the service. A UNIX® environment requires the agent to be installed with root-level rights.*
- *DDM Inventory Client Agent uses TCP/IP port 2738 for server to client communication. The information is passed over the TCP/IP port using the public key method. 7738 is also a*

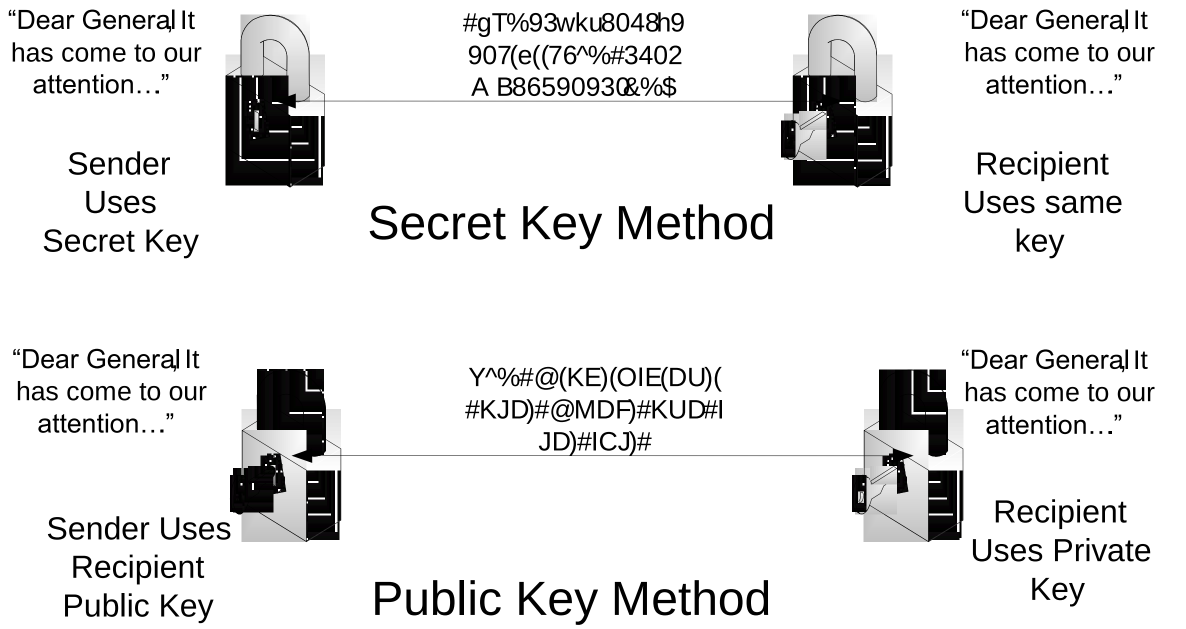
configurable port and register with IANA (Internet Assigned Numbers Authority) [*http://www.iana.org/assignments/port-numbers*](http://www.iana.org/assignments/port-numbers)

- *Once installed the Agent will listen passively and will challenge server identity when contacted. With a sealed certificate the Agent will refuse communication with any other server.*

Secure Key Exchange

- *There are two different methods used in key reading: the secret method and the public key method.*
- *The secret method uses the same key to encrypt and decrypt transmitted data. The problem with this method lies in transmitting the key to someone so they can use it. For example, in a Secret Key scenario, an Army Major sends information to a General using a secret key. The General reads this information using the same secret key.*
- *The public key method uses two keys. One is kept secret and never transmitted, and the other is made public. Sometimes the public key method is used to send the secret key used in the private method, and then the message is sent using the private key method. For example, the Major sends the information using a Public Key that was received from the General. The General then uses the private key to read the message. The private key is never sent.*
- *The following diagram depicts simple data transmission using both methods.*

Figure 3. Secret Key method versus Public Key method


"Dear General, It has come to our attention…"
#gT%93wku8048h9 907(e((76^%#3402 A B86590930&%$
"Dear General, It has come to our attention…"
Sender Uses Secret Key
Secret Key Method
Recipient Uses same key
"Dear General, It has come to our attention…"
Y^%#@(KE)(OIE(DU)(#KJD)#@MDF)#KUD#I JD)#ICJ)#
"Dear General, It has come to our attention…"
Sender Uses Recipient Public Key
Public Key Method
Recipient Uses Private Key

The Agent is a service, and normal users in a network cannot enable or install such a service. For Windows agent deployment, an administrative account is added to DDM Inventory Deployment Credentials. This account can be either the Local Administrator or a Domain Admin with rights to install services on the workstation. Once added, DDM Inventory uses these credentials to install the agent as a service. It is important to have this type of communication between the client and the server because the client side is in locations that tend to have security concerns. Compromising the Agent Binary will not have an effect on the server security. In DDMI, every effort is made to secure the data that is collected from the devices in the network with the agent secure key exchange.

Agent-less Communication

Additionally DDMI offers a method to use login credentials to access and run the Inventory process. This method allows you to use the same secure methods for accessing systems over the network. It provides an efficient way to solve the problem of installing agents to devices when companies have many agents running in the population. The ACS contacts the device over RPC installs a temporary service and uses the same methods mentioned above to secure the connection and collect the inventory. For UNIX this agentless inventory process uses SSH to secure the connection and run the inventory.

UNIX Agent deployment

In UNIX environments a custom script can be configured to deploy the agent to the UNIX systems from DDM Inventory. This deployment method allows an IT department to create a custom deployment process using a batch script and other programs. For example, it should be possible to implement a custom UNIX agent deployment using Secure Shell Server (SSH).

This custom script must receive the following information via command line parameters:

- *IP address of the device where the agent needs to be installed.*
- *NMID of the device in the DDM Inventory database. NMID is an abbreviation for Network Management Identifier, which is the ID (key) of the device or port in the Appliance.*
- *Version of the Win32 agent media to be installed (for example: "9.30.000.2244"). The agent media files need to be taken from the* `Live Agents` *directory.*
- *Version of the AIX agent media.*
- *Version of the HP-UX agent media.*
- *Version of the Linux agent media.*
- *Version of the Solaris agent media.*
- *Maximum bandwidth for the operation, in KB per second; or 0 (zero) if no limit was configured.*
- *The network workgroup from the network model. This is detected from the NetBIOS workgroup name, which usually corresponds to the destination computer's domain name.*

The deployment is considered to be successful if the program returns an exit code of 0.

Once the agent is installed to the UNIX systems, the same public and private keys are used as the example above shows.

Note: Additional details on creating a deployment metod for UNIX can be found in the Configuration and Customization guide under the Agent Communication Configuration chapter.

SSH Key Authentication Communication

With UNIX, deployment becomes a difficult issue with the DDMI Agents. Using similar methods as within Windows Agent-less methods, customers can use SSH to connect to a UNIX device and exchange a secure key of their choosing. With the added security users can now use DDMI to secure the connection to the UNIX devices and collect the inventory. You need to create the key using SSH Key generation and uses the public key that is generated with the DDMI configurations. Steps to add the public key can be found in the Installation Guide of DDMI.

Windows Firewalls

When using the Windows Firewall, certain settings can cause communication problems between the agents and the DDM Inventory server. The below information are recommended settings when DDMI is actively discovering devices directly and not using the DDMI Passive discovery logic.

Using GPO (Group Policy Objects) is by far the easiest way to administer and control the configuration in a Windows Firewall. The following is a list of ports and settings needed in the

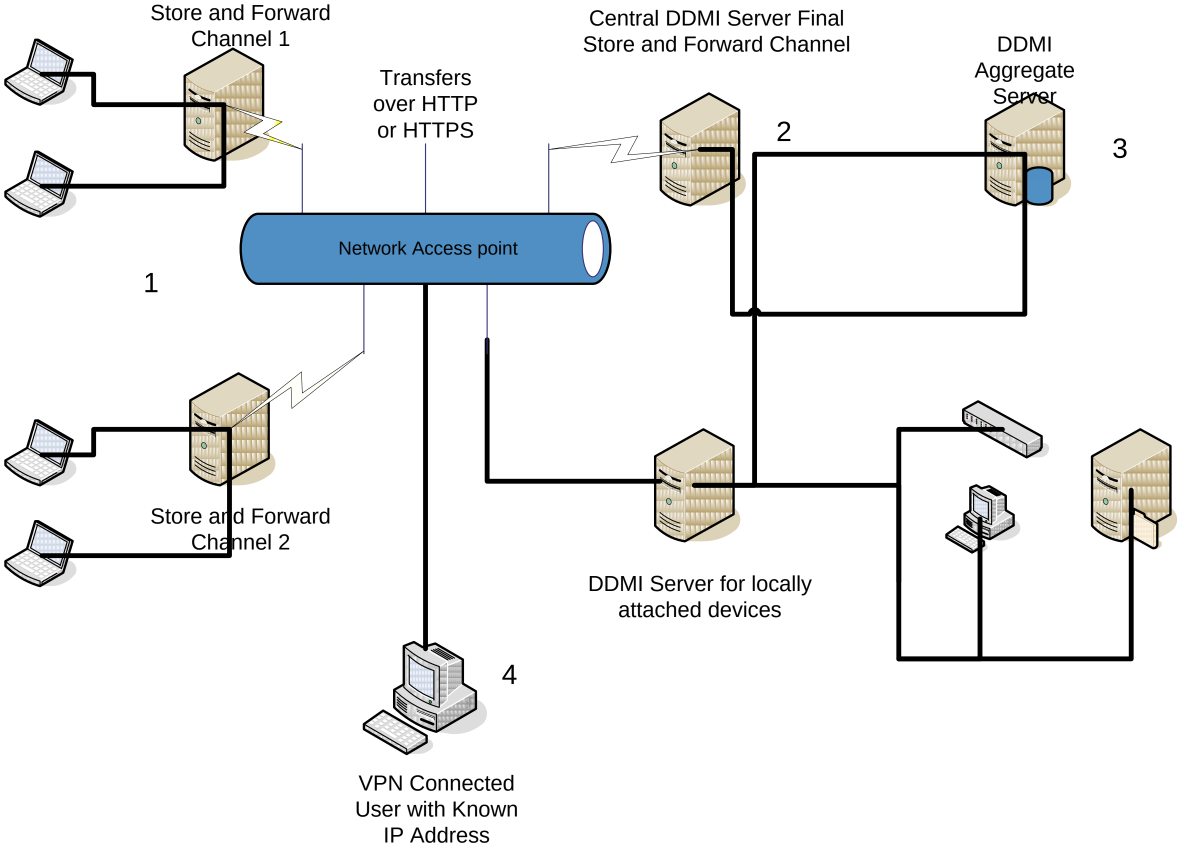
Windows Firewall to allow the DDM Inventory server to properly communicate with the DDM Inventory agent.

Policy	**Setting**
Windows Firewall: Allow ICMP Exceptions	
Allow outbound destination unreachable	Enabled
Allow outbound source quench	Disabled
Allow redirect	Disabled
Allow inbound echo request	Enabled
Allow inbound router request	Enabled
Allow outbound time exceeded	Disabled
Allow outbound parameter problem	Disabled
Allow inbound timestamp request	Enabled
Allow inbound mask request	Enabled
Allow outbound packet too big	Enabled
Policy	
Windows Firewall: Allow Remote Administration Exception	
Windows Firewall: Allow Remote Desktop Exception.	
Extra Registry Settings:	
`SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyOpenPorts\Enabled`	
`SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyOpenPorts\List\2738:TCP:xxx.xxx.xxx.xxx/x:enabled:discovery Service`	2738:TCP:xxx.xxx.xxx.xxx/x:enabled:discovery Service
`SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyOpenPorts\List\2738:UDP:xxx.xxx.xxx.xxx/x:enabled:discovery service`	2738:UDP:xxx.xxx.xxx.xxx/x:enabled:discovery service
`SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\GloballyOpenPorts\List\2738:UDP:xxx.xxx.xxx.xxx/x:enabled:discovery service`	2738:UDP:xxx.xxx.xxx.xxx/x:enabled:discovery service

Remote administration

In order to have the agent installed on the end user system using RPC (Remote Procedure Call), a local administrator or domain administrator who has permission to install a service must be added to the Deployment Credentials list. This serves as a login account to the system based on your Windows security level. After the agent is installed, the access point to the systems is no longer needed because the DDM Inventory server handles communications with devices on which an agent is installed. RPC is used only on Windows systems, in a domain or any other account that has local administrative access to the system. In some cases you need to configure the Windows firewall

Figure 4: Overview of Remote Administration Features


Store and Forward Channel 1
Transfers over HTTP or HTTPS
Central DDMI Server Final Store and Forward Channel
DDMI Aggregate Server
2
3
Network Access point
1
Store and Forward Channel 2
DDMI Server for locally attached devices
4
VPN Connected User with Known IP Address

Store and Forward

Store and Forward is a capability to move DDMI scan files from inside secure networks to a central area for processing. It's designed to use Manual DDMI Scanners for forwarding files and uses one TCP port to facilitate an automated process for transferring scan files.

By default the Store and Forward installer will use TCP/UDP port 5005 but is configurable to any TCP/UDP port that may already be used between networks. In figure 4, above, we show a simple configuration between a chain of store and forward networks. Manual scanners are configured to save scan file using HTTP or HTTPS to one of the Store and Forward servers. Once receive the scan files are sent to the central Store and forward server for processing using either HTTP or HTTPS over a configured port.

Call Home Feature

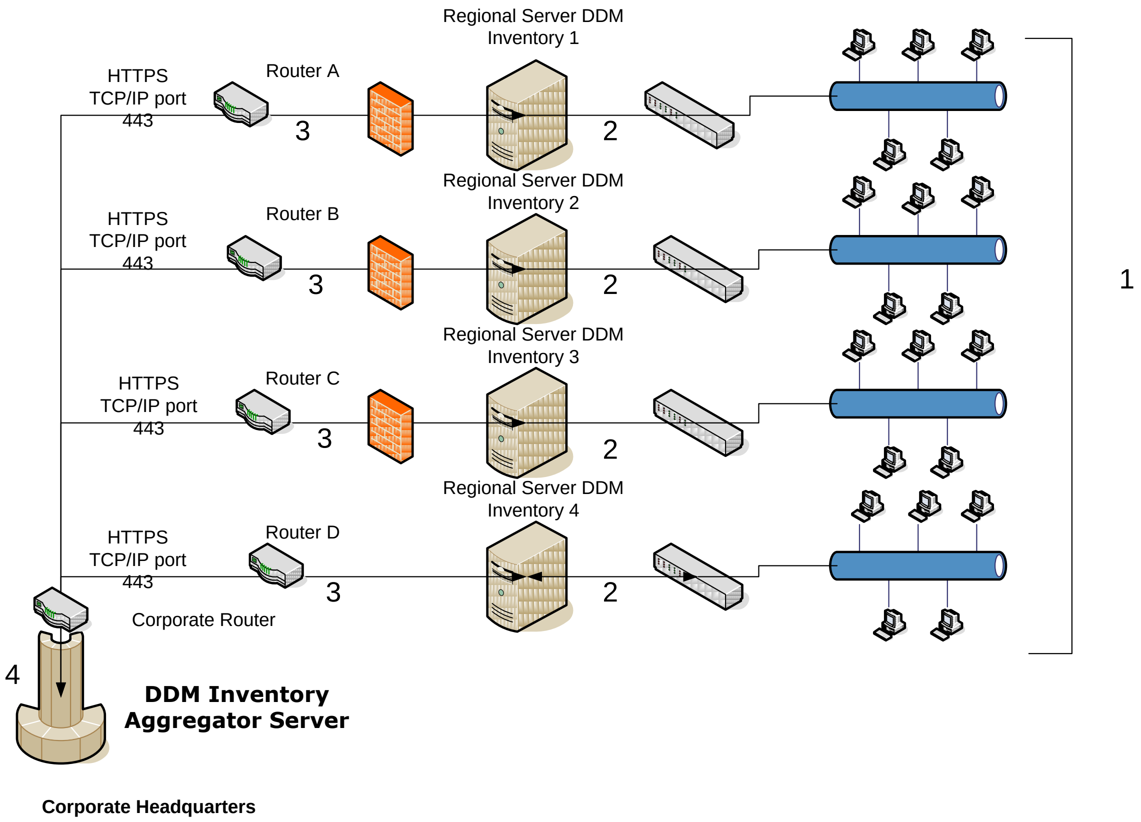
When devices do not connect on a regular basis you want to be sure that the device is discovered when it's on the network. Using Port 80, HTTP, devices tell the DDMI Server that they are ready for inventory. This allows the DDMI server to prioritize the device and get the inventory as they are connected. This ensures that inventory results are kept up to date keeping the device within policy of the company. Once the DDMI Server receives the connection the Agent Communication Service takes over and runs the inventory.

Aggregator security

The following diagram depicts the aggregator security configuration:

- *Aggregator security*
- *Workstation collection (1)*
- *Server configuration (2)*
- *Transfer of information (3)*
- *DDM Inventory aggregator consolidation (4)*

Figure 5. Aggregate security



How is information transferred in an Aggregator configuration?

The diagram above illustrates an DDM Inventory Aggregator configuration that enables you to manage up to 50 DDM Inventory servers. This configuration is intended for a very large network, or for a network where there is a firewall between sites for security reasons. Each server in an Aggregator configuration should be set up in the same way, and should use the same agent security keys (and certificate) so that the same security key can be used throughout the workstation population. The Aggregator acts as the main point through which information is transferred to a target system such as Asset Manager.

The DDM Inventory Aggregator server is also configured as a single server, but an Aggregator License is used over a standard license. Because of the role of the DDM Inventory Aggregator server, you can configure it to discover up to 100 devices with a maximum of 600 ports. HP suggests that you use the DDM Inventory Aggregator server to discover the Regional DDM Inventory servers, the routers that are configured between the sites, and any other core network device that controls communications between the sites. This allows for quick viewing of the devices that make up the WAN connection.

Note: For information about the hardware that should be used in the Aggregator server, see the *DDM Inventory Installation and Initial Setup Guide*.

End Point Collection(1)

Workstations are modeled by the regional DDM Inventory process, and then agents are sent for deployment. Each device in the regional network is then sent a scanner. The resulting scan file is merged with the discovered information into the Discovery database.

Server Configuration(2)

Each DDM Inventory server is configured with the security data described above, and collects all the information for each domain. Single-server security configuration enables an administrator to control the information in the region for which the administrator is responsible. At the same time, corporate headquarters can collect the information in a central repository.

Transfer of Information(3)

Information is transferred from the server over HTTPS using TCP/IP port 443, compiled in the Aggregator, and moved to the Discovery database.

DDM Inventory Aggregator consolidation(4)

Information can be moved from the Discovery database to Asset Manager. You can view reports and statistical information for each regional server from the Aggregator server.

Conclusion

Security features in DDM Inventory 9.30 provide for effective control of the data within the server. While vigilance is always essential to protecting sensitive data, following the recommendations in this document can help ensure the security of communications on your network and maintain the security of data that is stored on the DDM Inventory server.

For more information

Please visit the HP OpenView support web site at:
http://www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by being able to:

- *Search for knowledge documents of interest*
- *Submit and track progress on support cases*
- *Submit enhancement requests online*
- *Download software patches*
- *Manage a support contract*
- *Look up HP support contacts*
- *Review information about available services*
- *Enter discussions with other software customers*
- *Research and register for software training*

Note: Most of the support areas require that you register as an HP Passport user and sign in. Many also require an active support contract.

To find more information about support access levels, go to the following URL:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to the following URL:

http://www.managementsoftware.hp.com/passport-registration.html

Trademark acknowledgments, if needed.

4AA2-xxxxENW, Created 2011