Global Information Assurance Certification Paper

Michael A. Helm
CCNA, MCSE, MCP+I, CNA
11/17/2001

Introduction

This paper will describe the basic components, functions, and security methods that make up the GroupWise e-mail system by Novell, Inc.

Information included is a collection of numerous publications that cover the history, administration, security, encryption, and technical information documents to configure, manage, and secure a GroupWise e-mail system.

History

GroupWise originated from the WordPerfect Corporation and a product that was called WordPerfect Library 1.0. WordPerfect included an email component with group scheduling that was called WordPerfect Office 2.0. Novell bought WordPerfect and continued development on their last version called WordPerfect Office 4.0. Novell sold WordPerfect but retained the Email System and continued to make upgrades that enhanced the product while integrating it into Novell's existing Network Operating System and Novell Directory Services structure creating the GroupWise application.

Overview

GroupWise is the third most popular e-mail system in use today. GroupWise is a proprietary collaborative system that is an assemblage of directory stores, message stores, client software, message transport mechanisms, and administrative software components.

This document will use the hierarchical architecture to present the GroupWise System and its basic components, functions, and security methods. The components are located in the architecture to provide for a scalable, flexible, and distinct scope of administration. The architecture consists of domains, administrator component, post offices, gateways, and clients.

Domains

The GroupWise domain provides administrative links, controls message routes, and synchronizes the directory stores. A domain transfers messages between post offices, clients, GroupWise domains, and foreign domains. Domains also synchronize the directory stores throughout the mail system to ensure consistency. This e-mail system does not provide its own administrative module; instead, it uses plug-ins that provides links to the Novell Directory Services, which provides the administration for the domain.

The GroupWise system can contain a primary, secondary, external, and foreign domain. The primary domain is mandatory because it holds every object and provides a synchronization point for the entire system. This synchronization between the Novell Directory Services snap-in and the message transfer agents ensure system consistency. The secondary domains allow

administration to be distributed throughout a Wide Area Network. Each secondary domain contains its own database and directory structure with one or more post offices. The external domain is an individual primary domain with pointers or links to show routes between the two domains. The foreign domain also serves as a pointer to non-GroupWise systems. The combination of all these domains work together to create a message transport system.

All domains use a message transfer agent to configure the GroupWise domain. This message transfer agent (MTA) is a NetWare Loadable Module (NLM) that actually delivers the mail between domains, post offices, clients, GroupWise and foreign domains. When the MTA loads, it must point to the root of the domain directory. This directory contains the WPDomain.DB database that holds the configuration information for linking and routing within the domain.

Administrator Component

The GroupWise administrators are the only accounts that need access to the domain directory. The administrators in GroupWise can be configured in several different ways. Each configuration has good and bad points and these points fluctuate based on the size of your organization and the infrastructure that is available. The three standard configurations of the GroupWise Administrator are:

1. System Administrator
2. Single GroupWise Administrator
3. Multiple GroupWise Administrator

The system administrator configuration is the easiest to implement because the GroupWise administrator account just emulates the Netware system administrator's security. When a GroupWise administrator account is created, the account is given security equivalent to the Admin account in the Novell Directory Services tree. This gives the GroupWise administration full access to the complete server and tree and, therefore, access to the GroupWise components. This is the least secure configuration but provides complete access to GroupWise and network operating system. This account has excessive rights to perform the job functions of a GroupWise administrator, and is generally used in a one person IT shop or where one person handles both the Netware Server and the GroupWise services.

A single GroupWise administrator is an account that manages the entire GroupWise system, but does not have administer privileges to the rest of the server or the Novell Directory Services tree. This account must have directory, object, and property rights that are only needed to administer the GroupWise system. This configuration can also be used in a single person IT shop were one-person handles the Netware Server and the GroupWise services, but the administrator would have to logon to accounts based on the functions that he/she is performing. The downfall is the administrator has to login for each function, but having several accounts prevents any single account from having full access to the email and NetWare Operating System. Implementing this structure provides security by minimizing any breaches to the users account.

Using the Multiple GroupWise Administrator breaks down administration responsibilities into specific functions of GroupWise. A single administrator disburses the property rights providing limited access to the scope of administration. These administrative divisions are a domain administrator, post office administrator, and a link configuration administrator.

> The domain administrator carries file, object, and property rights to create and manage a single GroupWise Domain.
>
> The post office administrator has all directory, object, and property rights to create and maintain a single GroupWise post office.
>
> The link configuration administrator has all of the directory, object, and property rights needed to create and maintain the links between domains.

The separation of the administration functions increases the security of the email system. The distribution of rights prevents any single security breach from accessing the overall mail system. In addition, by defining a clear and concise work function, you have further defined the scope of administration and security. This configuration provides enhanced benefits to security but it does demand staffing and coordination between the different types of administrators.

Post Offices

A post office is a logical grouping of users based on their accessibility, location, and traffic patterns that have been generating. The Novell Directory Services represents the post office logically while the file directory is the physical structure of a post office on the server.

A post office can consist of users, accounts, external entities, resources, nicknames, distribution list, and libraries. These objects are associated to a specific post office representing a single sender and recipient of messages or a group of senders and recipients. Every object has its own specific function that amalgamates with other object to provide services. A user connecting to a single mail account and sending messages from a single user to multiple users is an amalgamation of the user, account, and distribution list objects.

The post office also consists of components. These components are a database, post office agent (POA), message store, guardian database, and document store.

The post office database is called wphost.db. This database makes up part of the directory store and provides an index that users make use of when they access the address book in the email software. This administration component of the post office agent updates the database after it receives administrative messages from the message transfer agent generated by the NetWare Administrator utility.

The post office agent (POA) component is a Netware loadable module that updates the WPHost.DB database. The POA is responsible for all administrative updates coming from the NetWare Administrator. This agent is the central software of the post office. It is the connecting point to the post office for users connecting through client/server sessions and it provides messages delivering to and from other post offices. The POA monitors the massage store and the queue for incoming and outgoing messages. It creates and delivers status messages to the sender, indexing library objects and their databases, and maintains the integrity of the message store databases.

The post office message store consists of a database system, which is a single database file with multiple message entries. This database model stores messages and places large attachments into discrete files that are placed into subdirectories to maximize the efficiency within the database distribution lists. The message database (MSGxx.DB) and user database (Userxxx.DB) are required database in all post office message stores.

Gateways

The GroupWise email system has several gateway configurations to access other systems. These gateway allow access to systems via asynchronous, Internet, and Web Access, etc. This paper will cover the basic gateway available in the GroupWise system:

The GroupWise Asynchronous gateway is used for indirectly connected users. This Asynchronous gateway is a NetWare Loadable Module (NLM) that can link domain-to-domain, GroupWise system to External systems, and remote user to the system. This gateway provides a connection that copies the database to remote computers and the data is work on offline, and then copied back to the server. An Asynchronous gateway is uses COM ports,digicards and other multiport card installed on the Netware Server.

Even though GroupWise is a proprietary system; it supports other open systems with a GroupWise Internet Agent (GWIA). The GroupWise Internet Agent (GWIA) is a translator or gateway for GroupWise to communicate with other systems on the Internet. This agent allows communication with five different open-standards:

1. Simple Mail Transfer Protocol (SMTP)
2. Multipurpose Internet Mail Extensions (MIME)
3. Lightweight directory Access Protocol (LDAP)
4. Post Office Protocol (POP)
5. IMAP4 (Internet Message Access Protocol)

Web Access gateways allow users to access the GroupWise mail using web browsers with an online http connection. No data is copied to the remote connection and all transaction must be done on the active connection.

GroupWise client

A GroupWise client is the front-end application at the workstations that perform the first part of the mail delivery function by passing the message to the message transfer agent or the post office agent that access the associated mailbox (message store). A client can connect to a server using direct, client/server, or remote access methods.

Security

The review of policies, procedures and training programs of the organization should be the start of the security assessment. The main physical risks that need to be reviewed are physical access, social engineering, data leakage, and other organizational structural weaknesses. The technological risks and attacks are information being changed, unauthorized access, virus attacks, and denial of service. All of these risks should be reviewed and plans of actions should be prepared, implemented, and reviewed to increase the security of the system.

The foundation of the security in GroupWise is the Network server, network operating system and the Novell Directory Services that the application runs on. So the application is only as secure as this foundation. The administrative links to GroupWise require a username and password to enter the Novell Directory Services as an object that has file, object, and property rights needed to manage the e-mail.

The domain security is established by incorporating a MTA password to communicate with other servers. This password is stored in the startup.mta files located in the sys:system directory of the Novell Server. The administrators are the only account with file system access to the system directories, domain directories, and domain objects and every message or attachment that leaves the MTA is encrypted before being broadcasted onto the network.

A post office can operate in a high or low security. The high level security requires the network user ID to match the GroupWise user ID. Low-level security does not verify the network User ID. To secure e-mail account that is operating with low-level security a separate password must be created in GroupWise on the post office.

A post office can be divided into two separate functions. The program directory should be access with on Read and File Scan rights. The object store should have file rights based on the access type used by the client. The direct access method connects using an UNC or mapped path to the server. It requires that the user have file system rights to read and File Scan in the software distribution directory, read and file scan directory rights to the stored messages directory, and the Novell Directory Services browse object right to the post office. To protect stored messages from unauthorized access GroupWise uses encryption. The client/server client does not need access to the directory store. The client/server connection only needs rights to the software distribution directory and does not need any rights to the post office directory. The client/server connection is the recommended method because it provides the most security. The remote connection method

is the weakest security type. This connection uses a gateway password to access the post office and never checks for an individual's mailbox password. This leaves the system open to anyone entering on the gateway password. All of these client configurations provide connectivity, but each one must be evaluated base on the benefits and downfalls of each configuration.

The gateways act as a translator that not only acts as a communication point between the proprietary system and other systems, it also provides entry and exit points for the monitoring of e-mail. The SMTP security dialog protects the GWIA from Spam and mailbombs. This program can be set to reject mail where the source cannot be identified, or by setting the mailbomb thresholds to prevent any host from dominating a specific inbound thread.

All transactions that transverse the Internet agent are susceptible for virus scanning and monitoring procedures. This Internet Agent can redirection mail to different directories so that other processes may be performed before forwarding the messages. This allow for a dynamic evaluation of all messages entering and exiting the email system. The GroupWise gateway requires that user passwords be set with the property page in NetWare Administrator each specific gateway.

The GroupWise client encrypts any message and attachment before sending the message onto the network while providing several security configurations on the client application itself like:

- Defines the password for an individual mailbox.
- Implement proxy access to another user's mailboxes
- Conceal Subject, Status Tracking, Notifications, Require password to complete route
- Digital Signature (S/Mime version 2)
- Encryption (depending on security provider)
- An administrator cannot establish any proxies.
- An administrator in Netware can reset or clear the password through NetWare directory service to override-forgotten passwords, but the administrator cannot view an existing password

Encryption

GroupWise encryption is internal and cannot be turned off manually. When an object is defined, a pseudo-random key is generated. The object store and messages are encrypted before being transmitted using a symmetric (single-key). The encryption key is created from the sending user ID, sending Post office, sending domain, type of message, and time values. Because the time value is used in the creation of the encryption key all messages are encrypted with a unique key. GroupWise can maintain it's proprietary security when leaving the GroupWise system if the source and destination systems are GroupWise. This gateway feature is a passthrough configuration. A passthrough message is when the entire GroupWise message is encapsulated with a protocol and the message maintains the GroupWise proprietary encryption. If the

destination system is not a GroupWise system you can use one of these third party programs and others prior to sending the message on to the network.

> Secure/Multipurpose Internet Mail Extensions is based on the popular Internet MIME standard. It provides cryptographic security services for electronic messaging applications that include authentication, message integrity, and non-repudiation of origin, and privacy and data security using encryption. RC-2/40 and tripleDES encryption needs to be active on the sending and receiving agents.
>
> PGP uses the RSA encryption algorithm for its security.

All of the securities that GroupWise support is based on the common algorithms like RC2 and RC4. RC-2 is a conventional block encryption algorithm with an input /output of 64 bits each. The algorithm can handle up to 128 bytes for the key size, but he base system in 8 bytes. The RC-4 is a stream cipher symmetric key algorithm. It uses variable length key from one to two hundred and fifty-six bytes to initialize a 256 byte state table this table generates pseudo-random bytes and then to generate a pseudorandom stream which is XORed with the plaintext to provide cipher text. This cipher text is limited to 40 bits due to export restriction but can use up to 2048 bit.

Summary

The GroupWise email system is a proprietary collaborative product. The security is initiated based on the proprietary focus of the system; its encryption for storage and transmitting of data, and it uniqueness compared to other email structures. This system provides integration between the client, post office, domain, gateways and operating system of the server to imbed a depth of defense within the application's design. The security methods can be incorporated on the perimeter of the system, between the architectural components, within the agents and client applications, and on the computer file systems in which they reside. Even when leaving the scope of the proprietary system this email can utilize different techniques to maximize the safety of the messages being transported. All together this system starts with a solid foundation of security while providing the administrators the ability to implement enhancements within numerous areas of the GroupWise design.

References

Howard Tayler, Tay Kratzer & Ross Phillips, "Administrating GroupWise 5.5" McGraw-Hill Publishing 1999

Novell, Technical Information " Novel GroupWise System Security", October 1999
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2954214.htm

Novell, "Novell GroupWise Security Book 1: Administrator, Agent, and User Rights"
URL: http://novell.curtin.edu.au/grpwise/ADMIN/sb100001.htm

"Secure Hash Standard", National Institute of Standards and Technology ,FIPS PUB 180-1 April 7, 1995
URL: http://www.itl.nist.gov/fipspubs/fip180-1.htm

Ronald Rivest, "RC4 Encryption Algorithms
URL: http://www.ncat.edu/~grogans/algorithm_history_and_descriptio.htm

Ronald. Rivest, "A Description of the RC2® Encryption Algorithm", MIT Laboratory for Computer Science RFC-2268 March 1999
URL: http://www.imc.org/rfc2268

Bob McKindles, "Use the Quick Viewer to Avoid Viruses", Novell Inc., 6 November 2001
http://www.novell.com/coolsolutions/gwmag/features/tips/t_quick_viewer_virus_gw.html

S. Dusse, P. Hoffman, B. Ramsdell, L. Lundblade, L. Repka, "S/MIME Version 2 Message Specification", March 1998

Novell, Inc, "A History of GroupWise"
http://www.novell.com/coolsolutions/gwmag/features/gw55backgrounder.html