Global Information Assurance Certification Paper

Securing GroupWise

Author: Leslie N. Helou
Version: 1.2f
Certification: GSEC

Introduction

As additional services are added to the GroupWise system so are additional security risks. Even though Novell products typically deny access to services unless specific rights are given, there are a few exceptions worth noting that relate to GroupWise. The idea of providing only enough access to perform ones' job does not hold true in several areas of the GroupWise system. The purpose of this paper is to provide administrators with a guide to follow when enhancing, or checking, the security of an existing GroupWise 5.5 and GroupWise WebAccess system. Access will be set so that a single administrative account will be able to properly maintain the GroupWise system while preventing unwelcome tampering from unauthorized individuals. Additionally, access should be set so that only those users that need a particular service can use it. Throughout the paper, the following assumptions will be made:

1. GroupWise and WebAccess have been installed with the default configuration.
2. The Agents and Clients have the necessary rights to function properly.
3. NetWare Administrator will be used to change the configuration unless mentioned otherwise.
4. The reader will have a general knowledge of NetWare, GroupWise, WebAccess and NetWare Administrator.

Lastly, due to the complex nature of some of the links contained in this document, it is necessary to set Internet Explorer as your default browser. If a link is clicked and Netscape attempts to open it, the browser will likely crash.

Physical and Logical security

When securing a system that runs an e-mail service one must consider both physical and logical security issues. The physical location of the server should be such that only individuals that administer the server should have access to it. Ideally this would be a room that requires a person to use a unique ID, say an electronic passkey, for access. For heightened security the addition of video monitoring equipment may be advisable. Other considerations might include whether the room is adequately ventilated. Propping a door open to increase ventilation can defeat the most intricate lock systems.

Once the physical security issues are taken care of we can focus on logical security. Securing the system console may be a good place to start. If the server will not be accessed remotely there is no need to load the following NLMs; REMOTE, RSPX, RS232 and for Netware versions past 4.x RCONAG6. In the event remote access is needed, access should be secured with a password. This is accomplished by typing LOAD REMOTE followed by a password, and then strike return at the server console. A number of additional options are available to the REMOTE NLM, such as using an encrypted password, and are detailed through the following links:

Encrypted passwords for REMOTE on NetWare v4.x
Encrypted passwords for REMOTE on NetWare v5.x

The server console should also be locked. Under NetWare v4.x this is accomplished by selecting 'lock file server console' from the Console Monitor screen (LOAD MONITOR) and striking return. The user will be prompted for a password and then asked to verify. Under NetWare v5 and later the console is locked using the SCRSAVER.NLM. At the server console enter SCRSAVER ENABLE; DELAY=60;ENABLE LOCK. This will cause the console to lock

after 60 seconds and require an administrator's password to gain access. For additional parameters you may refer to the following link:

SCRSAVER Parameters

Administrator Account Set Up

Setting up an administrator to maintain the server running the e-mail services can be accomplished in two ways depending on the how server administration is set up in one's organization. The e-mail services administrator, here after referred to as E-admin, can simply be made Admin equivalent, that is have full access to the server(s) that the Admin account administers. Using NetWare Administrator, you make the E-admin account Admin equivalent as follows:

1. Double click the E-admin account
2. Click on 'Security Equal To'
3. Click 'Add…'
4. Browse to the context of the Admin account
5. Double click the Admin user object
6. Click 'OK' to save the changes

This is the easiest way to set up the E-admin account but may not be appropriate in organizations where administrative tasks are distributed. In that case, specific rights will need to be assigned. There are several ways to set up a distributed system, depending on how specialized the administration will be. Tasks could be limited to a single domain, single post office, or the connections between post offices. In order to administer an entire domain the E-admin account must have the appropriate directory and object and property rights. Available rights that apply to directories include Supervisor, Read, Write, Create, Erase, Modify, File Scan, and Access Control which we will abbreviate as S, R, W, C, E, M, F, and A.

The E-admin account must have R and F rights to SYS:PUBLIC, the location of the NetWare Administrator and GroupWise Administrator DLLs. R, W, C, E, M, F, and A should be given for the directories that contain the installed GroupWise agents, domain, post office, software distribution, and library storage files. Note, for systems that contain multiple domains, post offices, and so forth, access should be set on each the E-admin is to maintain. By default, the agents are installed in SYS:SYSTEM. The locations of the remaining directories can be found using NetWare Administrator. Locate the domain object in NetWare Administrator and right click it. From the menu that pops up, select 'Details…'. On the 'Information' page you will see the location of the domain in the UNC field. It will be of the form \\server\volume\directory\subdirectory… The location of the post office can be found in a similar fashion. The location of the library may be the same as the post office. To check the location of the library object in NetWare Administer, right click and select 'Details…'. The 'Storage Areas' page will give the location(s). The software distribution library may be found by right clicking the post office object located in the GroupWise View and selecting 'System Operations…' from the pop up menu. Double click 'Software Directory Management' and its location will be listed.

Depending on the object, available object rights may include Supervisor, Browse, Create, Delete, Rename, and Inheritable that we will abbreviate S, B, C, D, R, and I. Additionally, an object may have the following property rights, Supervisor, Compare, Read, Write, Add Self, and

Inheritable which will be abbreviated S, C, R, W, A, and I. C and D object rights must be given for the container that will hold or holds the GroupWise object. The object property rights need to maintain the GroupWise system is given in Table 1.

Object	Property
Domain	NGW: File ID NGW: GroupWise ID NGW: Language NGW: Link Configuration NGW: Location NGW: Network Type NGW: Time Zone ID NGW: Type NGW: Version Description Members Name
Post Office	NGW: Access Mode NGW: Distribution List Member NGW: Domain NGW: File ID NGW: GroupWise ID NGW: Language NGW: Library Member NGW: Location NGW: Network Type NGW: Resource Member NGW: Time Zone ID NGW: Version Description Members Name
Gateway	NGW: Domain NGW: File ID NGW: GroupWise ID NGW: Language NGW: Location NGW: Network Type NGW: Platform NGW: Time Zone ID NGW: Type Description Name
User	NGW: Account NGW: File ID NGW: Gateway Access

	NGW: GroupWise ID NGW: Mailbox Expiration Date NGW: Object ID NGW: Post Office NGW: Visibility Department Description E-mail Address Fax Number Given Name Last Name Telephone Title
Resource	NGW: File ID NGW: GroupWise ID NGW: Owner NGW: Post Office NGW: Type NGW: Visibility Description Name
Distribution List	NGW: Blind Carbon Copy NGW: Carbon Copy Member NGW: GroupWise ID NGW: Post Office NGW: Visibility Description Members Name
Library	NGW: Archive Max Size NGW: Document Area Size NGW: File ID NGW: GroupWise ID NGW: Library Display Name NGW: Post Office NGW: Starting Version Number Description Members Name
Agent	NGW: File ID NGW: GroupWise ID NGW: Platform NGW: Type Description Name Network Address

External Entity	NGW: Account ID NGW: External Net ID NGW: File ID NGW: GroupWise ID NGW: Mailbox Expiration Date NGW: Object ID NGW: Post Office NGW: Visibility Department Description E-mail Address Fax Number Given Name Last Name Telephone Title

Table 1. (GroupWise 5.5 Security, p. 15-20)

If there are multiple objects (domains, post offices, etc...) that must be maintained, the previous table should be applied to each. Setting object property rights is also done through NetWare Administrator as is outlined below.

1. Locate the object of interest in NetWare Administrator, the GroupWise Domain for example.
2. Right click the object and select 'Trustees of this Object…'
3. If the user, E-admin, is not already a Trustee, click 'Add Trustee…'
4. Browse to the context of the E-admin account, then double click the user
5. Ensure the user is highlighted in the Trustee box and check the appropriate Object rights, Create and Delete for example for the container holding the GroupWise domain.
6. In the Property rights section click on 'Selected properties'
7. Click the first property needed, then while holding down the control key (ctrl) select the rest of the properties one at a time.
8. Click Read and Write in the Property rights section, then click 'OK'.

E-admin will need the 'Write' right to the ACL attribute of the e-mail server in order to unlock a console locked with the SCRSAVER NLM. To give the user this right highlight the e-mail server in NetWare Administrator, right click the object and select 'Trustees of this Object…'. Click 'Add Trustee…', browse to the context of the E-admin then double click the object. In the property rights section click 'Write' if there is not already a check in the box, then click 'OK' to save the changes. If the GroupWise Internet Gateway is installed add E-admin as a gateway administrator. This is accomplished by double clicking the gateway. On the Gateway Administrators page click 'Add…'. Browse to the context of E-admin, double click the user object, then click 'OK'. Do the same for the WebAccess agent and the E-admin account should now have all the necessary rights necessary to maintain the GroupWise system.

Post office security

Post office security has two settings - low (the default) and high. It is recommended to set the security to high for a variety or reasons. If an account has no password and the post office security is set to low, any user, whether authenticated or not, will be able to access the account by simply supplying the user name. Setting the post office security to high will prevent this from happening. If an unauthenticated user attempts to login to a GroupWise account with no password set and the post office security set to high, they may receive the following message:

> Access to GroupWise has been denied. Please ensure that you are using the correct user ID.

Note, neither post office security setting by itself requires the user to set a password. Therefore, there is still the issue that an account without a password can be accessed by any authenticated user that provides the correct user name to the GroupWise client. WebAccess on the other hand will require a password to be set if the post office security is set to high since there is no user authentication involved when accessing the e-mail system over the Web. TID 10052079 reveals a potential security problem when a post office is left with a low security setting. It is possible that one may unknowingly grant e-mail access through a GroupWise Library account. If a user and library share the same name it is possible to login using that name and a blank password. If a password is then supplied, the account will be available through WebAccess.

Security can be set by bringing up the details of the post office(s) in question. On the information page you will be able to change the default security setting by selecting High from the drop down menu. Click 'OK' and the changes are enables. It is also worth noting that if a user sets a password on their account, which is contained in a post office set to low security, the users account is set to high security. This is due to the fact that the security on the users account overrides that of the post office.

GroupWise Internet Agent Security

If users must access their e-mail through POP3 or IMAP4 then we should make some adjustments to the GroupWise Internet Agent, the GWIA. The following is a list of settings that should be checked and are available after double clicking the agent.

1. Both POP3 and IMAP4 are enabled when the agent is installed, if both are not needed then one should be disabled. This can be changed by selecting the POP3/IMAP4 page and unchecking the appropriate option.
2. The default class of service allows all users to have POP3/IMAP4 access. Restricting this service to only those users that need it may prevent the misuse of certain accounts. This can be accomplished by first changing the default class of service to the POP3/IMAP4 from allowed to prevent, and then creating another group that is allowed and add the appropriate users. We begin by selecting the Access Control page, click 'Default Class of Service', then 'Edit…'. On the IMAP4 and POP3 pages select 'Prevent access' then click 'OK'. Next we must create a group to contain the users permitted to use the POP3/IMAP4 services. Click 'Create…' and enter a name, such as "Allowed POP3", then click 'OK'. Select the appropriate service(s), POP3 and/or IMAP4, and select 'Allow access' then click 'OK'. Click the 'Users' button then add the relevant users. Click 'OK' once to be taken back to the 'Access Control' page for additional

changes. Be sure **not** to change the SMTP Incoming or Outgoing settings unless you wish to prevent e-mail from traveling between your environment and the Internet.

3. It is important to disable SMTP relaying. Relaying allows users not authorized on your system to utilize your mail server. Although useful years ago it now used more often by spammers to anonymously send their e-mail. A system that is identified as an open relay may be black listed by other servers. That is, the receiver will reject any e-mail sent from your system, whether it is legitimate or not. Also located on the 'Access Control' page, click 'SMTP Relay'. On the following screen click 'Prevent message relaying' then click 'OK'.
4. To prevent a few users from over taxing the system with large attachments, it would be a good idea to enable a maximum message size for both inbound and outbound traffic. Large attachments should be sent via ftp rather then through e-mail. To ensure this applies to all users, select 'Default Class of Service' then click 'Edit…'. Check 'Prevent messages lager than' and enter a maximum size, say 4,000 Kbytes, for e-mail coming into your system from the Internet. Perform the same task on the 'SMTP Outgoing' tab then click 'OK'. In the event you need an account with the ability to send and receive large files through e-mail simply create another class of service without a size restriction.
5. The internet agent provides a mechanism to prevent the system from a mailbomb attack. That is, an individual tries to overwhelm a mail system by flooding it with 100s or 1000s of messages in as short amount of time as possible. The default setting is 30 messages in 10 seconds, but is disabled by default. To enable this feature we must go to the SMTP/MIME Settings page, click 'Security…' and check ''Enable mailbomb protection'. Click 'OK' twice to save the changes, including those from the previous issues.

GroupWise WebAccess Agent Security

Similar to POP3/IMAP4 access, WebAccess provides access to the e-mail system from outside the network by way of a web interface, so precautions are necessary. Again, by default, everyone is permitted access provided their e-mail account has a password. It would be advisable to restrict access to those individuals that need the service. This may be accomplished by selecting the 'Access Control' page from the WebAccess agent's details. Select 'Default Class of Service' then click 'Edit…'. Select 'Prevent access' and click 'OK'. Now we must create a group that will have access. Click 'Create…' and enter a name, such as "Allowed WebAccess", then click 'OK'. Click 'Allow access' then click 'OK'. To select individual users, click the 'Users' button and start adding users. When finished adding users click 'OK' twice and the changes are complete.

Vulnerabilities - Needed fixes/patches

To date, the GroupWise system has been fortunate not to be plagued with many of the viruses that depend on the scripting ability built into some other e-mail clients. This by no means indicates though, that we have a fail-safe system. In mid August of 2001 Novell issued a security alert for GroupWise 5.5 enhancement pack and GroupWise 6. It was discovered that an individual's username and password could be discovered under a particular session. For this to occur an individual must have a protocol analyzer placed such that it would be able to view packets between a server and client running in Live Remote or Smart Caching mode. Two

patches, Padlock Fix, were also made available, one for the server and one for the client. The patches are available at http://support.novell.com/padlock.

It is also important to note that Novell is not usually the first to catch potential security problems with their software. When WebAccess is installed a default account is created to manage the WebAccess servlets. Securityteam.com issued the following alert on 21-Dec-2001:

Vulnerable systems:
GroupWise 5.5 Enhancement Pack
GroupWise 6.0

Exploit:
http://server/servlet/ServletManager
username servlet
password manager

Solution:
Change the password:

Edit the SYS:\JAVA\SERVLETS\SERVLET.PROPERTIES file.
There is a section for ServletManager like the following:

```
# ServletManager servlet
servlet.ServletManager.code=com.novell.application.ServletGateway.ServletManager

servlet.ServletManager.initArgs=datamethod=POST,user=servlet,password=manager,bgcolor

#c0c0c0
servlet.ServletManager.preload=true
```

Other security vulnerabilities that may be an issue involve the Netscape Enterprise Server for Netware, which may be installed along with WebAccess. Vigilante, a company that specializes in assessing network security, reports systems running NetWare v5.0 or 5.1 prior to support pack 1 are vulnerable to a denial of service attack. Previous versions may also be vulnerable but were not tested. The attack is accomplished by sending a malformed URL to the web server. Novell has released a fix that is included in the latest Support Packs.

On a similar note, security.com issued an alert on 20-Dec-2001 that there is an issue with the web server installed by default on systems running v5.1 of NetWare. Included with the web server are some default web pages and in particulate a "viewcode" application that displays the source code of some sample pages. Through some recrafting of a URL it is possible to view system files located on the server that should otherwise be unseen. The attacker must however know the relative path to the requested file in order for the request to be successful.

Conclusions

Through its ease of use and availability, e-mail has become a necessary part of everyday business. Provided we take some time to learn how the system works and integrates along with other services, we can provide a secure and dependable delivery system. To do this we should:

1. Take time to read though the manuals and online documentation provided with the software.
2. Create a lab environment in which to test different configurations.
3. Communicate with other colleges to gain additional information.
4. Monitor the vendor's site for recent patches/fixes.
5. Keep up to date on current security issues.

References

Gray, Adam. "Novell GroupWise Servlet Gateway Default Username and Password", 21-Dec-2001
URL: http://www.securiteam.com/securitynews/6G00Q003FE.html

GroupWise 5.5 Security – online documentation
URL: http://www.novell.com/documentation/lg/gw55/pdfdoc/gw55sec.pdf

Netscape Enterprise Server for NetWare Virtual Directory Vulnerability
URL: http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2000001.htm

NetWare Web Server Sample Page Source Disclosure
URL: http://www.securiteam.com/securitynews/6B00I2K3FA.html

Padlock Fix Details
URL: http://support.novell.com/padlock/details.htm

Possible security problem when a library and
URL: http://support.novell.com/cgi-bin/search/searchtid.cgi?/10052079.htm

Post Office Security
URL: http://www.novell.com/documentation/lg/gw55/index.html?gw55pods/data/a4bbal1.html

Using REMOTE on NetWare 4.x
URL:
http://www.novell.com/documentation/lg/nw4/docui/index.html#../utlrfenu/data/hhi58tbu.html

Using REMOTE on NetWare 5.x
URL: http://www.novell.com/documentation/lg/nw51/index.html?utlrfenu/data/hhi58tbu.html

Using SCRSAVER
URL: http://www.novell.com/documentation/lg/nw6p/index.html?utlrfenu/data/hrs18jbe.html]