Security Policies

XVI

Securing GroupWise Data

80

80.1 Limiting Physical Access to GroupWise Servers

Servers where GroupWise® data resides should be kept physically secure, where unauthorized persons cannot gain access to the server consoles.

80.2 Securing File System Access

In ConsoleOne®, Server objects for servers where GroupWise domains, post offices, and agents reside should be assigned appropriate trustees and rights to prevent access from unauthorized persons.

For additional data security, encrypted file systems should be used on servers where GroupWise domains, post offices, and agents reside. Only GroupWise administrators should have direct access to GroupWise data.

80.3 Securing Domains and Post Offices

In ConsoleOne, administrators in addition to the Admin user should be given rights judiciously, as described in Chapter 75, “GroupWise Administrator Rights,” on page 1135.

The POA should be configured for client/server access, so that GroupWise users do not require any direct access to any databases in the post office. For more information, see Section 36.2.1, “Using Client/Server Access to the Post Office,” on page 486.

Securing GroupWise Agents 81

81.1 Setting Up SSL Connections

All of the GroupWise® agents should be configured to use SSL connections, as described in:

- “Securing the Post Office with SSL Connections to the POA” on page 498
- “Securing the Domain with SSL Connections to the MTA” on page 629
- “Securing Internet Agent Connections with SSL” on page 772
- “Securing WebAccess Agent Connections with SSL” on page 875
- “Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 985

81.2 Protecting Agent Web Consoles

If you do not provide passwords on the GroupWise agent Web consoles, unauthorized persons can access them by simply knowing the IP address or hostname of the machine where the agent runs, along with the HTTP port the agent is using. Set up GroupWise agent Web consoles with passwords as described in:

- “Using the POA Web Console” on page 530
- “Using the MTA Web Console” on page 657
- “Using the Internet Agent Web Console” on page 787
- “Using the WebAccess Agent Web Console” on page 929
- “Configuring Authentication and Intruder Lockout for the Monitor Web Console” on page 985

81.3 Protecting Agent Startup and Configuration Files

The startup and configuration files for all GroupWise agents should be protected from tampering. Agent startup files are found in the following default locations:

Table 81-1 *Locations of GroupWise Agent Startup and Configuration Files*

Platform	Directory	Startup Files
NetWare	sys:\system	*post_office*.poa *domain*.mta gwia.cfg webac70a.waa gwdva.dva
Linux	/opt/novell/groupwise/agents/share	*post_office*.poa *domain*.mta *gwia*.cfg *webac70a*.waa gwdva.dva monitor.xml
Windows	c:\grpwise c:\grpwise c:\grpwise\gwia c:\wabacc c:\gwmon	*post_office*.poa *domain*.mta *gwia*.cfg *webac70a*.waa gwdva.dva monitor.xml

81.4 Protecting Agent Log Files

The log files for all GroupWise agents should be protected against access by unauthorized persons. Some contain very detailed information about your GroupWise system and GroupWise users. Agent log files are found in the following default locations:

Table 81-2 *Locations of GroupWise Agent Log Files*

Platform	Directory	Startup Files
NetWare	*vol*:*post_office*\wpcsout\ofs *vol*:*domain*\mslocal *vol*:*domain*\wpgate*gwia*\000.prc *vol*:*domain*\wpgate*webac70a*\000.prc sys:\system\gwdav.dir\log	*mmdd*poa.*nnn* *mmdd*mta.*nnn* *mmdd*gwia.*nnn* *mmdd*web.*nnn* *mmdd*dva.*nnn*
Linux	/var/log/novell/groupwise/*post_office*.poa /var/log/novell/groupwise/*domain*.mta /var/log/novell/groupwise/*domain*.*gwia* /var/log/novell/groupwise/*domain*.*webac70a* /var/log/novell/groupwise/gwdva /var/log/novell/groupwise/gwmon	*nnmm*poa.*nnn* *mmdd*mta.*nnn* *mmdd*gwia.*nnn* *mmdd*web.*nnn* *mmnn*dva.*nnn* *mmnn*mon.*nnn* *mmnn*hist.*nnn*

Platform	Directory	Startup Files
Windows	*post_offce*\wpcsout\ofs	*nnnm*poa.*nnn*
	domain\mslocal	*mmdd*mta.*nnn*
	domain\wpgate*gwia*\000.prc	*mmdd*gwia.*nnn*
	domain\wpgate*webac70a*\000.prc	*mmdd*web.*nnn*
	c:\webac\gwdva.dva\log	*mmnn*dva.*nnn*
	c:\gwmon	*mmnn*mon.*nnn*
		*mmnn*hist.*nnn*

81.5 Protecting Agent Processes on Linux

On Linux, the GroupWise agents are installed to run as the `root` user by default. This is not a secure configuration. Immediately after installation, you should set up a non-`root` user for the agents to run as, as described in "Running the Linux GroupWise Agents as a Non-root User" in "Installing GroupWise Agents" in the *GroupWise 7 Installation Guide*.

81.6 Protecting Trusted Applications

Trusted applications are third-party programs that can log into POAs and Internet Agents in order to access GroupWise mailboxes. For background information, see Section 4.12, "Trusted Applications," on page 69.

Trusted applications log into GroupWise agents by using trusted application keys that are created when the trusted application is created. It is essential that these keys are protected and not allowed to become public. Steps you can take to protect trusted application keys include:

- Associating the trusted application key with a single IP address whenever possible
- Reviewing third-party log files for sensitive data such as the key before sharing them with others
- Not sharing trusted application keys with others for any reason
- Removing old keys that are no longer needed

Securing GroupWise System Access

82

82.1 Using a Proxy Server with Client/Server Access

POAs in your GroupWise® system should be located behind your firewall. If GroupWise client users want to access their GroupWise mailboxes from outside your firewall using the Windows client or the Cross-Platform client, you should set up a proxy server outside your firewall to provide access, as described in Section 36.3.1, “Securing Client/Server Access through a Proxy Server,” on page 496. WebAccess client users access their GroupWise mailboxes through their Web browsers, so your Web server handles the access issues for such users.

82.2 Using LDAP Authentication for GroupWise Users

LDAP authentication provides a more secure method of mailbox access than standard GroupWise authentication, which is the default when you set up your GroupWise system. Therefore, you should implement LDAP authentication, as described in Section 36.3.4, “Providing LDAP Authentication for GroupWise Users,” on page 501.

On the Post Office object, the LDAP user name that you provide on the Security property page should be granted only browser rights in the eDirectory tree. The password for the LDAP user should be long and randomly generated.

On the LDAP Server object, *Require TLS for All Operations* should be selected on the SSL/TLS Configuration property page. On the LDAP Group object, *Require TLS for Simple Binds with Password* should be selected.

On your LDAP servers, the trusted root certificate file should be write protected so that it cannot be tampered with.

82.3 Managing Mailbox Passwords

GroupWise offers varying levels of password security, as described in Section 70.1, “Mailbox Passwords,” on page 1111. Make sure that you understand the options available to you and that you select the level of password security that is appropriate to your GroupWise system.

82.4 Enabling Intruder Detection

You can configure the POA to lock out a user that provides the wrong mailbox password too many times, as described in Section 36.3.5, “Enabling Intruder Detection,” on page 506.

Secure Migrations

83

83.1 GroupWise Server Migration Utility

During its operation, the GroupWise Server Migration Utility prompts for some restricted-access information. It also modifies critical GroupWise agent startup files. This section explains why.

83.1.1 Source Server Credentials

The Server Migration Utility prompts for a user ID and password that provides read/write access to the NetWare or Windows server so that the Linux server can mount the source server with read/write access.

In addition, the Server Migration Utility needs read/write access to the domain or post office directory that is being migrated. Read/write access enables the Server Migration Utility to copy the contents of the post office directory or domain directory, including the post office database and domain database, so that file locking is respected while the data is being copied, File locking prevents database damage.

83.1.2 Destination Server root Password

The Server Migration Utility prompts for the `root` password so that it can mount the NetWare volume or the Windows share to the Linux file system. It also needs the `root` password in order to communicate with the SSH (secure shell) daemon on the Linux server. The SSH daemon allows `root` access for the utility to install the GroupWise RPMs, to run the programs required for migration locally on the Linux server, and to create and save the Linux agent startup files.

In addition, `root` permissions might be required to write the post office or domain data to the Linux server, depending on where the user decided to locate the post office or domain. After the migration, the user can configure the GroupWise agents to run as a non-`root` user for improved security, as described in “Running the Linux GroupWise Agents as a Non-root User” in “Installing GroupWise Agents” in the *GroupWise 7 Installation Guide*.

83.1.3 Agent Startup Files

When the Server Migration Utility migrates an agent, the only change it makes to its startup file is to modify the --home switch to point to the new location of the post office or domain on the Linux server. Existing switch settings are retained, except for paths and IP addresses that would be invalid in the new Linux environment.