An In-Depth Look at the GroupWise® Internet Agent

Robin Redgrave
Collaboration Technical Specialist
rredgrave@novell.com

Tim Heywood
CTO NDS8
tim.heywood@nds8.co.uk

Lawrence Kearney
Enterprise Service Analyst
lawrence.kearney@earthlink.net

Novell®

Agenda

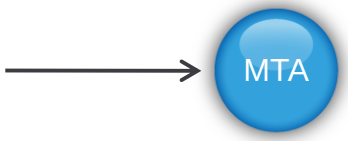
- Architecture and design
- Configuration
- Design
- Security
- Functionality
- Tips and Tricks
- Trouble shooting

Novell.

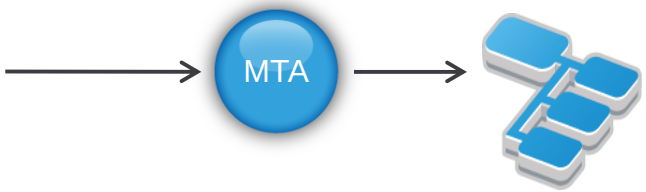
Architecture and Design

GWIA Architecture

GWIA Architecture

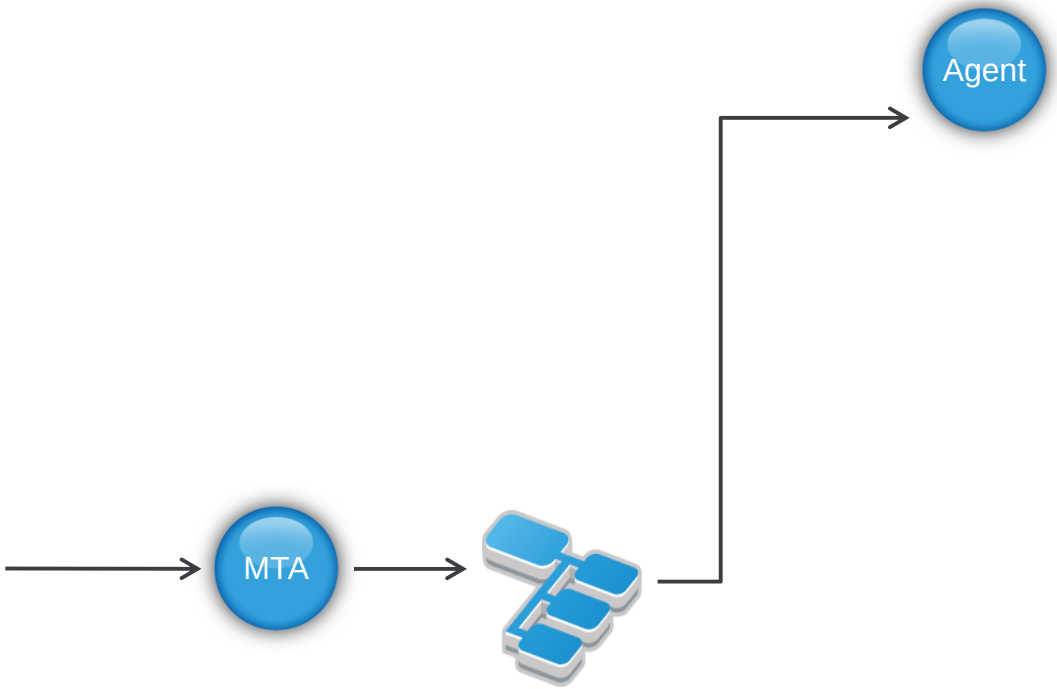


GWIA Architecture



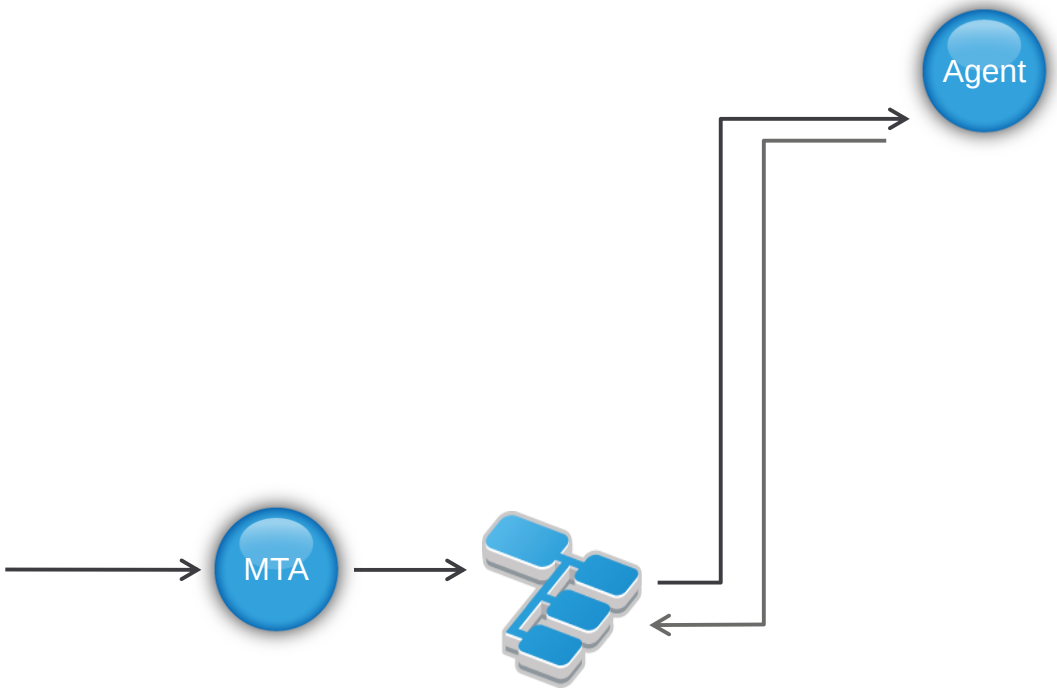
Novell

GWIA Architecture



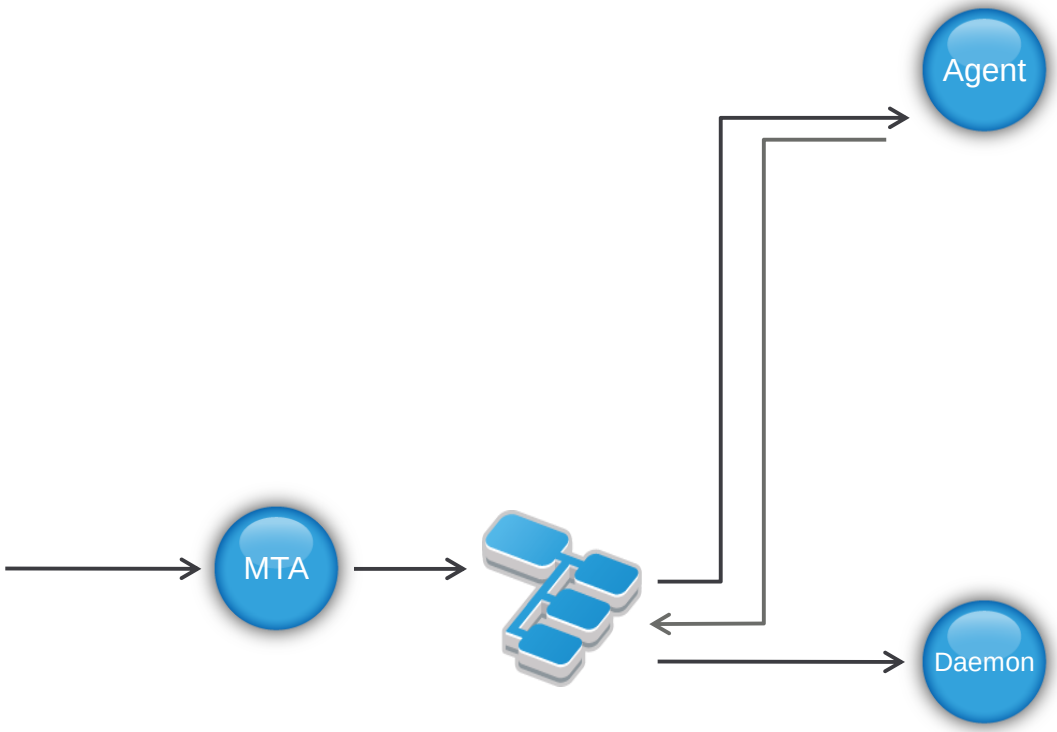
Novell

GWIA Architecture



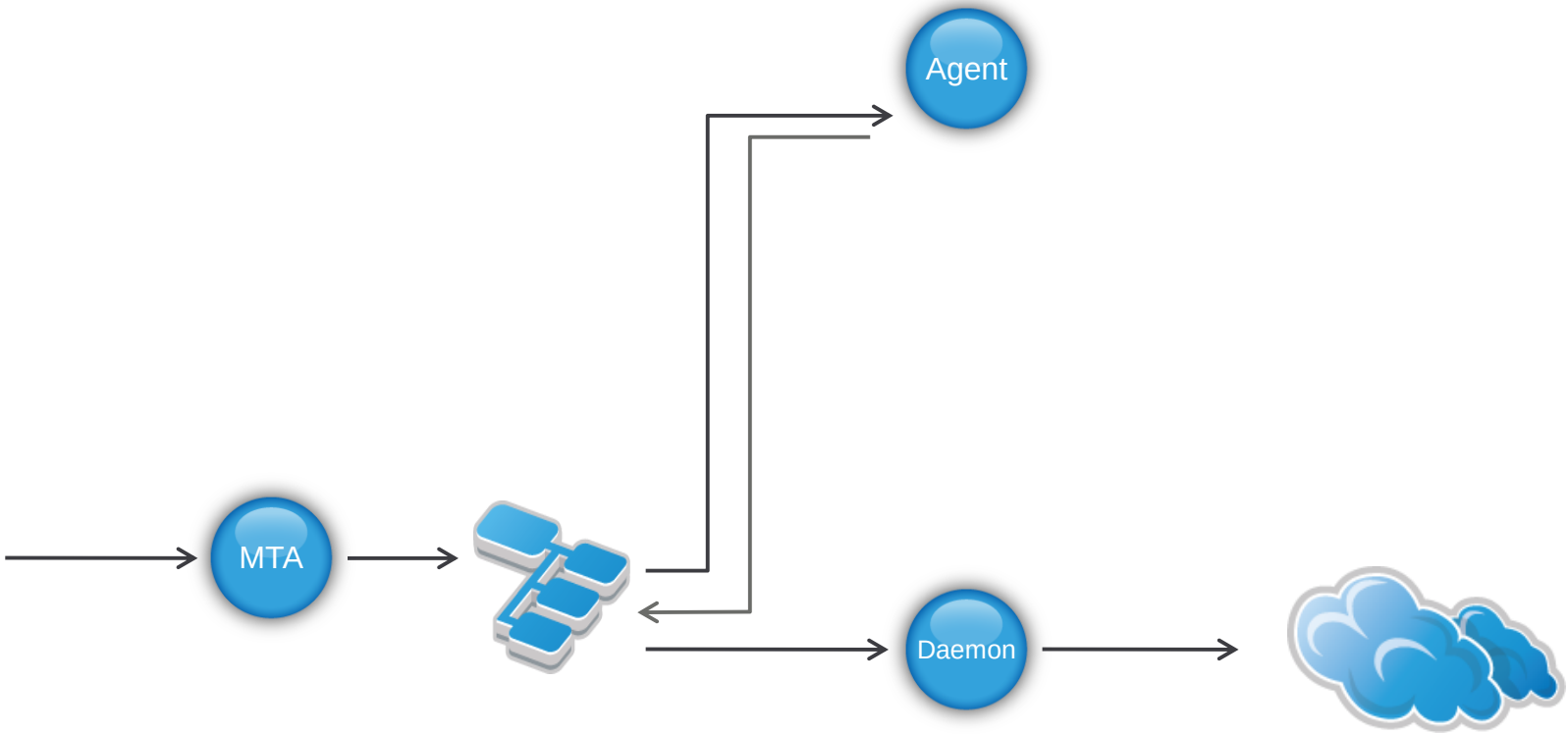
Novell

GWIA Architecture



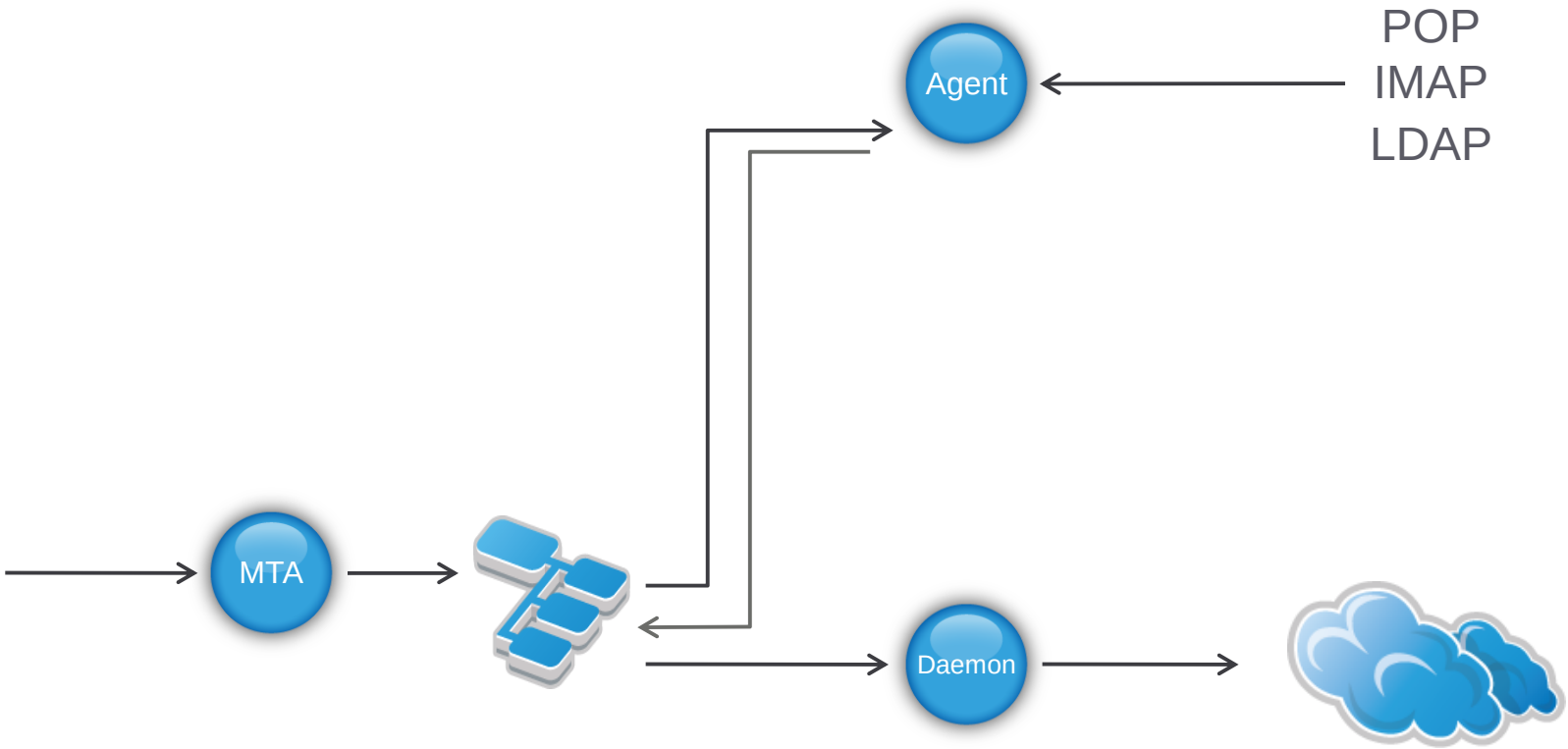
Novell

GWIA Architecture



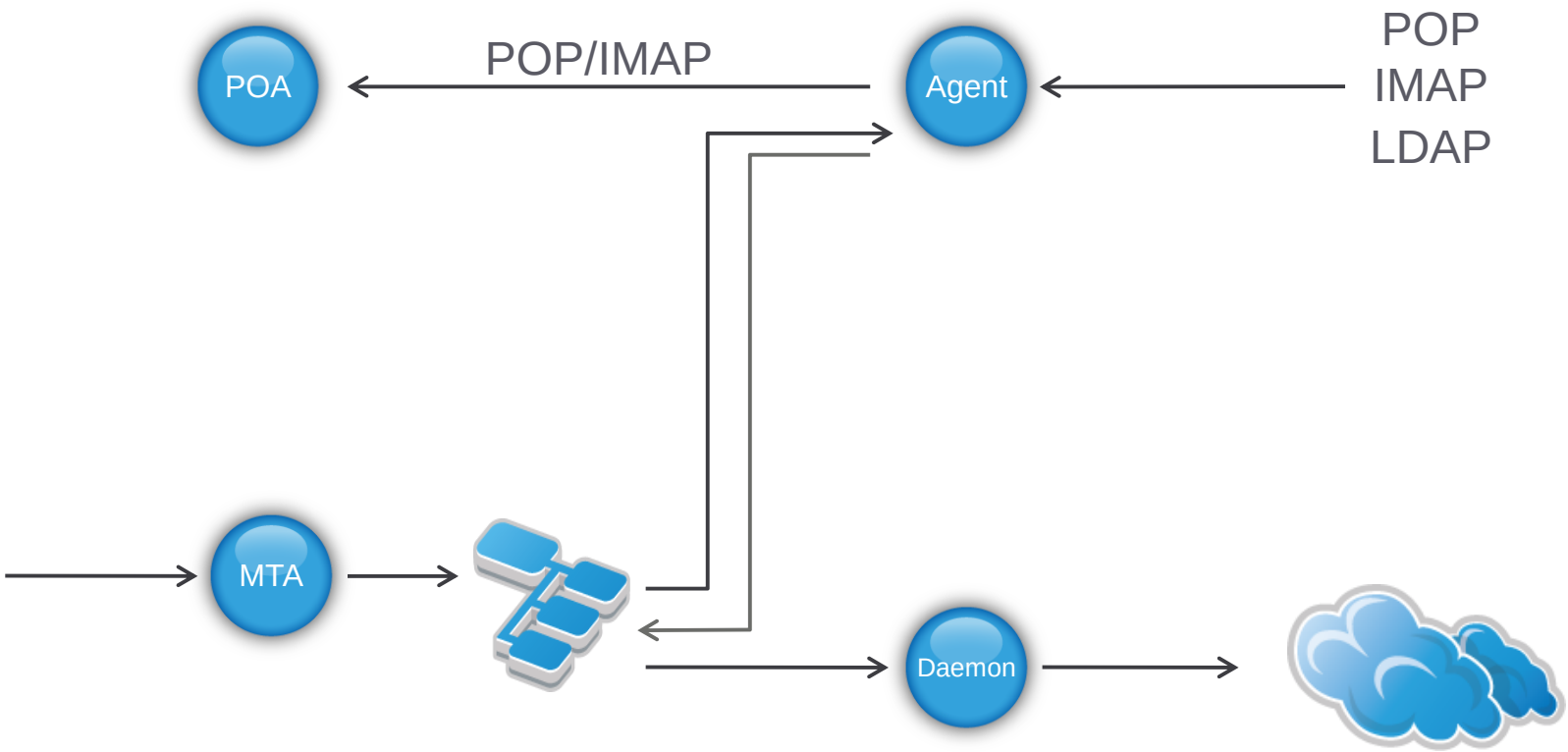
Novell

GWIA Architecture



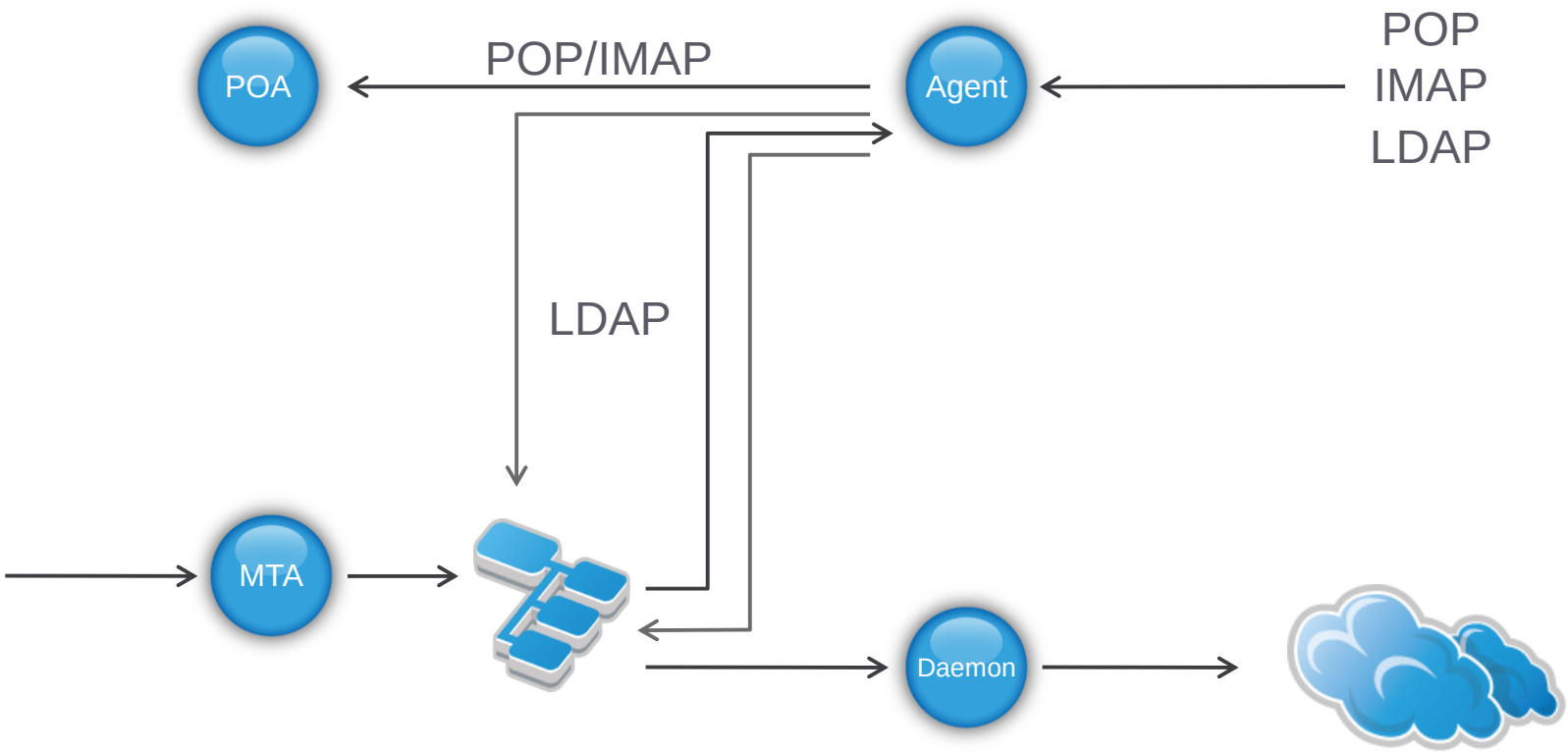
Novell

GWIA Architecture



Novell

GWIA Architecture



Novell

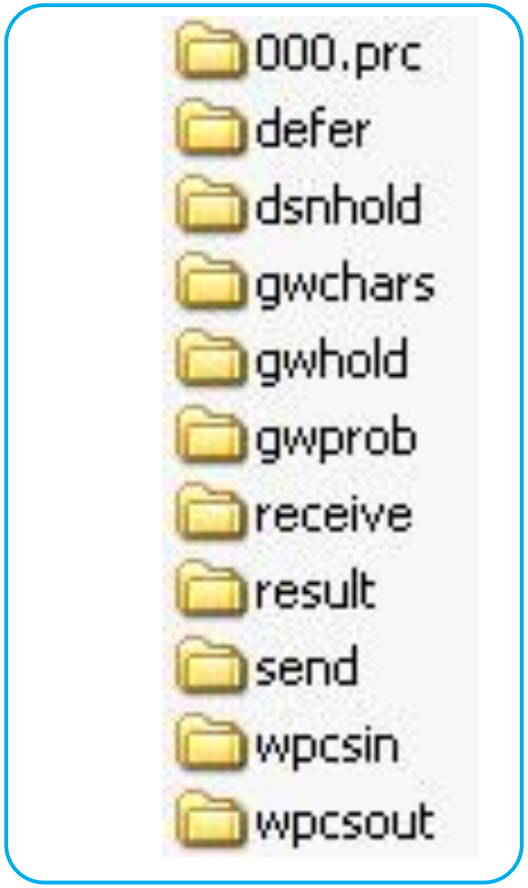
What can we do to improve services?

- Clever architecture and design choices
  - Using relay servers
  - Weighting MX records
  - Use native load management tools
- Service access control and redirection
  - Using Access Control Lists
  - Alternate GWIAs
- Service load balancing/management
- Service redundancy/high availability
  - GroupWise® high availability and clustering
- Service I/O fencing and demarcations (QoS really)

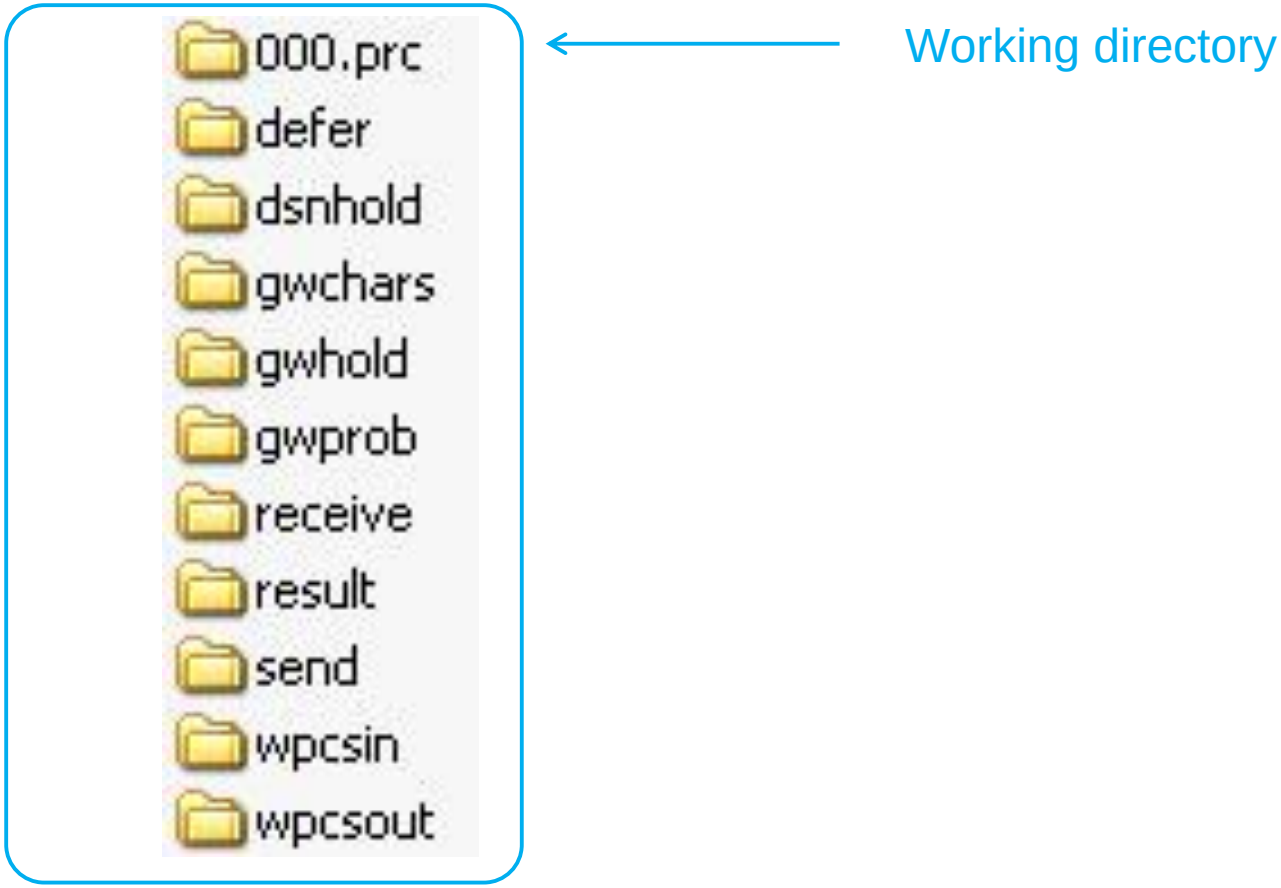
Novell.

Configuration

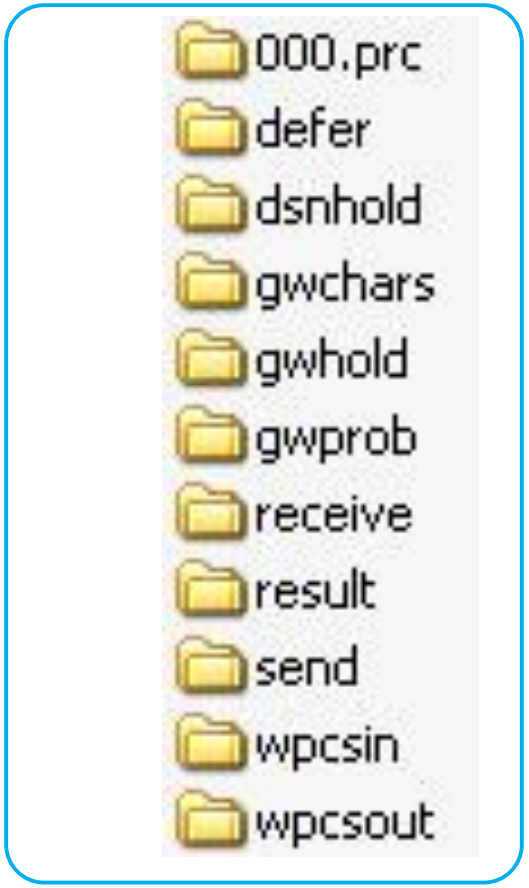
Directory Structure



Directory Structure



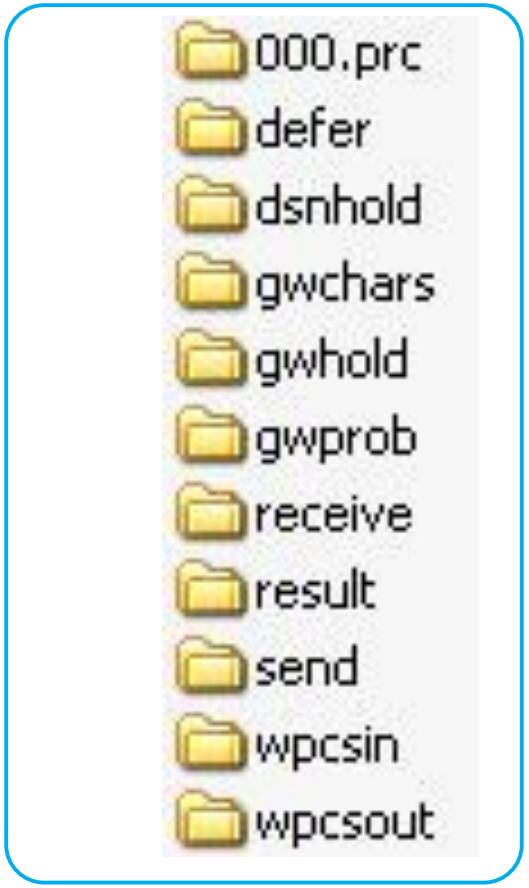
Directory Structure



Working directory

Deferred delivery messages

Directory Structure

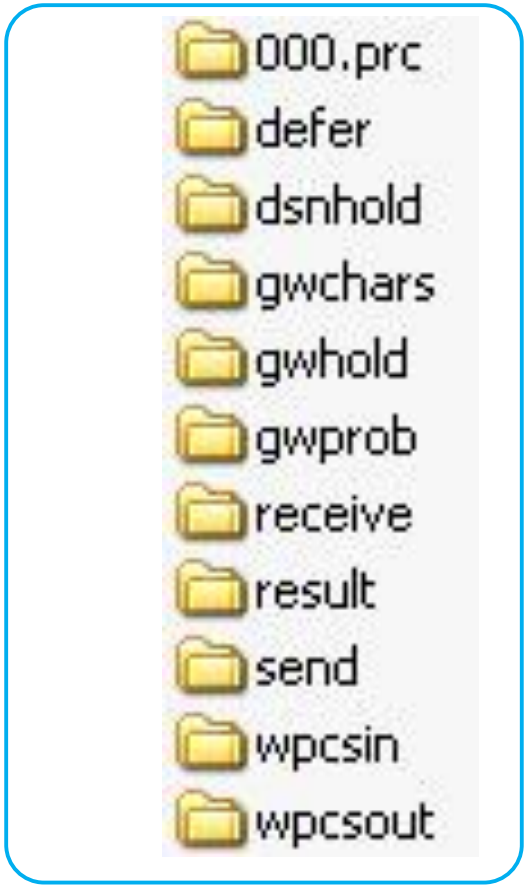


Working directory

Deferred delivery messages

DSN notification messages

Directory Structure



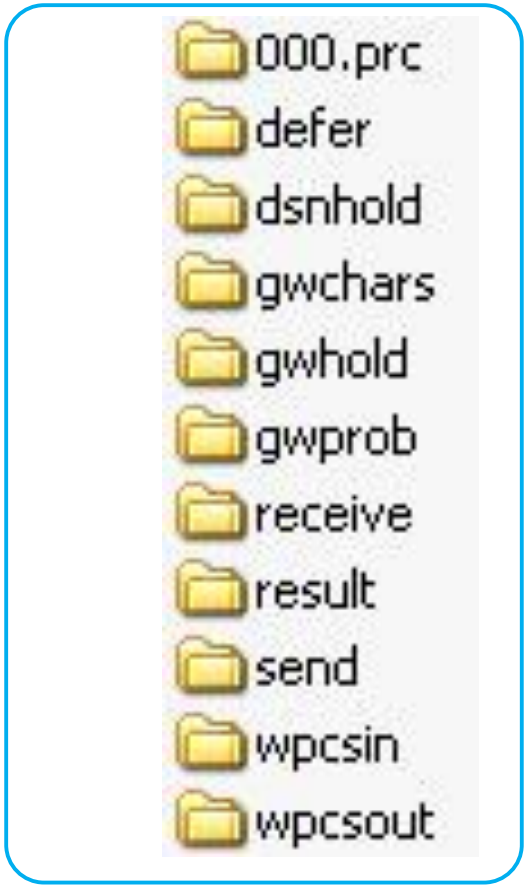
Working directory

Deferred delivery messages

DSN notification messages

Character mappings

Directory Structure



Working directory

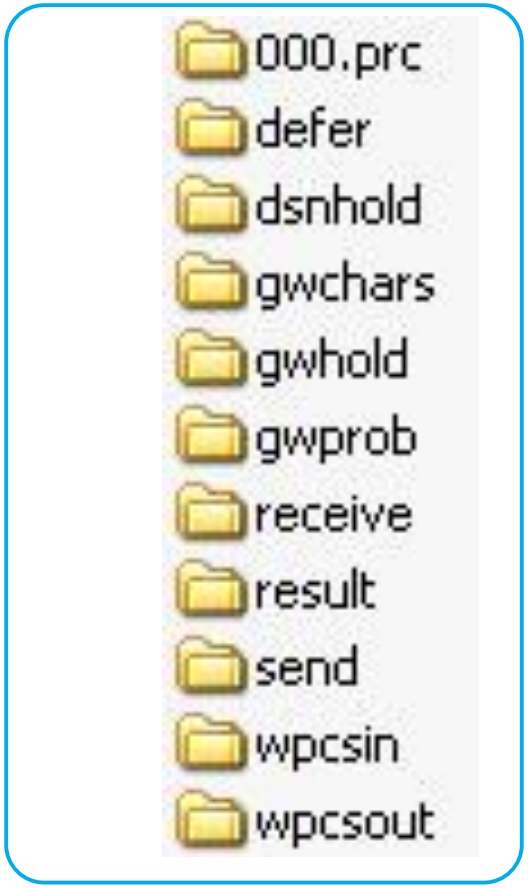
Deferred delivery messages

DSN notification messages

Character mappings

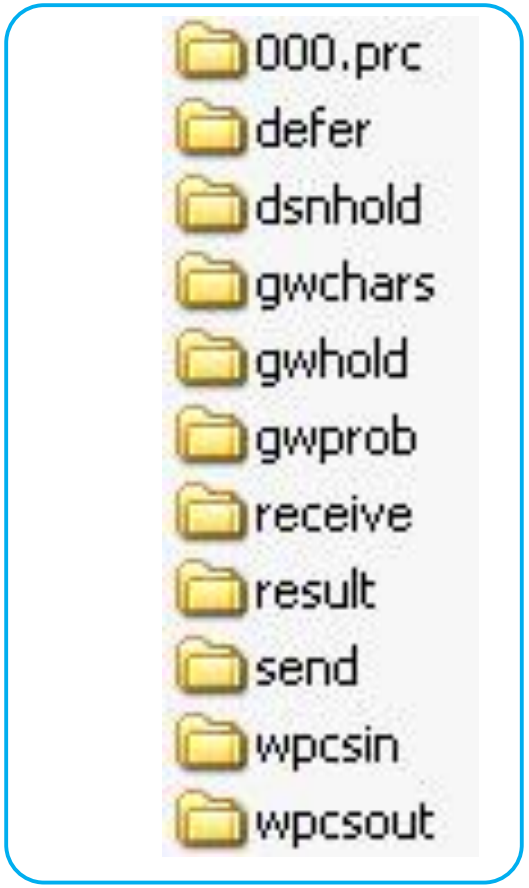
Delayed delivery messages

Directory Structure



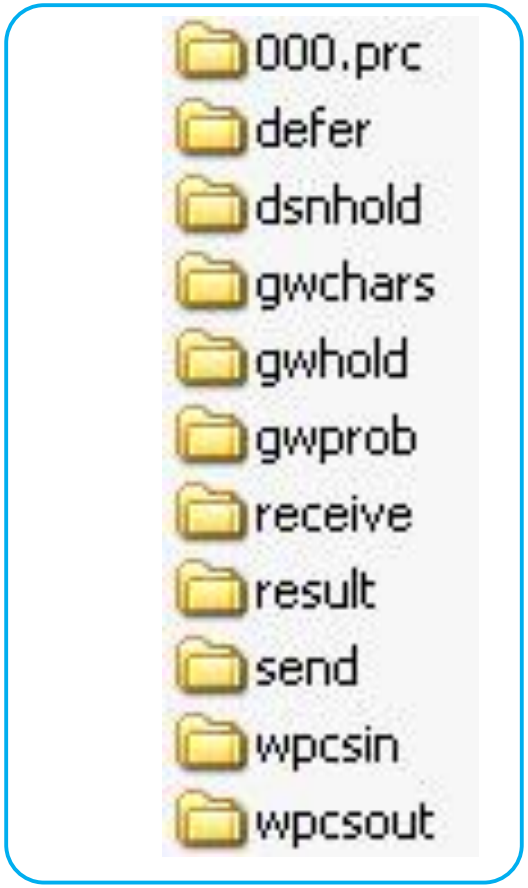
- Working directory
- Deferred delivery messages
- DSN notification messages
- Character mappings
- Delayed delivery messages
- Problem messages

Directory Structure



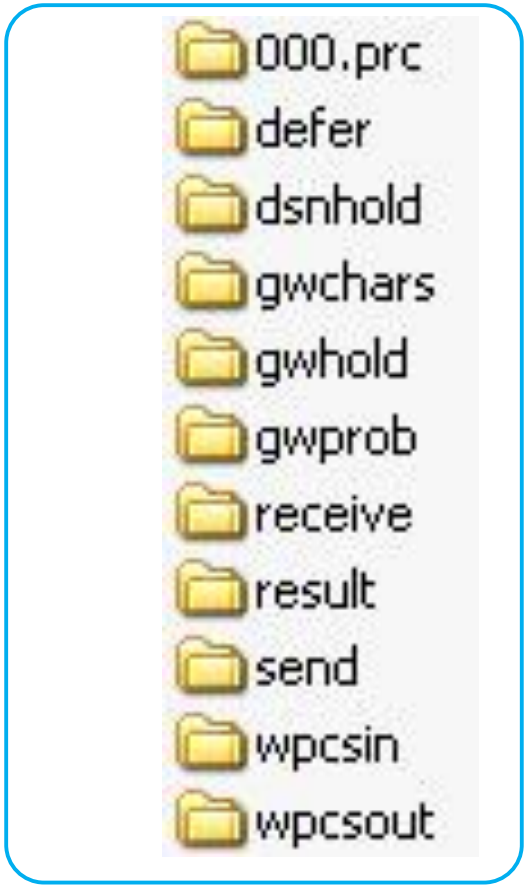
- 000.prc — Working directory
- defer — Deferred delivery messages
- dsnhold — DSN notification messages
- gwchars — Character mappings
- gwhold — Delayed delivery messages
- gwprob — Problem messages
- receive — Inbound SMTP messages

Directory Structure



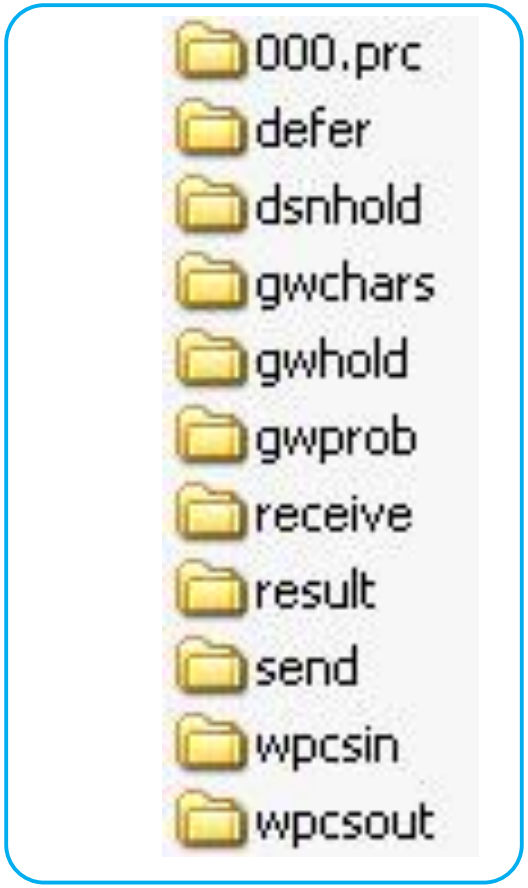
- Working directory
- Deferred delivery messages
- DSN notification messages
- Character mappings
- Delayed delivery messages
- Problem messages
- Inbound SMTP messages
- Result messages

Directory Structure



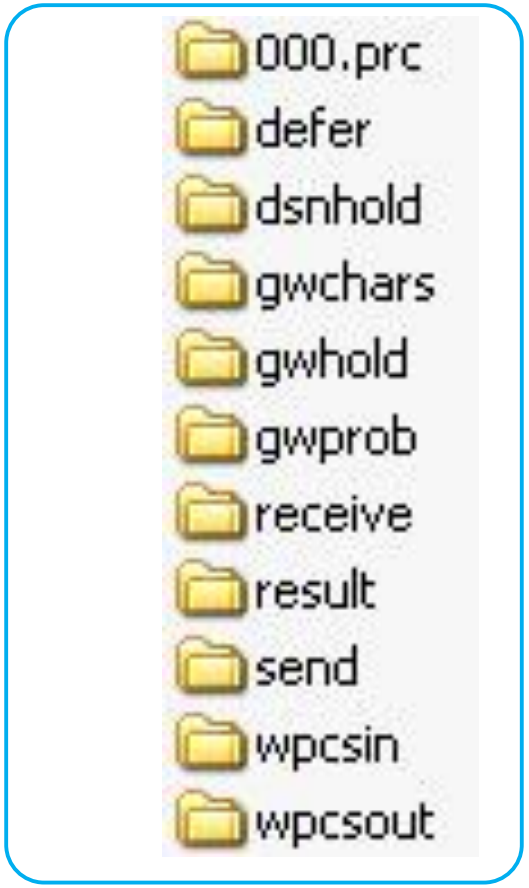
- Working directory
- Deferred delivery messages
- DSN notification messages
- Character mappings
- Delayed delivery messages
- Problem messages
- Inbound SMTP messages
- Result messages
- Outbound SMTP messages

Directory Structure



- 000.prc — Working directory
- defer — Deferred delivery messages
- dsnhold — DSN notification messages
- gwchars — Character mappings
- gwhold — Delayed delivery messages
- gwprob — Problem messages
- receive — Inbound SMTP messages
- result — Result messages
- send — Outbound SMTP messages
- wpcsin — MTA inbound queue

Directory Structure



- 000.prc — Working directory
- defer — Deferred delivery messages
- dsnhold — DSN notification messages
- gwchars — Character mappings
- gwhold — Delayed delivery messages
- gwprob — Problem messages
- receive — Inbound SMTP messages
- result — Result messages
- send — Outbound SMTP messages
- wpcsin — MTA inbound queue
- wpcsout — MTA outbound queue

Configuration Files

• gwia.cfg	Startup switches, mostly now in db
• exepath.cfg	Path to the gwia.cfg
• route.cfg	Routing overrides
• status.xml	Returned status messages
• preamble.*	Mime warning
• blocked.txt	Blocked IP sources
• mimetype.cfg	Content type mapping
• frgnames.cfg	Legacy foreign names
• gwauth.cfg	SMTP host authentication

Exepath.cfg

- Located in the domain\wpgate\gwia directory
- Used by ConsoleOne® to locate the gwia.cfg file
- The file must contain the path to the gwia.cfg file
- Default Paths:
  - Windows : domain\wpgate\gwia
  - Linux : /opt/novell/groupwise/agents/share
    - or \server\opt\novell\groupwise\agents\share

Route CFG

- Used to override any DNS entries for a destination
  - Ignore a relay host for some internal destinations
  - Some hosts are unknown to the DNS
  - Some destinations you may want to virus scan
  - Create the file in the domain\wpgate\gwia directory

```
novell.com      gwia.novell.com
unixbox         [123.1.2.3]
```

- Ensure that the last entry is followed by a carriage return

Novell.

SUSE® Linux Enterprise Server Open Enterprise Server 2

- Postfix
  - Do not disable
- Edit /etc/postfix/main.cf
  - Change the "inet_interfaces= all"
    - "inet_interfaces=127.0.0.1"
- Set GWIA to bind exclusive at “load time”

Novell.

Design

GroupWise® Design

- Have domain local to the GWIA
  - Recommended to be on a dedicated secondary domain
  - Do not run a gateway across the network
  - Design the IP space for your system
  - Use MTP between MTA and GWIA
    - Needed for alternate GWIA functionality

Novell.

Multiple GWIAs

- Why
  - Flexibility
  - Stability
  - Security
  - Performance
- Usage
  - Inbound/outbound mail
  - Internal/external mail
  - Dedicated POP or IMAP services
- Resilience
  - MX records can point to multiple inbound GWIAs
  - Can have a fail-over GWIA if routing via MTP
  - Can have multiple outbound relay hosts

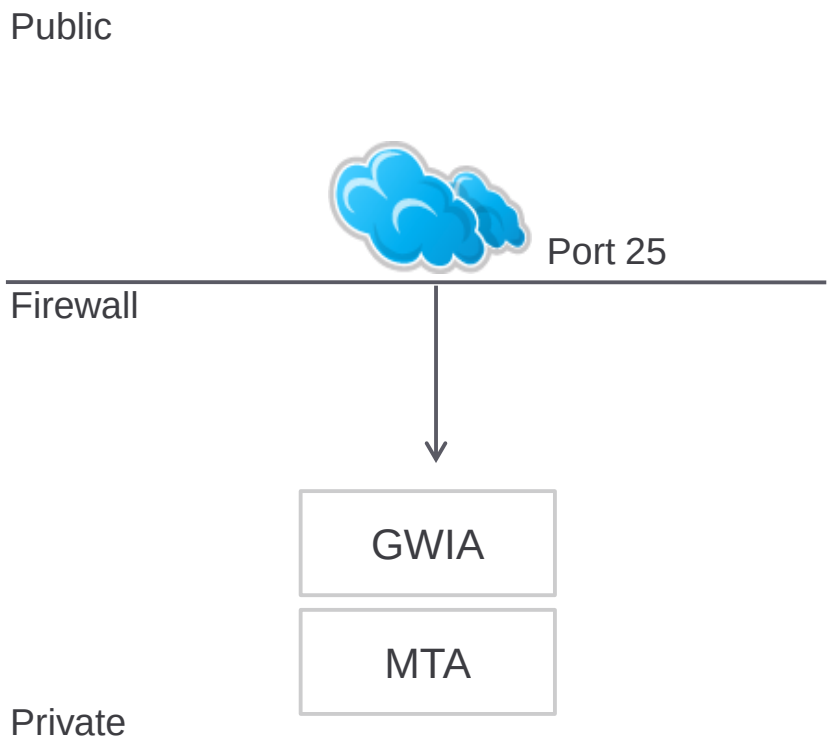
Novell.

Clustering

- Types: Novell Clustering Services and Linux High Availability
- Badly formatted messages can stop multiple nodes
  - Do not fail over to all nodes
- If no SMTP Relay there is direct external access
- Virtualisation can compete
  - Potential additional cost or overhead

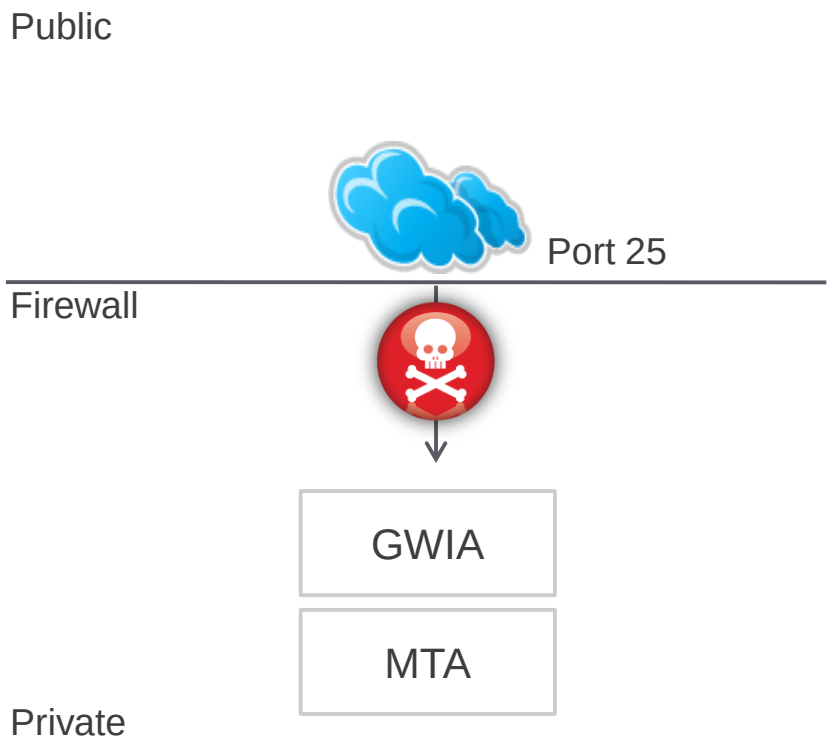
Security

Security



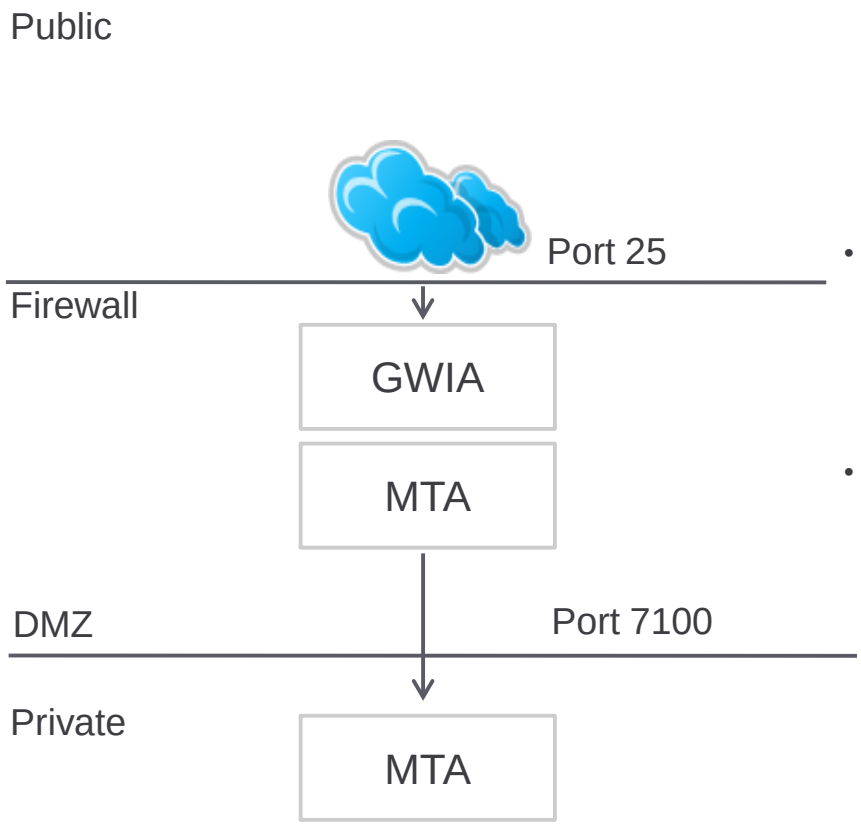
- Avoid having direct connections from the Internet into the production Network

Security



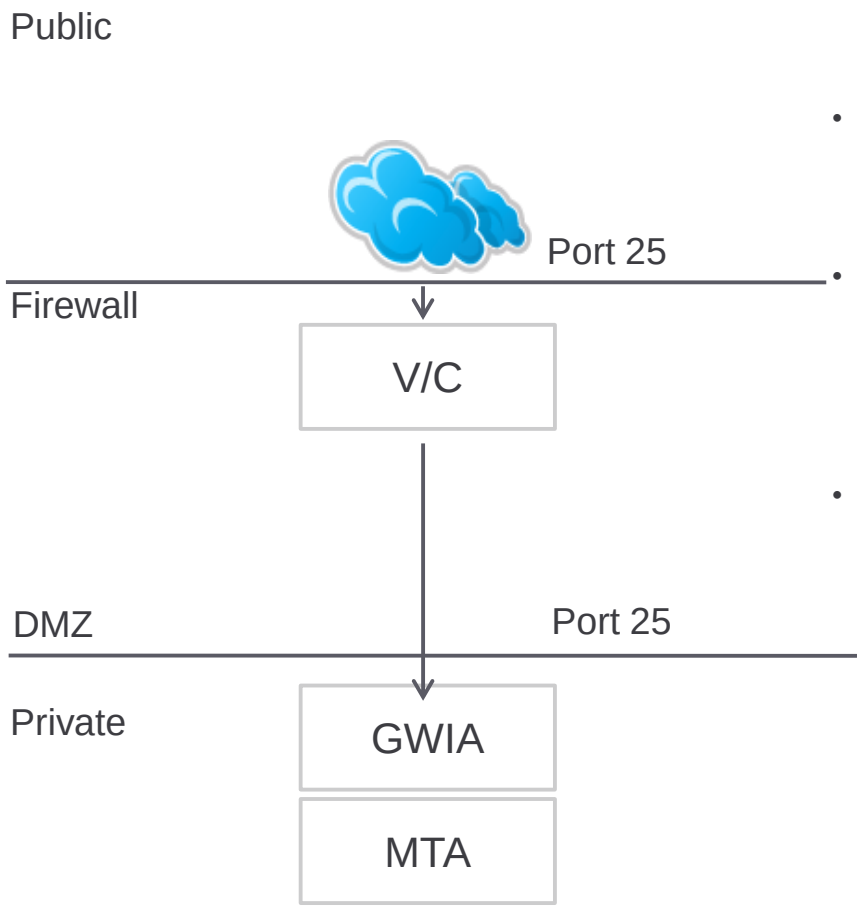
- Avoid having direct connections from the Internet into the production Network

DMZ Security



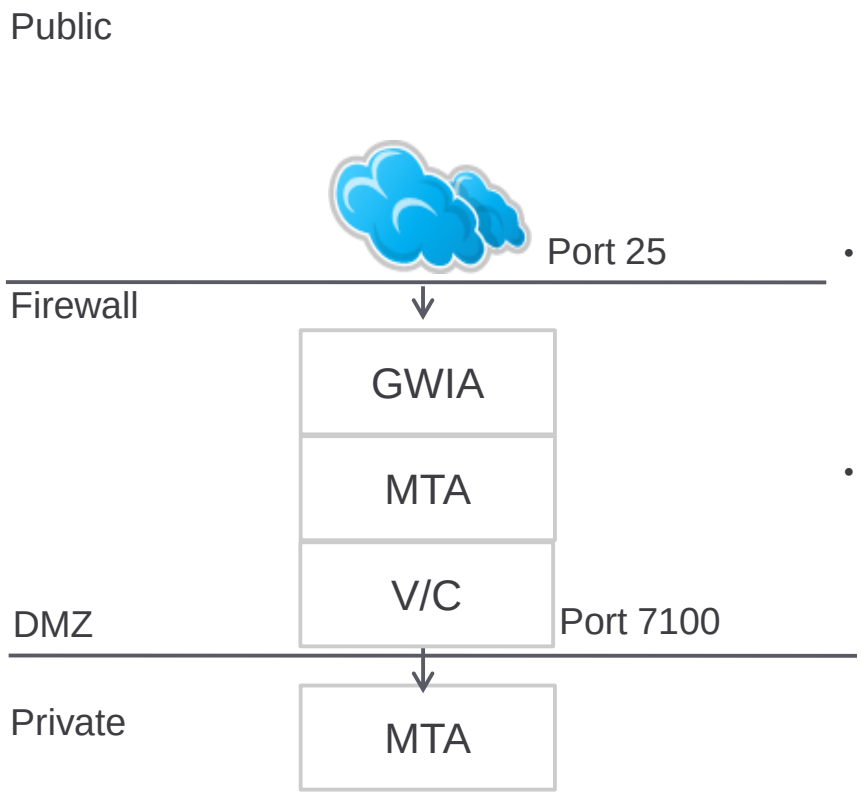
- Place the GWIA on its own domain in the DMZ
- If running on OES, ensure it is in its own tree
  - But GWIA domain and objects are still in production tree..

Virus/Spam Checking



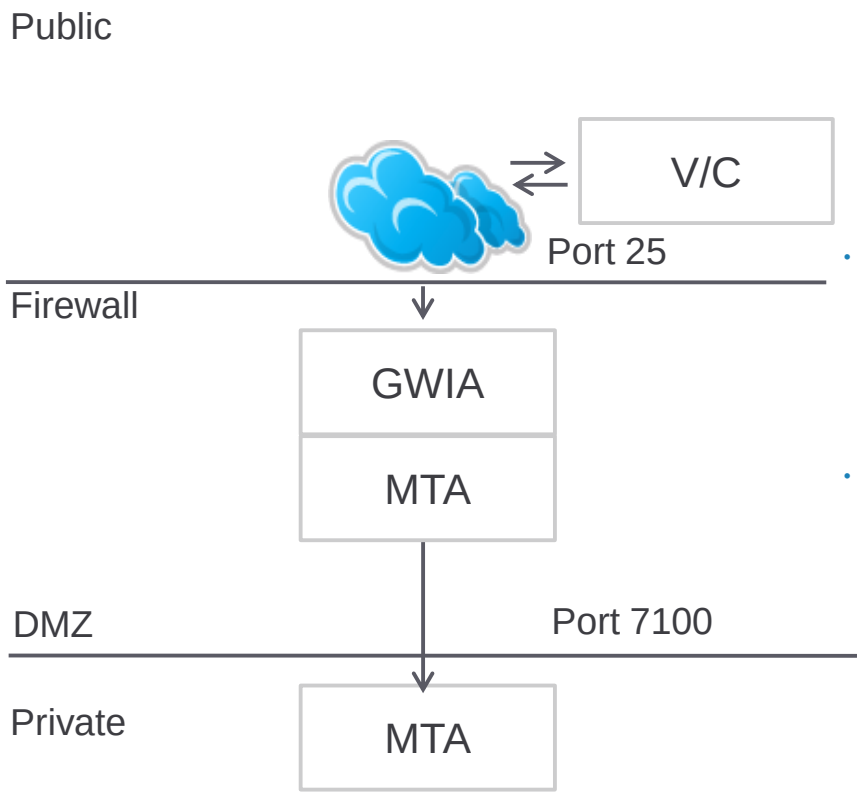
- Check before the GWIA
- Place a virus checker/ relay in the DMZ
- Relay benefits
  - I/O isolation and management
  - Alternate access control point
  - Addition of non-native features and services

Virus/Spam Checking



- Check between one MTA and another MTA.
- Examples: GWAVA

Virus/Spam Checking



- Use an external virus checking organisation.
- Examples: MessageLabs

Access Control

- All access control is stored in the gwac.db
  - Can be deleted or can be copied between different GWIAs
- Class of service use
  - Domain (Mostly)
  - Post Office
  - Network Address
  - User
  - Distribution List
- Benefits
  - Prevention of unauthorized access to services
  - Internal misuse and security compliance issues
  - OMG … if you just checked those logs

Novell.

Access Control

- Can control
  - Incoming/outgoing SMTP
  - Maximum message size
  - Allow/deny messages to/from specific users/domains
  - Access to POP/IMAP
    - On Linux can use firewall to control access
- Block/allow all rule-generated messages
  - **/realmailfrom**
  - **/flatfwd**

Novell.

Access control

- Class of Service – Restricted GWIA
  - GroupWise specific ACL requirements
    - 10.1.1.1
    - *@*.*
    - Blank-Sender-User-ID

If these aren't in your GWIA Class of Service configurations you'll get disappointing results

Novell.

Security

- Relay
  - Disable, users can relay if they authenticate
    - Remember need SSL for authentication
- Mailbomb
  - Only enable mailbomb protection if you have a direct Internet connection
- SSL
  - If another site supports it consider using TLS
  - Enable for POP/IMAP
- Do not publish GroupWise connection information

Novell.

Functionality

POP3/IMAP

- Security
  - Ensure SSL is enabled
    - Credentials should not be sent in plain text
  - If not in use then disable for improved security
  - Cannot secure third party “local” message stores
  - Enable intruder detection at the Post Office
  - Internal mail policies circumvented
    - Retention
    - Quotas

Novell.

POP3/IMAP4

- IMAP at the POA
  - Direct access to the PO and therefore improved performance
    - But multiple access points need to be managed
- Bandwidth overconsumption
  - Messages not compressed
  - Connections kept open
  - Attachments expand in size with MIME encoding

Novell.

POP3/IMAP4

- Specific POP/IMAP start up switches

- Danger
  - SMTP will allow credentials sent in clear
  - Consider using a dedicated Internet Agent
  - Beware Mac mail!

Novell.

Lightweight Directory Access Protocol

- Lightweight Directory Access Protocol
  - No, not a database, an access protocol
  - References the GroupWise® domain database
    - Returns only 4 attributes
      - First Name Last Name
      - Email address Telephone
- Use NLDAP instead
  - References eDirectory™ so all user attributes available
  - eDirectory is optimised for LDAP and is therefore faster
- Do not make LDAP access publicly available!

Novell.

ESMTP

- Delivery Status Notification
  - Told delivered status by receiving system
- Size limitations
  - Based on the MIME size of the message
- Authentication
  - Inbound and outbound
- STARTTLS
  - SSL between SMTP servers

Blocking Messages

- Real-time blacklists
  - SBL – Known Spam Sources
  - XBL – Transitory Spam relay sources
  - Can override by adding to the exceptions list
- Blocked.txt
  - List of blocked sites
  - Created when editing access control
- Can check your services
  - http://www.dnsbl.info/dnsbl-database-check.php
  - http://www.mxtoolbox.com

Accounting Files

- Logs all inbound and outbound traffic
  - Delivered to the accountant as a CSV file at midnight
  - Gives the following information
    - Date/time
    - Subject
    - Inbound/outbound
    - Priority
    - Recipient
    - Size
    - Sender
    - Message type

    and others...
- Parsing tools
  - GroupWise Monitor
  - Cool Solutions
    - www.novell.com/communities/node/405/groupwise-accounting-data-report-20

Monitoring

- Console
  - Use show option in gwha.conf (Debugging only)
- HTTP monitoring
  - Browser-based monitoring of the GWIA
- GWMonitor
  - Visual representation that the Gateway is running
  - Multiple thresholds can be set
- Third Party monitoring tools

Tips and Tricks

Improving Performance

- Send and receive threads
  - The number of concurrent messages processed
  - The more threads, the more server resources used
  - Decrease the poll intervals for agent and daemon directories
  - Conversion and queue directories should be local
    - Increase threads allocated
- Turn off Delayed Ack, Nagle and Minshall

Novell.

Aliases/Nicknames

- Users can be known by other than the default names
- Gateway alias
  - A user can only have one per gateway alias type
  - A GWIA instance can have only one alias type
  - Effects the return address on outbound mail
  - Try not to use
    - Use the override option on Internet Addressing
- Nicknames
  - Can have more than one per user
  - Does not effect the return address on outbound mail
- ConsoleOne® Alias to Override tool

Novell.

Schizophrenia

- Users can have multiple inbound personalities
  - Multiple inbound iDomains
  - Multiple personalities from
    - Internet addressing
    - Nicknames
    - Gateway alias
  - But they only have the one outbound address
  - Can publish all addresses to eDirectory™
- Resolution
  - Use multiple outbound GWIAs
    - Define different gateway alias types for each / use different aliases
  - Use POP/IMAP accounts on client and relay off GWIA
  - Proxy to another account

Novell.

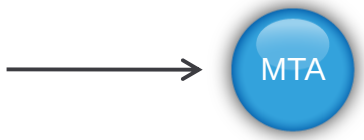
Troubleshooting

Message Flow

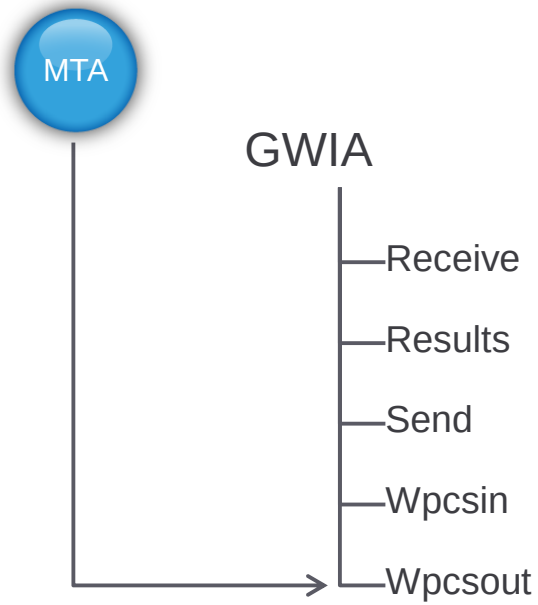
- Why understand the message flow
  - Know which component is causing a problem
  - Know which directories to find messages in

Novell.

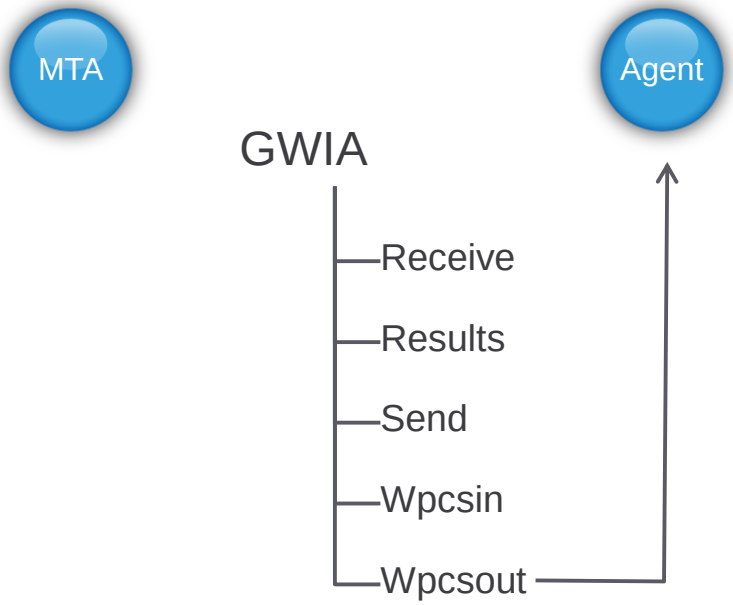
Message Flow



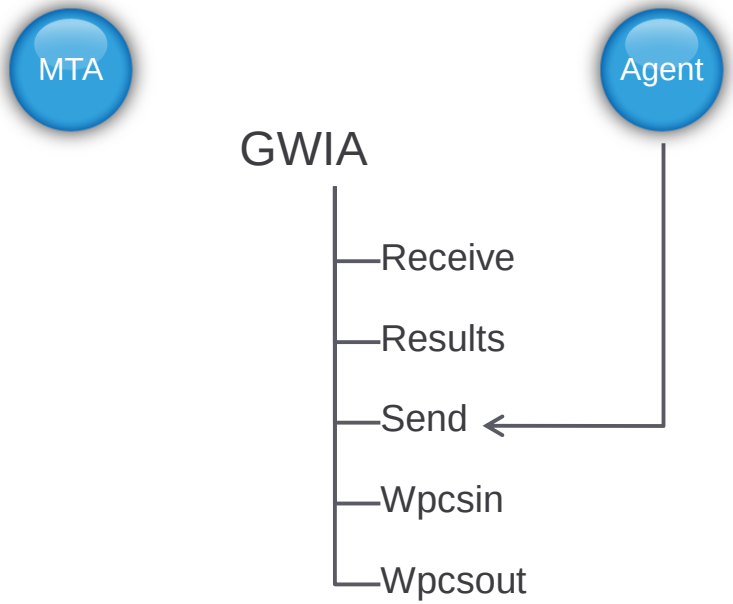
Message Flow



Message Flow

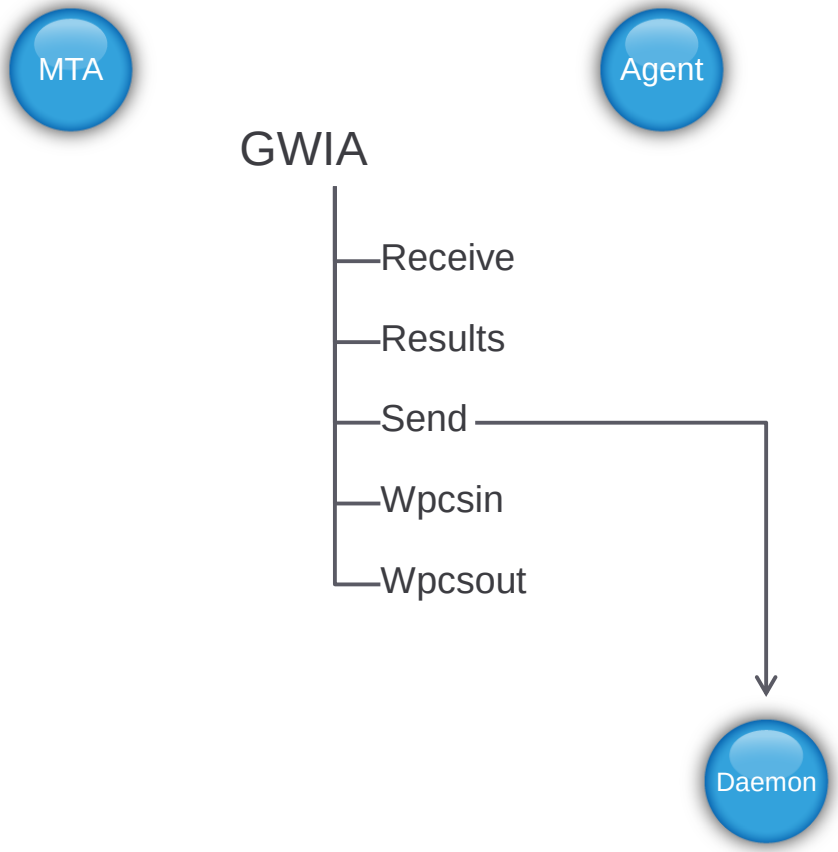


Message Flow

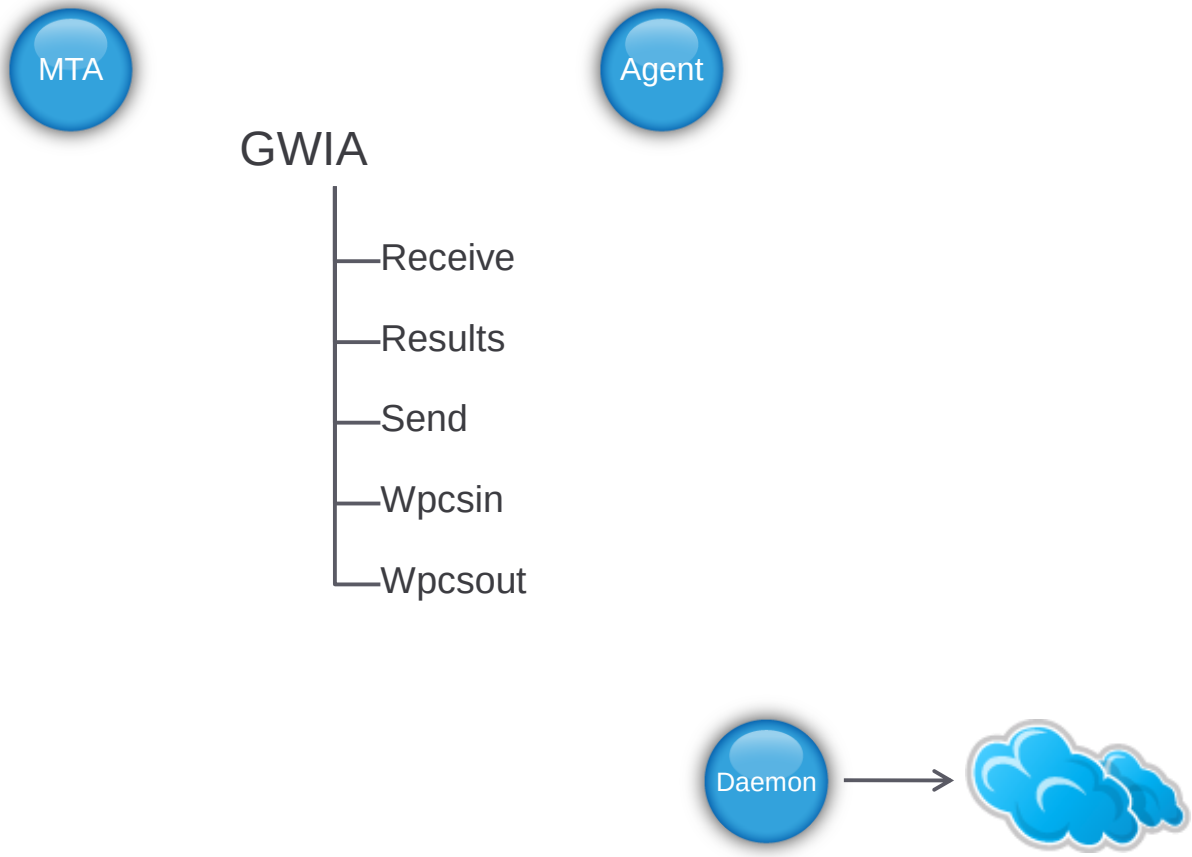


Novell

Message Flow



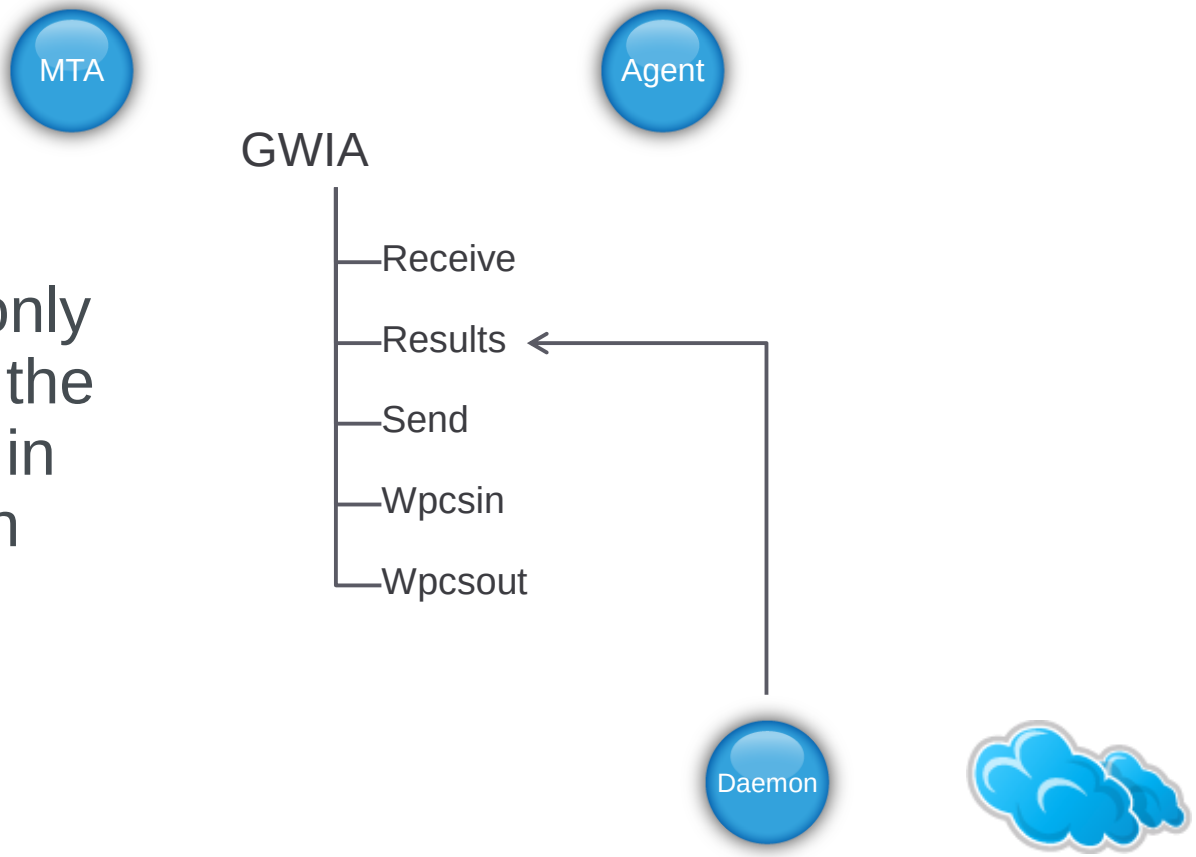
Message Flow



Novell

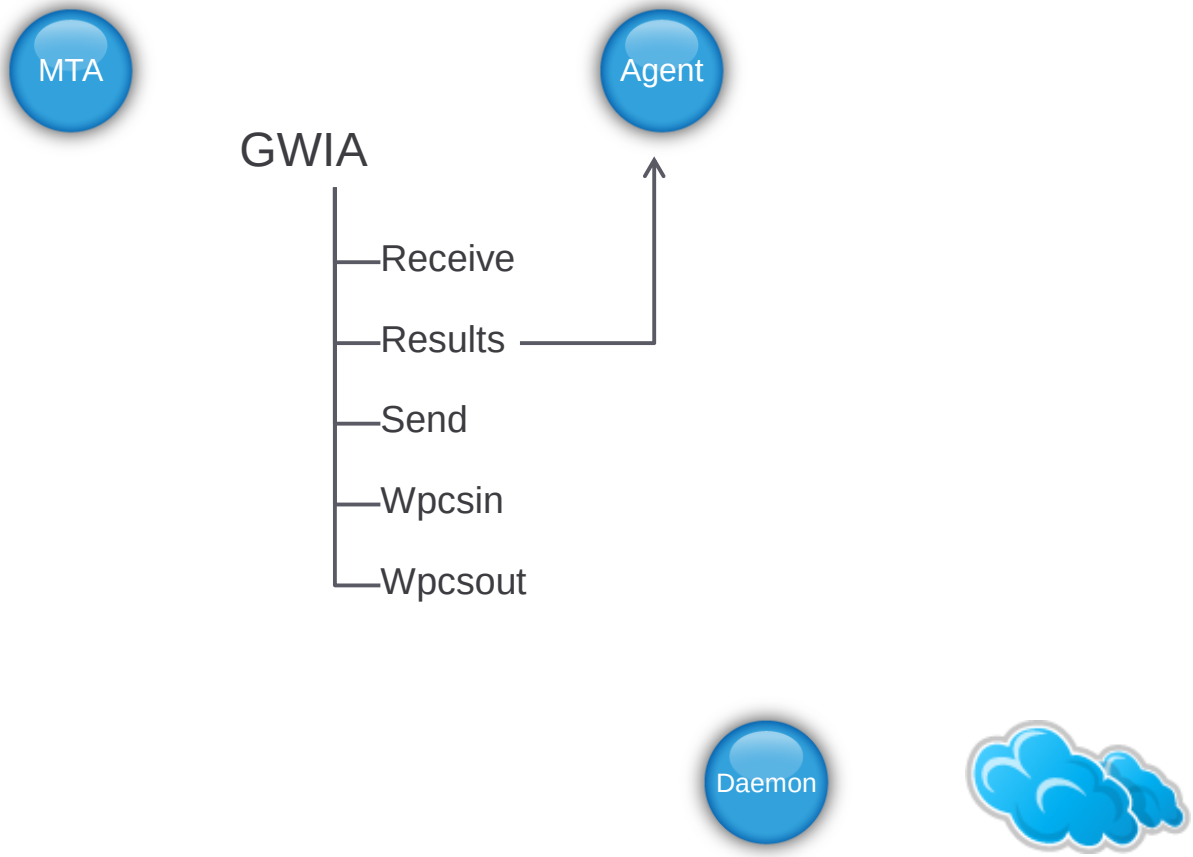
Message Flow

The daemon only writes back to the Results folder in the event of an unsuccessful transmission.



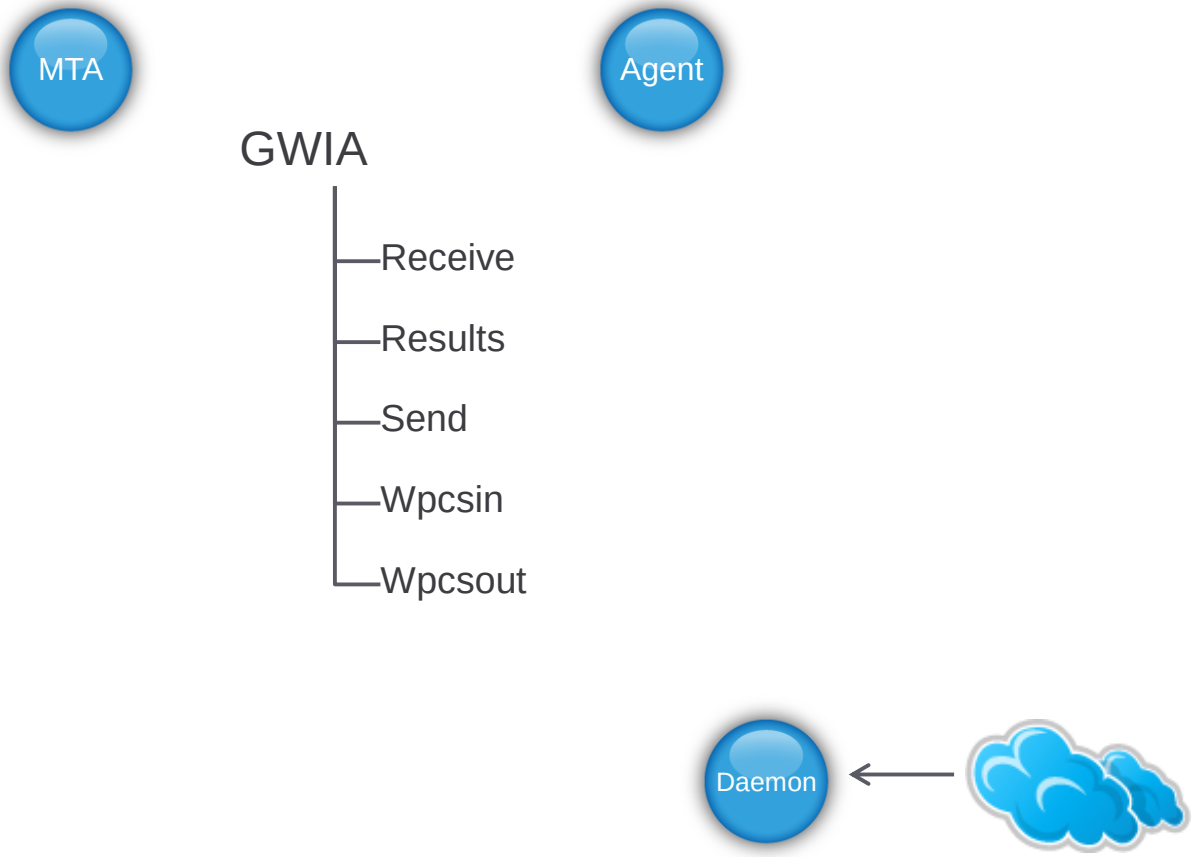
Novell

Message Flow



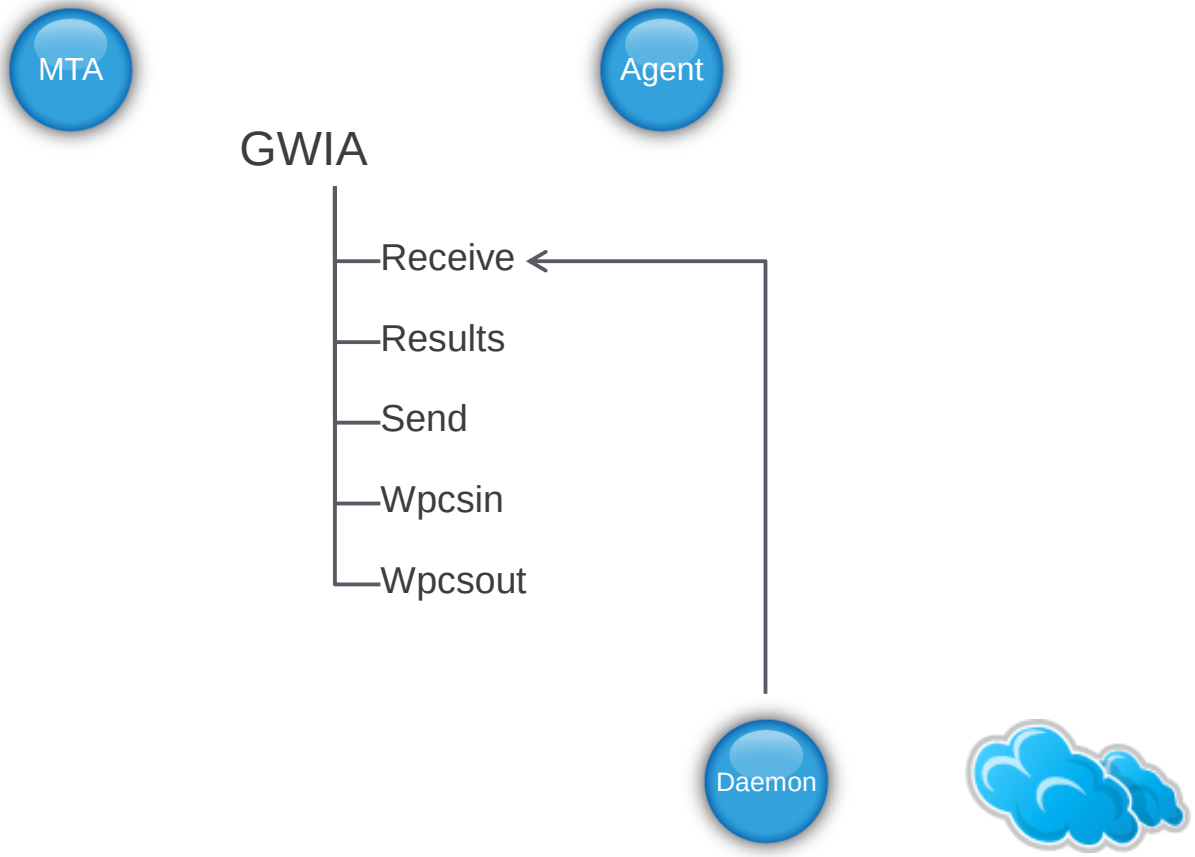
Novell

Message Flow



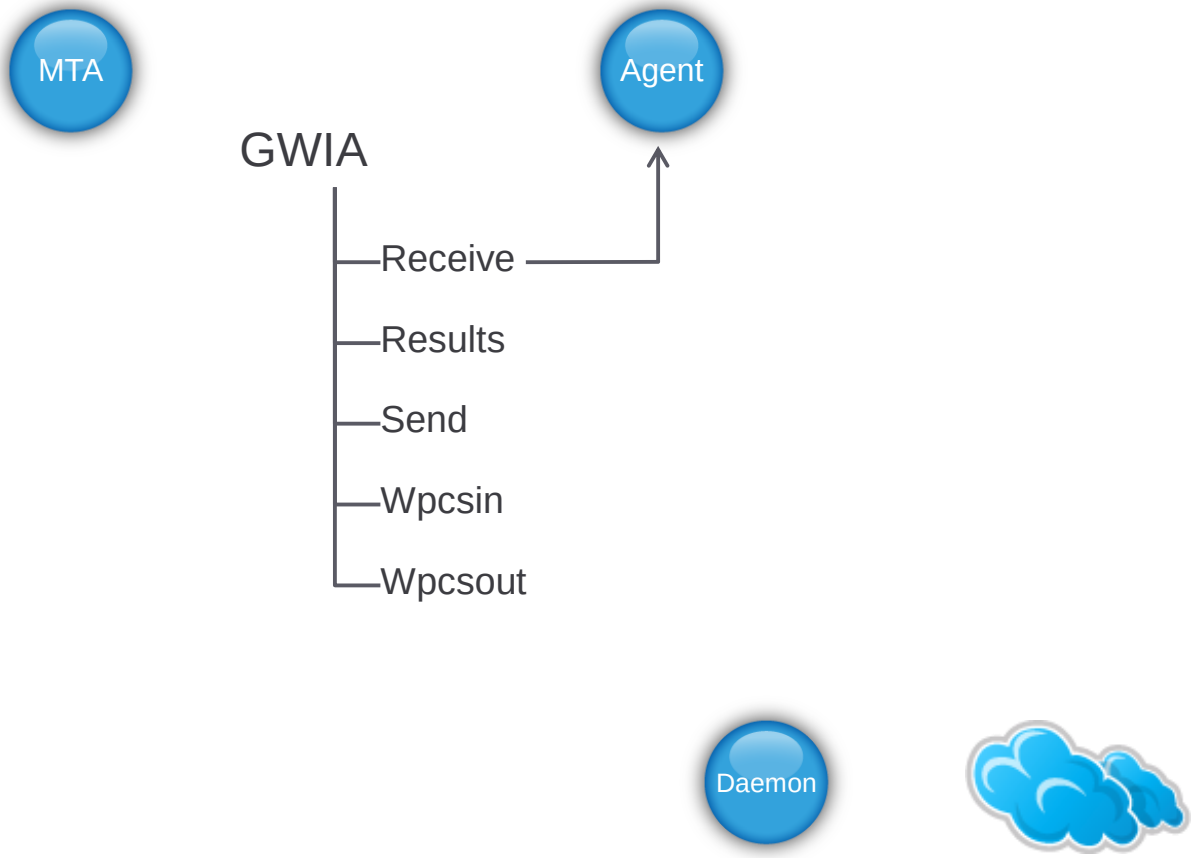
Novell.

Message Flow



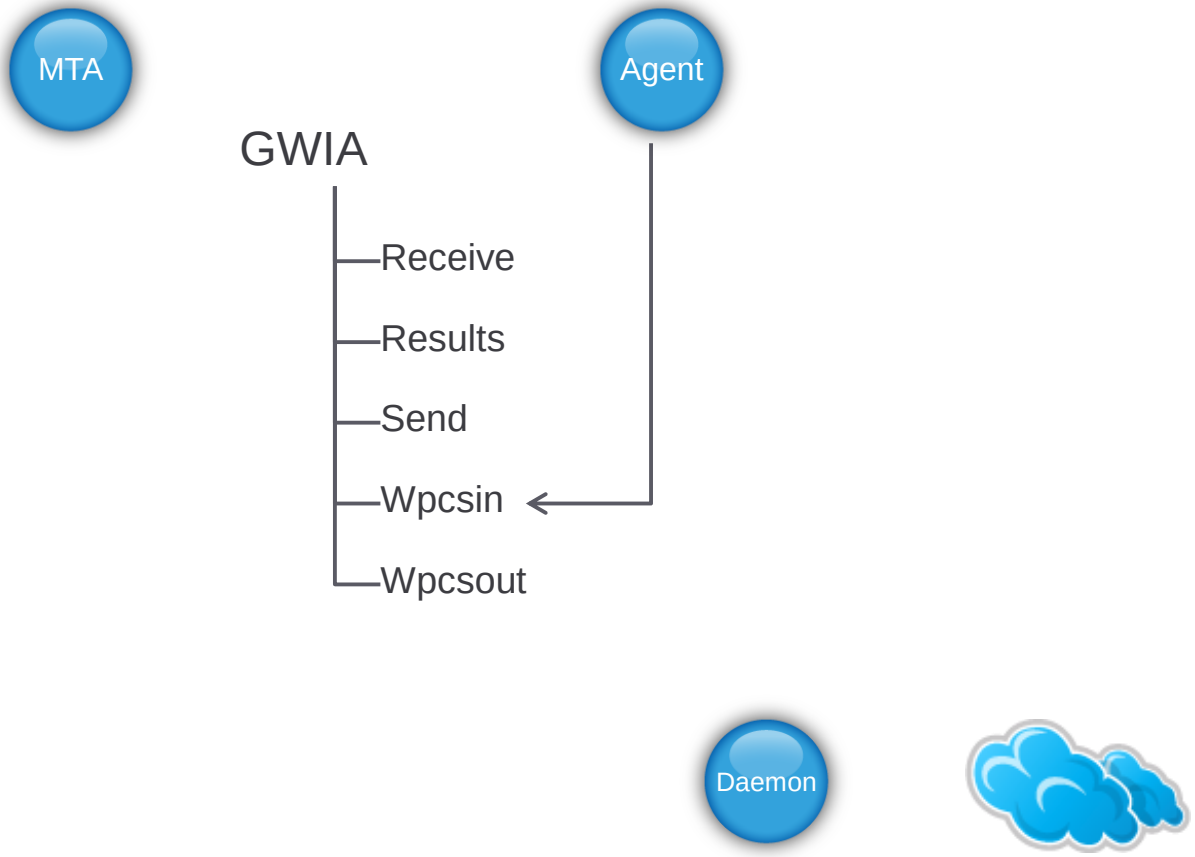
Novell

Message Flow



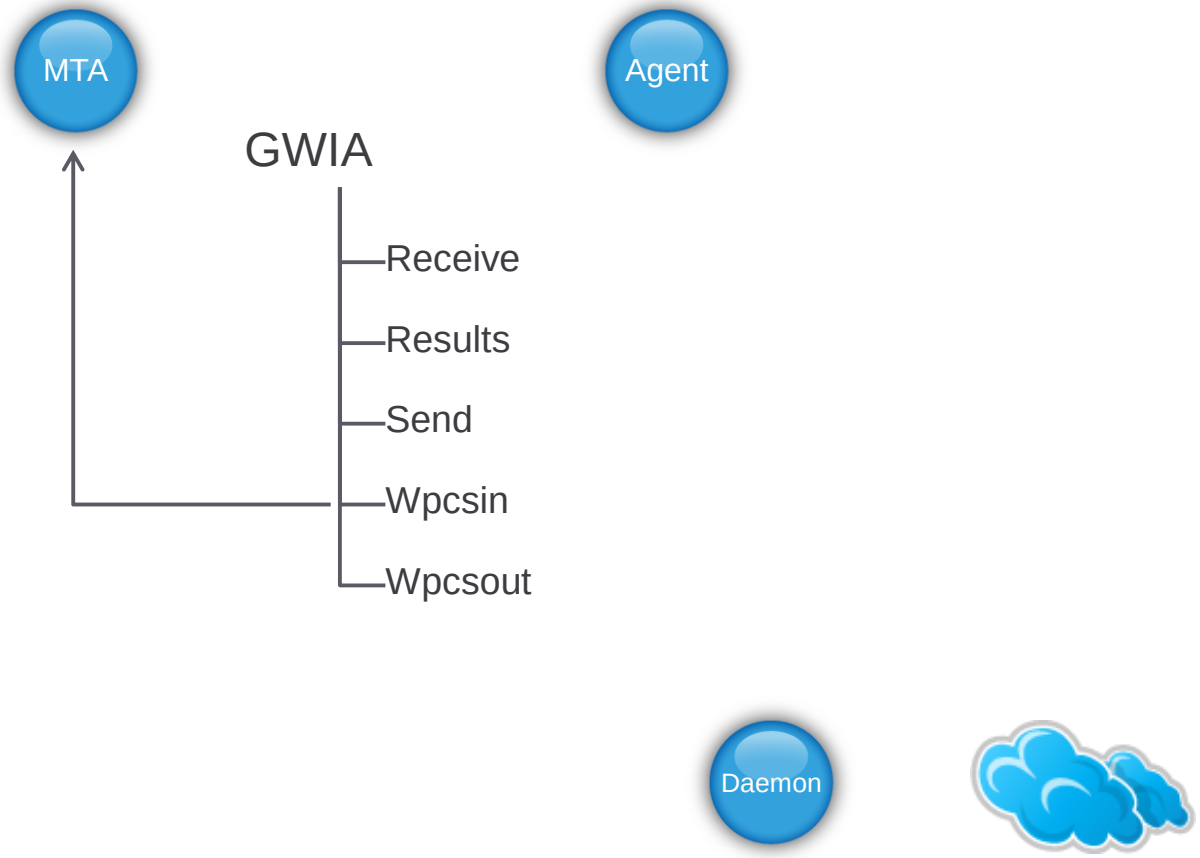
Novell

Message Flow



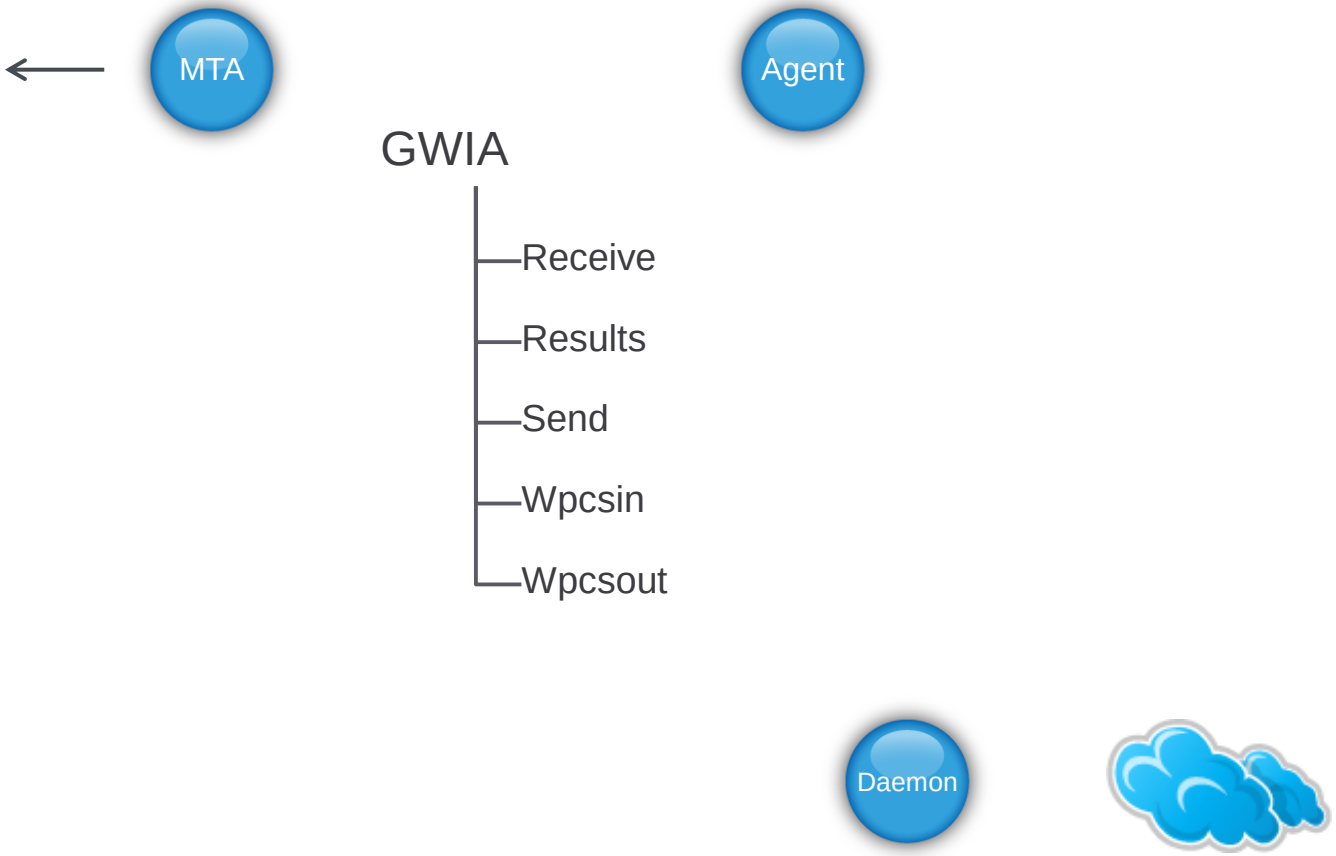
Novell

Message Flow



Novell

Message Flow



Novell.

SMTP Response Messages

- Code
  - 2xx
    - Status: Command succeeded
  - 3xx
    - Status: Command accepted but more information expected
  - 4xx
    - Status: Command failed, however the problem may be temporary. Retry later
  - 5xx
    - Status: Command failed

Novell.

Inbound Undeliverable Messages

- If unknown recipient
  - '550 No such recipient' is returned to sending server
  - Message is dropped without receiving body/attachments
  - The Message is not placed in problem directory
- Why?
  - Saves bandwidth and disk space
- Use nicknames to monitor old addresses
- Service/application accounts should have a mailbox
  - Return paths for bounces and relay denials

Novell.

Troubleshooting

- Telnet to the GWIA on port 25

Helo acme.com

Mail From:john@acme.com

Rcpt To:alice.smith@novell.com

Data

This is a test

.

quit

Novell.

Troubleshooting

HELO relay.example.org
MAIL FROM:john@acme.com
RCPT TO:alice.smith@novell.com
RCPT TO:theboss@novell.com
DATA
From: “John Jones" john@acme.com
To: "Alice Smith" alice.smith@novell.com
Cc: theboss@novell.com
Date: Tue, 15 Jan 2008 16:02:43 -0500
Subject: Test message
Hello Alice.
This is a test message with 5 header fields and 4 lines in the message body.
Bob
.
quit

Novell.

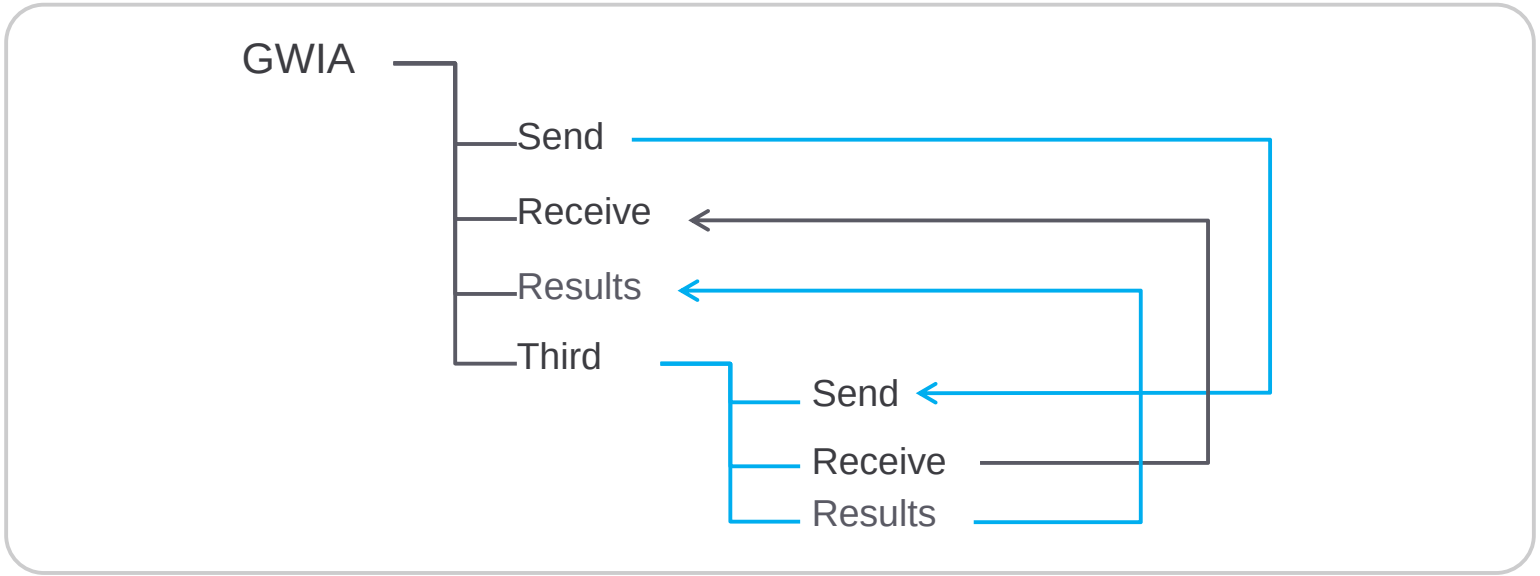
Troubleshooting

- Problem messages are stored in the gwprob directory
  - Can be re-queued
    - Rename the .BAD file to .001 or other number extension
    - Open the message and determine if it is inbound or outbound
    - Modify the message, if required, to correct the problem
    - Move the message in the respective RECEIVE or SEND directory
- These messages can be deleted without causing a problem

Novell.

Troubleshooting

- Third party directory
  - Separate send and receive directory used by daemon
  - Need to move mail between the directories



Tracking inbound messages

GWIA

```
13:12:31 000 DMN: MSG 9321338 Receiving file:/smtpdom2/wpgate/smtpia2/receive/f3fc59d4.606

13:12:32 920      MSG 9321338 Processing inbound message: /smtpdom2/wpgate/smtpia2/receive/f3fc59d4.606

13:12:32 920      MSG 9321338 Sender: fluffy.pilpott@earthlink.net

13:12:32 920      MSG 9321338 Recipient: lkearney@georgiahealth.edu

13:12:32 920      MSG 9321338 Queuing to MTA

13:12:32 920      MSG 9321338 File: /smtpdom2/wpgate/smtpia2/wpcsin/4/4d95cf41.yw7 Message Id:
(4D960780.4F4:148:62708) Size: 2.8 Kb
```

GWIA MTA

```
13:12:33 112 RTR: SMTP2: 00666996.YW4: Routing /smtpdom2/mslocal/gwinprog/4/00666996.YW4 (3 kb)

13:12:33 112 RTR: SMTP2: 00666996.YW4 Priority 4  4D960780.4F4:148:62708 : Transfer to DOMAIN1

13:12:33 112 RTR: SMTP2: 00666996.YW4: Message queued:/smtpdom2/mslocal/mshold/dom219d/4/00666996.001
```

Novell.

Tracking inbound messages

Destination MTA

```
13:12:34 0C5 RTR: DOMAIN1: 0040c817.YW4: Routing e5/domain1:\domain1\mslocal\gwinprog\4\0040c817.YW4 (3 kb)

13:12:34 0C5 RTR: DOMAIN1: 0040c817.YW4 Priority 4  4D960780.4F4:148:62708 : Transfer to DOMAIN1.PO6:OFS

13:12:34 0C5 RTR: DOMAIN1: 0040c817.YW4: Message queued:
e5/domain1:\domain1\mslocal\mshold\po64fc1\4\0040c817.001
```

Destination POA

```
13:12:35 09E MTP:  Received file: E6\mail6:\po6\wpcsout\ofs\4\4d95cf43.YW2, Size: 2996

13:12:35 07E Processing 4d95cf43.yw2 Message ID(4D960780.4F4:148:62708)

13:12:35 07E Sender of message (4d95cf43.yw2) fluffy.pilpott@earthlink.net

13:12:35 07E Distribute message from: fluffy pilpott

13:12:35 07E Begin distribution to 1 users

13:12:35 07E Processed OK
```

Novell.

Open Connections

- netstat -patune | grep ':25' > /tmp/abc.txt
  - Replace 25 with 110, 143, 993 or 995

```
tcp   1 0 10.6.10.97:25   10.6.10.167:61430     CLOSE_WAIT  1071  54707306  19318/gwia
tcp 100 0 10.6.10.97:25   166.137.14.31:39105   CLOSE_WAIT  1071  54699863  19318/gwia
tcp   1 0 10.6.10.97:25   158.93.190.200:44671  CLOSE_WAIT  1071  54685441  19318/gwia
tcp   1 0 10.6.10.97:25   68.47.36.215:52209    CLOSE_WAIT  1071  54707314  19318/gwia
```

Novell.

Questions?


Novell®

Corporate Headquarters
1800 South, Novell Place
Provo, Utah 84606

801.861.7000 (Worldwide)
800.453.1267 (Toll-free)

Join us on:
www.novell.com

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Novell, Inc. may make improvements in or changes to the software described in this document at any time.