NOETICA TECHNICAL SUPPORT INFRASTRUCTURE GUIDANCE

Version 6.1

TABLE OF CONTENTS

Version Control	02
Summary	04
Platform Architecture	04
Verifying Synthesys™/MiCC Outbound Servers and Services are operational	05
Restart Order	05
SQL Server	06
SQL Server Restart Check List	06
SQL Server Recommended Best Practices	06
Application Server	06
Application Server - SynthesysCore Services Control Panel	07
Application Server Restart Check List	07
Application Server Recommended Best Practices	07
Web Server	08
Web Server Restart Check List	08
Web Server Recommended Best Practices	08
NVP/CM Server Checks	09
Noetica Voice Platform/Call Manager Restart Check List	09
Noetica Voice Platform/Call Manager Server Recommended Best Practices	09
Housekeeping and Other FAQ's	10
Hardware	10
Windows Operating System	10
Server Performance	10
Anti-Virus & End Point Protection	10
SQL Database Management	11
Application Management	11
Firewall And Ports	12
Ports required	12
Explanation of ports	12
Application Logs	13

Noetica.

SUMMARY

The Noetica Technical Support team provides a service limited to 2nd line and 3rd line technical support levels for Noetica software-related issues. Please refer to our Noetica Technical Support Policy Documentation for further information on the responsibilities of Noetica Technical Support Services.

This document describes the first line troubleshooting steps that must be carried out by your own IT Support owners. These tasks should be performed prior to escalating a problem into the Noetica Service desk.

It is out of the scope of this document to provide a step-by-step guide to support Microsoft Windows instructions. Noetica assumes your own IT support is familiar with the Windows Server Operating System. Restarting Windows Services, reading Windows Event Logs and checking system environment variables as well as management of supporting Networking functionality including routing, DHCP, DNS and firewalls are deemed to be out of Noetica scope.

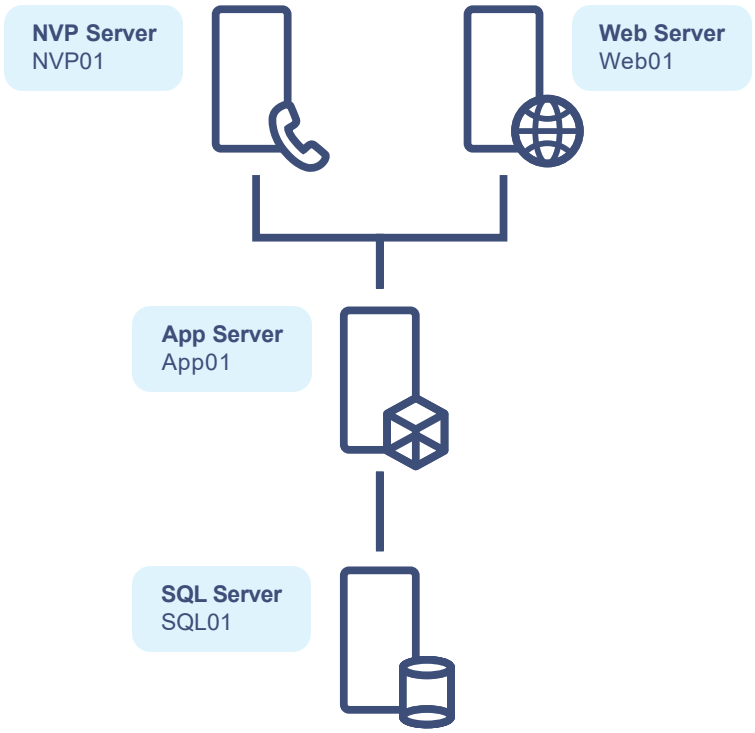
If you have any questions, please contact Noetica and ask to speak to our Technical Support Manager.

PLATFORM ARCHITECTURE

Every customer would have their own arrangement of servers, but generally each platform is made up of the following servers;

1. Database / SQL Server.
2. Synthesys/MiCC Outbound Core Application Server.
3. Web Server.
4. Noetica Voice Platform/Call Manager.
   - With SIP connectivity to an external service provider.
   OR SIP connectivity to another telephony platform/PBX.

Our platform prerequisites detail the minimum system requirements for Noetica software on each server. For smaller deployments servers can perform dual roles or for larger deployments multiple web and NVP/Call Manager servers can exist.



VERIFYING SYNTHESYS™/MICC OUTBOUND SERVERS AND SERVICES ARE OPERATIONAL

Prior to escalating any issue into the support desk, please verify the entire Synthesys/MiCC Outbound platform including server and its services are up and running. In the event that one of the servers or services is not operational, please ensure the steps below are followed to restore them.

You should connect and login to your servers using remote desktop connection to ensure that the server is reachable to the network and functional.

RESTART ORDER

The order for restarting the Servers is extremely important, as this allows services to start up and connect in a particular way where dependencies are present between the servers across the platform.

Servers should be restarted in the following order and sufficient time should be left between restarting one server and the next to allow servers to fully boot and finalise any operating system updates.

At a high level, the following checks should be performed;

1. **SQL**
Check SQL server and SQL reporting services are up and running before rebooting the next machine.

2. **APP**
Check all Synthesys services are up and running before rebooting the next machine.

3. **WEB**
Check all Syntheses Web services are up and running before rebooting the next machine.

4. **CTI(NVP/MiCC-CM)**
Check all Noetica Voice Platform services are up and running.

SQL SERVER

Unless you hold additional SQL DBA support within your Noetica software agreement then we do not cover the operation and maintenance of your database server, this includes the maintenance, backups or the correct performance operation of Microsoft SQL Server. Noetica does provide a recommended maintenance plan for Synthesys/MiCC Outbound databases (this can be supplied on request).

If you have just restarted your platform or the SQL instance supporting the application databases is not responding then the SQL Server services should be checked;

Run 'Services.msc' and check "SQL Server (MSSQLSERVER*)" is running

If you are using our 'Standard Reports' you should verify 'SQL Server Reporting Services (MSSQLSERVER)' is also in the 'Running' state.

SQL SERVER RESTART CHECK LIST

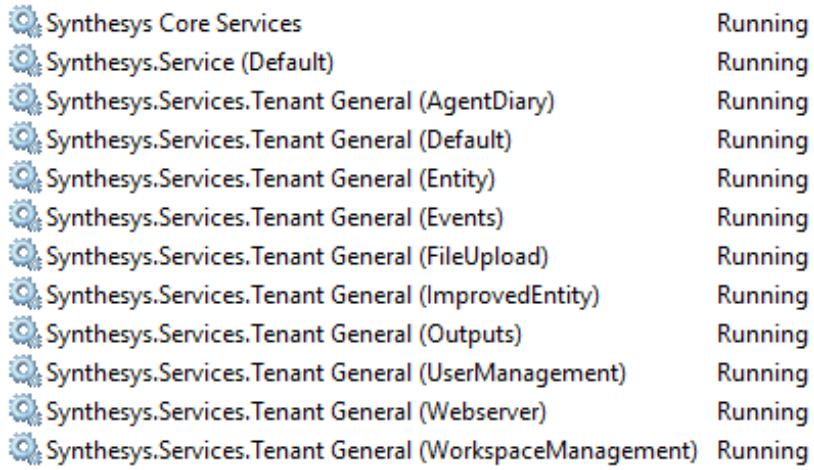
- ✓ SQL Services are running.
- ✓ Server resources are healthy.
- ✓ Any SQL import/maintenance jobs have finished running.
- ✓ Expensive queries or non standard reports are not running against the live SQL databases used by the application.
- ✓ SQL Error logs are clean.
- ✓ Windows Eventlog is not reporting any application errors.

SQL SERVER RECOMMENDED BEST PRACTICES

- ✓ The SQL Server is configured in the most optimum manner. Including memory allocations, disk & RAID configuration, separation of data (MDF) and log (LDF) files.
- ✓ Database backups should be managed.
- ✓ Database maintenance should always be carried out outside of core operational hours including reindexing and organisation.
- ✓ Non standard reports or expensive queries should not be run on the SQL server during operational hours.
- ✓ Regular Database integrity and consistency checks are performed.
- ✓ SQL Data File size checks against SQL Data storage within these files.
- ✓ SQL Log file growth, truncating and backup.
- ✓ For larger sites, the use of Data Warehousing or a separate archived database should be implemented.
- ✓ Management of SQL Replication to separate reporting instances.
- ✓ Daily review of SQL jobs, tasks and event logging.
- ✓ Setup of email notifications is advised.

APPLICATION SERVER

The Synthesys/MiCC Outbound Application Server is the heart of the solution and is where the 'Core' application is installed. If you have just restarted your platform, run 'Services.msc' and check the below Windows services are in a 'running' state.



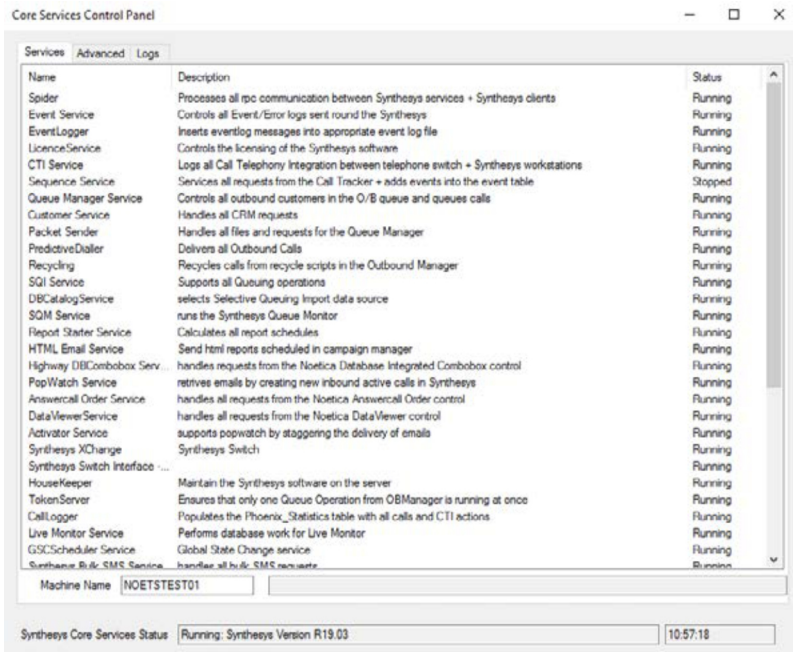
Please restart any service that are in a stopped state. If they fail to start, investigation will be required and a ticket being logged with Noetica Technical Support.

APPLICATION SERVER - SYNTHESYS CORE SERVICES CONTROL PANEL

The 'Synthesy Core Services' service as can be seen in the above image can be described as the engine of the application and is the first Windows service in the sequence of services that needs to be running. The service houses core components such as the predictive dialler, API and Web services, data import/export utilities and CTI integration and runs these as subsidiary services. The Control Panel allows you to access and interact with these services and check their state.

To access the Control Program, you can run the shortcut on the desktop of the application server which is installed for all users.

If you do not see the shortcut, you can launch the Control Panel directly from the following path \\[APPSERVER NAME]\Synthesys\Server\bin\CoreServicesControlPanel.exe



If a service is not in the running state, you can right click on the service and select to 'start' the service. This should be attempted to see if the problem is resolved. If they fail to start, investigation will be required and a ticket being logged with Noetica Technical Support.

APPLICATION SERVER RESTART CHECK LIST

- ✓ Services are running.
- ✓ All Core Services in control panel are running.
- ✓ CTI integration services (Mitai Interface) are running.
- ✓ Server resources are healthy.
- ✓ Windows Eventlog not reporting any application errors.

APPLICATION SERVER RECOMMENDED BEST PRACTICES

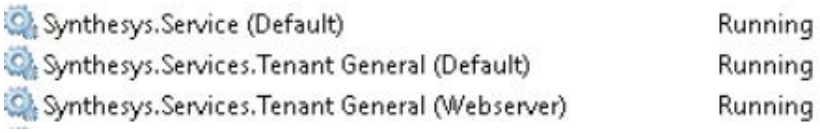
- ✓ Synthesys Windows services are set to automatic delayed start.
- ✓ Application service user passwords are strong and set to never expire. If passwords do need changing this should be scheduled with Noetica for reconfiguration to take place.
- ✓ Service users should be local admins of the machine.
- ✓ Fragmentation levels of disks are checked periodically.
- ✓ Virus exclusions are in place.
- ✓ Network/bandwidth performance regularly monitored.
- ✓ Service monitoring in place.
- ✓ UAC should be disabled.
- ✓ Windows updates should be enabled and configured to only run outside of operational hours.

Noetica.

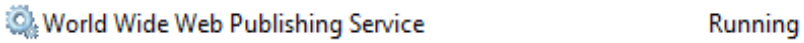
WEB SERVER

The Web Servers are used to deliver the Synthesys/MiCC Application's via the web browser to the agents.
If you have restarted the server or can no longer access any of the front facing websites such as the agent portal then please conclude the following checks.

Run 'Services.msc' and check the following services are in a 'Running' state.



The web services operate under Microsoft IIS (Internet Information Services). Please check that IIS is up and running on your server and that the service 'World Wide Web Publishing Service' is in a 'Running' state.



Checks should be performed using the IIS Manager to ensure that 'Synthesys General' and Synthesys related websites are operational (not stopped) and the related Application Pools are operational. An IIS reset can also be performed if needed.

WEB SERVER RESTART CHECK LIST

- ✓ Services are running.
- ✓ Server resources are healthy.
- ✓ IIS is running and functional.
- ✓ All front end sites are accessible.
- ✓ Connection from Agents machine is allowed over the network and not restricted by network/server congestion or a bottleneck via a VPN connection or proxy server for instance.
- ✓ Agents can log in and start work.
- ✓ Windows Eventlogs not reporting any application errors.

WEB SERVER RECOMMENDED BEST PRACTICES

- ✓ Synthesys Windows services are set to automatic delayed start.
- ✓ Application service user passwords are strong and set to never expire. If passwords do need changing this should be scheduled with Noetica for reconfiguration to take place.
- ✓ Service users should be local admins of the machine.
- ✓ Fragmentation levels of disks are checked periodically.
- ✓ Virus exclusions are in place.
- ✓ Network/bandwidth performance regularly monitored.
- ✓ Service monitoring in place.
- ✓ UAC should be disabled.
- ✓ Windows updates should be enabled and configured to only run outside of operational hours.
- ✓ IIS application pools configured to recycle out of operation hours.
- ✓ IIS logging disabled and switched on only when required.
- ✓ For larger deployments multiple web servers can be used and load balancing can be implemented.

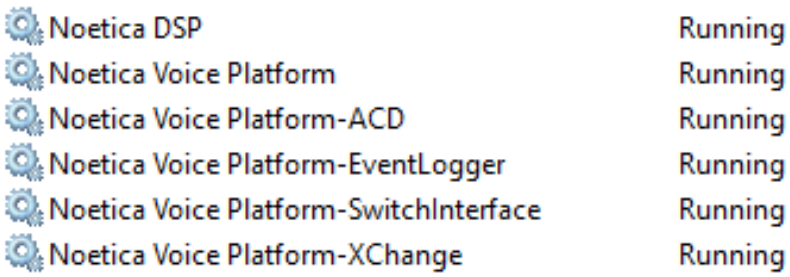
NVP/CM SERVER CHECKS

The Noetica Voice Platform/Call Manager server handles the telephony element of the application and allows the application to make/receive calls via a dedicated sip trunk. The Synthesys Application Server will communicate directly with the Noetica Voice Platform to enable the telephony integration.

The Noetica Voice Platform (Call Manager) is comprised of a number of key elements;

- Noetica DSP Service: This services handles all SIP signalling and RTP traffic in and out of the server. It is therefore very important that firewall/group policies are only changed with careful consideration. You should ensure that guidance is provided by your SIP provider and Noetica if any changes are required here.
- Noetica Voice Platform XChange Services: These are the NVP core services that interface with the application. They also handle the ACD, IVR's, Call Recording and other functionality required for the NVP to operate.
- SIP line connectivity: Connection to a SIP Provider or MiVB/MiVC will be defined in the configuration on this server.
- Call Recording: The NVP will provide call recording (Full, Agent & Customer) – as long as it is correctly enabled. This necessitates the need for the NVP Server disk configuration to be correctly setup and sized for the storage of the call recordings. It is possible for the NVP to move call recordings to an alternative storage location after recording; this could be onto a separate SAN disk or NAS device.

Run 'Services.msc' and check the below Windows services are in a 'running' state.



NOETICA VOICE PLATFORM/CALL MANAGER RESTART CHECK LIST

- ✓ Services are running.
- ✓ Server resources are healthy.
- ✓ Softphone registration works and configuration is correct.
- ✓ Connection from Agents machine is allowed over the network and not restricted by network/server congestion or a bottleneck via a VPN connection or proxy server for instance.
- ✓ Two way audio can be established and if not firewall/routing has been checked.
- ✓ The SIP provider is providing an optimum level of service.
- ✓ The SIP trunk to MiVB/MiVC or other telephony switch is online and can be pinged.

NOETICA VOICE PLATFORM/CALL MANAGER SERVER RECOMMENDED BEST PRACTICES

- ✓ Synthesys Windows services are set to automatic delayed start.
- ✓ NVP service user passwords are strong and set to never expire. If passwords do need changing this should be scheduled with Noetica for reconfiguration to take place.
- ✓ Service users should be local admins of the machine.
- ✓ Fragmentation levels of disks are checked periodically.
- ✓ Virus exclusions are in place.
- ✓ Network/bandwidth performance regularly monitored.
- ✓ Service monitoring in place.
- ✓ Windows updates should be enabled and configured to only run outside of operational hours.
- ✓ Separate SAN disk or NAS to archive call recordings.
- ✓ Sip provider can handle a minimum of 15 calls per second (CPS) for each 100 concurrent predictive dialler agents.
- ✓ Checking firewall and routing rules with your sip provider to ensure all media ports are allowed.

HOUSEKEEPING AND OTHER FAQ'S

This part of the describes further best practices that should be considered and maintained by IT support teams.

HARDWARE

It is essential to manage the physical hardware that hosts the software. Below are a list of the most common items that need to be checked.

- ✓ Disks are operating in an optimal state; degraded disks can cause major performance problems.
- ✓ RAID Controller back up batteries, these may need replacing from time to time, these batteries can save hours of database repair works in a critical situation.
- ✓ Server production life. 3-5 years is the usual bracket for operating a live production server within.
- ✓ Server infrastructure should be placed under a support agreement so that replacement parts can be acquired in a timely manner.
- ✓ Network connectivity to the server infrastructure is adequately managed and configured.

WINDOWS OPERATING SYSTEM

The installation, configuration and maintenance of the Server operating systems is also essential for correct systems operation.

- ✓ The operating system should be patched regularly against a set schedule.
- ✓ Malware Protection should be configured and updated.
- ✓ Exceptions should be in place for specified Synthesys directories.
- ✓ Backup processes should be in place.
- ✓ SQL Backup is especially important, as regular transactional log backups should be managed
- ✓ Disk space should be monitored and never allowed to be low.
- ✓ Server real-time monitoring tools should be enabled to provide proactive information.

SERVER PERFORMANCE

Server checks should be carried out against the points listed below on all serves, this is especially important if server monitoring systems have not been implemented.

- ✓ Hard disks have sufficient free space.
- ✓ Check to ensure that memory and CPU usage is not operating at high utilisation, ie 100%
- ✓ Check to ensure that hard disk usage (disk queuing) is outside of normal operating values. Windows Resource Manager can be used for identifying processes that are causing the servers performance to be hindered. A common cause of performance problems have been certain Malware protection products and backup services that operate during operational hours.

ANTI-VIRUS & END POINT PROTECTION

Server performance can severely be hampered with real time scanning enabled, this can either block the communications between the server and client machines or severely increase load on server resources which could cause a number of performance related issues for the contact centre and agents. Noetica do not make any recommendations on Anti-Virus Products but do recommended you chose an AV where exclusions can be defined when real time scanning. Full system scans can still be scheduled outside of contact centre operational hours. Please check following AV exclusions are set from real time scanning, the below paths should include all subdirectories.

- **App**
  \\APP_SERVER\Synthesys*\Program files\Noetica\Synthesys.NET
- **Web**
  *\Program file\Noetica\Synthesys.NET
- **NVP**
  *\Synthesys\ *\Voice Platform\

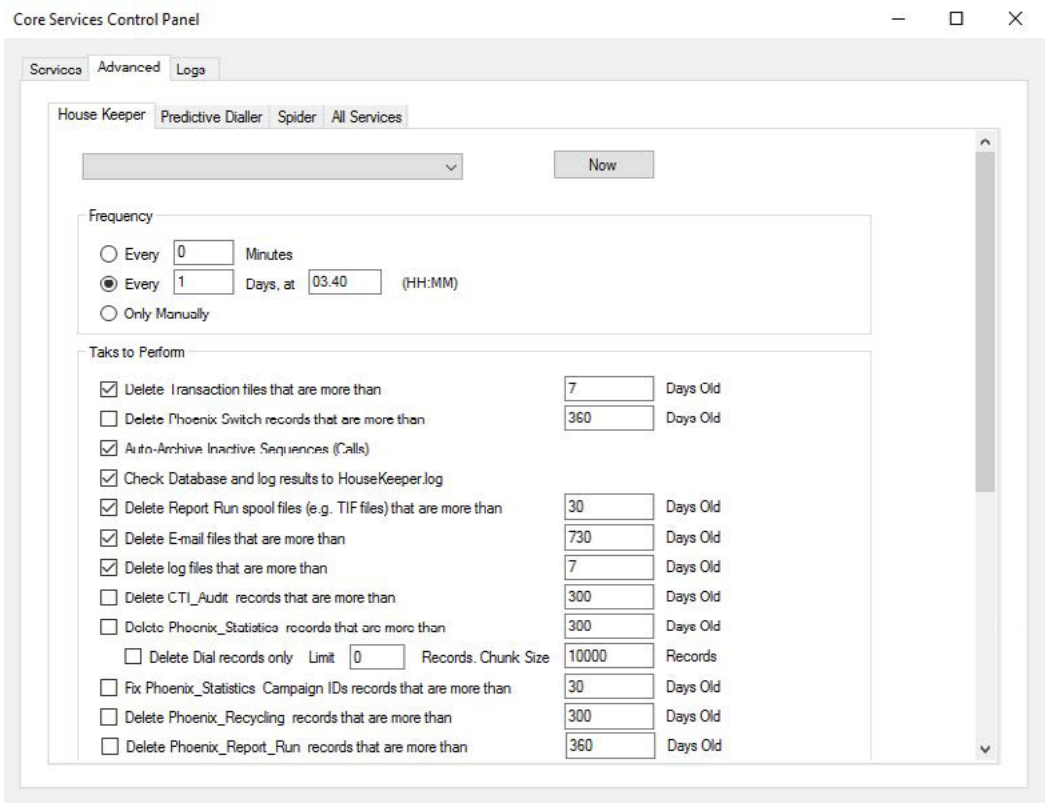
SQL DATABASE MANAGEMENT

The SQL database is probably the most important components of the system. Microsoft SQL Server manages many basic tasks within its standard installation however, the Synthesys databases can grow due to all of the call and campaign data that is managed by the system. It will be a requirement for a SQL Database Administrator to be allocated to manage the SQL Server databases on a scheduled basis.

APPLICATION MANAGEMENT

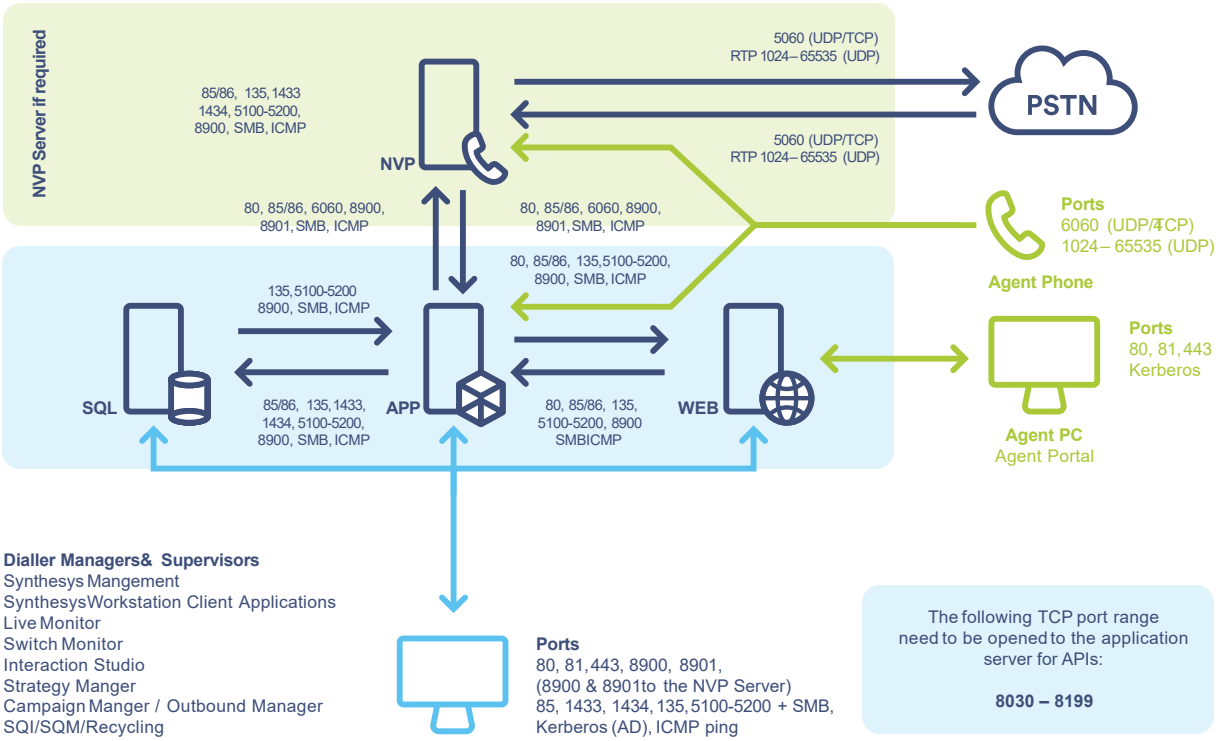
Within the Synthesys/MiCC Outbound product is the Housekeeper service and its configuration is accessible via the Core Services control Panel. This service allows some lightweight tidy-up of the DB and will be covered in detail during system training. It is important that this is configured before beginning to use Synthesys in a production environment. Initial configuration is required and other higher levels of DBA support would be required later to manage data levels and other tables.

The Housekeeper should be configured with different values depending on the size of platform and other components that maybe enabled. A large contact centre will generally store 120 days of data in the production system, any data older than this will be archived and accessed within a separate data store.



FIREWALL AND PORTS

The following network ports are used within the solution:



Dialler Managers& Supervisors
Synthesys Mangement
SynthesysWorkstation Client Applications
Live Monitor
Switch Monitor
Interaction Studio
Strategy Manger
Campaign Manger / Outbound Manager
SQI/SQM/Recycling

Ports
80, 81, 443, 8900, 8901,
(8900 & 8901to the NVP Server)
85, 1433, 1434, 135, 5100-5200 + SMB,
Kerberos (AD), ICMP ping

The following TCP port range need to be opened to the application server for APIs:

8030 – 8199

Pleasenote: Additional firewall rules and port configuration may be required depending on the overall design.

PORTS REQUIRED

Originating Machine	Destinaation Machine	Port / Protocol
App Server	Web Server	Ports 80, 85/86, 135, 5100-5200, 8900, SMB, ICMP
Web Server	App Server	Ports 80, 85/86, 135, 5100-5200, 8900, SMB, ICMP
App Server	SQL Server	Ports 85/86, 1433, 1434, 5100-5200, 8900, SMB, ICMP
SQL Server	App Server	Ports 135, 5100-5200, 8900, SMB, ICMP
Web Server	SQL Server	No connection required
Client Machines	Web Server	Ports 80, 81, 443, Kerberos
Client Machines	App Server	Ports 80, 81, 443, 8901, 85, 1433, 1434, 135, 5100-5200, SMB, Kerberos, ICMP
For NVP if required		
NVP Server	App Server	Ports 80, 85/86, 5060, 6060, 8900, 8901, SMB, ICMP
App Server	NVP Server	Ports 80, 85/86, 5060, 6060, 8900, 8901, SMB, ICMP
Client Phone	NVP Server	Ports 5060/6060, 1024-65535 (UDP)

EXPLAINATION OF PORTS

Port	Description
85-86	Used for internal communication by Synthesys; these can be reconfigured.
80	Used for Interaction Studio to communicate with Synthesys Web Server; can be reconfigured, but this requires manual configuration on client machines.
81	Used for web based applications (Portal); can be reconfigured.
135, 5100-5200	Used by MSDTC. The 5100-5200 range can be reconfigured.
1434	This is used by SQL Browser to negotate SQL connections as well as browsing.
1433	Default port used for SQL Server connections; can be reconfigured.
8900/8901	Used for web services communication.
8030-8199	Used for API connectivity.
For NVP if required	
5060/6060	Used for SIP connectivity.
1024-65535	Used for RDP voice.

Noetica.

APPLICATION LOGS

The Noetica Platform generate a large amount of logs for each of the SynthesysApplication modules including the NVP. Application logs are generally stored on the server for 7 days and archived for 30 days before being purged; however this can be adjusted.

- ✓ Logs can generally be found within the .\Synthesys\EventLogsfolder or on the NVP server .\Voice Platform\ LogFiles on the NVP.
- ✓ Logs are named inline with the application module.
- ✓ Additional logging can be found within the Phoenixdatabase, within the EventLogtable.
- ✓ Microsoft Windows EventLogs can contain details of critical errors and should be checked periodically.
- ✓ Understanding of these logs do require Noetica Resourceand issues/errorsshould be logged with the Noetica Technical Support team via a ticket

Call. 0345 0181070
Email. marketing@noetica.com
Visit. www.noetica.com

London office.
The Beehive Building, City Place
Gatwick, RH6 0PA, UK.

Durham office.
Unit 17,City West Business Park
St. Johns Road,Meadowfield Industrial Estate
Durham DH7 8ER, UK.

© Noetica Limited 2022.All rights reserved.