Opus™ Guide for IT Managers

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>System Requirements</td>
<td>2</td>
</tr>
<tr>
<td>Configuration</td>
<td>3</td>
</tr>
<tr>
<td>Integration</td>
<td>3</td>
</tr>
<tr>
<td>Networking</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>5</td>
</tr>
<tr>
<td>Interconnectivity</td>
<td>6</td>
</tr>
<tr>
<td>History Archival Sizing</td>
<td>7</td>
</tr>
</tbody>
</table>

Introduction

Opus, powered by the Niagara\textsuperscript{AX} Framework, is a suite of Java-based products designed to integrate a variety of devices and protocols into a common distributed automation system. It incorporates software technology to integrate diverse systems and protocols into a common model, embedded at the controller level and supported by a standard Web browser interface. Opus enables monitoring and control systems based on LonWorks, BACnet, Modbus and a wide range of legacy protocols to work together as a seamless web-enabled system. Opus also includes integrated network management tools to support the design, configuration, installation and maintenance of interoperable networks.

This document addresses IT management concerns and issues related to Novar’s Opus product line and Niagara Framework. The following figure shows a typical Opus architecture:

![Figure 1. Typical Opus Architecture](image-url)
An Opus installation can consist of one or more of the following components:

**xcm.10, xcm.20, xcm.10S and xcm.20R controllers:** XCM site controllers are devices that provide integrated control, supervision, and network management services for networks of monitoring and control devices. When connected over an Ethernet network, XCM's can communicate with each other on a peer-to-peer basis as well as communicating with other Ethernet-based devices. With the optional Web User Interface Service (UI), an XCM can serve graphical views of the information contained in the connected devices to a Web browser such as Internet Explorer™.

**Opus Supervisor:** The Opus Supervisor is a flexible network and data server for multiple XCM site controllers. The Opus Supervisor is designed to provide efficient integration and aggregation of the information coming in from multiple, deployed XCM controllers. In effect, the Opus Supervisor provides a single point of access for these multiple devices, while providing a powerful network environment with comprehensive database management, alarm management and messaging services. In addition, the Opus Supervisor provides the engineering environment (coupled with Opus Architect) used to set up and manage systems, and a graphical user interface. This software is designed to run on Windows and Windows Server Operating Systems. It can be connected to the Internet or Intranet where the system’s graphical views can be accessed using a Web browser such as Internet Explorer™.

**Opus Architect:** This is the Opus engineering client tool that is used to create applications by defining components and wiring them together to create logic and displays. It allows the user to develop comprehensive applications for control, monitoring, alarming, data logging, reporting, and real-time data visualization using a single graphical tool. Opus Architect installs and runs as a standalone application on a PC and is connected to either an Opus Supervisor or XCM site controller.

**Niagara Daemon:** This is a Windows service application installed with Opus that provides the runtime services for running the Opus Supervisor on a Windows PC platform. This service must be running for the Opus Supervisor to execute. The service provides the user with the “Platform” configuration services allowing for the configuration, software upgrades, network configuration and fault recovery of the Opus Supervisor application.

---

**System Requirements**

For currently supported hardware, operation systems and software
Reference release notes for the specific Opus release.

Configuration

When configuring Opus systems, you need to consider functional, size and performance requirements.

The ability of an Opus Supervisor to support large numbers of XCM stations is dependent on the hardware, software, system and application configuration.

Please keep the following guidelines in consideration when configuring large systems:

Consider dedicating the computer to running Opus Supervisor. Avoid running other high performance software and applications not related to Opus.
Separate, dedicated instances of the Opus Supervisor may be used to collect alarms and histories into centralized database. This can reduce resource burdens on the main supervisor instance used for day to day site browsing.
Randomize histories imports to ensure imports happen over a period of time and not concurrently from all XCM stations.

Ensure adequate process heap memory has been configured in the nre.properties file (located in \Novar\Opus-x.x\lib). The minimum recommended process heap memory for Opus is 1024 MB.

On a Windows 32 bit Operating system, no more than 1.2 GB (when 4-8 GB of RAM is available) should be allocated to Opus, to ensure other non-Opus system processes run as intended.

On a 64 bit Operating system, no more than 10 GB (when 24-32 GB of RAM is available) should be allocated to Opus, to ensure other non-Opus system processes run as intended.

Integration

Opus uses a proprietary Fox communication protocol implemented over a TCP/IP based connection. Other standard protocols supported are HTTP, HTTPS, SMTP, DNS, DDNS, NTP, FTP, Telnet and SNMP (optional) protocols. Implementation of these protocols complies with their associated Requests for Compliance.

Networking

Network Traffic and Bandwidth
The following categories of traffic will affect network bandwidth for an XCM system controlled by Opus Supervisor:

Configuration

Configuration traffic is associated with the initial setup and commissioning of an Opus implementation. Commission and download of an XCM site controller is typically done one time and entails sending software upgrades and control application configuration to the XCM. During system commissioning, bandwidth will vary according to the number and type of objects being configured.

Browsing

Day to Day single user browsing traffic depends on runtime conditions. This is where the user of the Opus Architect client connects to the Opus Supervisor and the user navigates and connects to an XCM site controller to browse the site for viewing current operating conditions. The frequency is based on the user roles and availability. The bandwidth usage is typically a nominal 10 kbit/sec usage with 1-2 sec peaks at 3 Mbit/sec bursts.

History Collection

History collection traffic is the scheduled transfer of historical data being passed from the remote XCM site controllers to the Opus Supervisor. This can be tuned to fulfill operational requirements and bandwidth considerations. The formula for calculating history collection bandwidth is:

- Single point: ~150 kbit/sec for ~2 seconds (1x per day)
- 300 points: ~115 kbit/sec for ~90 seconds (1x per day)

Real-time data and inter-XCM link traffic is transferred from station to station for operational purposes. Inter-XCM links might be used for peer-to-peer control or other similar activities. This can be tuned to fulfill operational requirements and bandwidth considerations.

Alarm reporting traffic is data sent when alarm conditions within the XCM site controllers are detected. The alarm messages are optionally sent to the Opus Supervisor to be reported and archived. The number and frequency of these alarm messages depends on how aggressively the alarm set-points are configured within the XCM controllers. The size of an alarm packet can vary between 1 kbytes and 1.5 kbytes. The bandwidth usage for a typical alarm transfer is:

- Single alarm: ~ 10 kbit/sec for < 1 second.

Novar can work with end users to configure their systems to ensure
minimal impact to their networking environment.

**DHCP**

All current versions of Opus support DHCP, but static IP addresses provide the most reliable connectivity. Opus does not support dynamic native DNS; therefore, the DHCP server must be linked to the DNS server or HOSTS files on each station must be used.

DHCP can be used reliably if users:

- Reserve a static DHCP address for the MAC address of each Opus device and set the device for DHCP. When the device requests a DHCP address, it will be assigned the same one.

- Use a HOSTS file on each Opus station.

**Communication**

The XCM initiates conversation with an Opus Supervisor:

- When an alarm event occurs in the XCM.
- To archive data. This conversation is based on log setup.
- If the XCM is set-up to monitor the Opus Supervisor.

The Opus Supervisor initiates conversation with an XCM:

- If the Opus Supervisor is set up to monitor the XCM.
- If global functions (e.g., Master Schedules) are set up in the Opus Supervisor and a change is made.
- If the TimeSync Server function is set up on the Opus Supervisor, the TimeSync Client function is setup on the XCM, and the XCM sends a time synchronization call to the Opus Supervisor.

**Security**

**Security Policy Support**

LDAP authentication is support. The Opus Supervisor can be configured to authenticate LDAP user credentials by configuring the network provided Active Directory properties into the LDAP user service within the supervisor. Also, the supervisor can be configured for single sign-on that allows this same active login to be used when navigation changes between remote XCM site controllers. This eliminates the user needed to re-enter credentials each time the access a new XCM site controller.

Alternately, the Opus Supervisor provides a proprietary authentication scheme that is maintained in a database within the supervisor and in all remote XCM site controllers. This authentication mechanism can be optionally configured for strong passwords. With strong passwords, the
local user password must meet the following minimum requirements:

- 8 characters in length
- 1 alphabetic character in upper case
- 1 alphabetic character in lower case
- 1 special character (!@#$%_0123456789)

**Opus System Security**

The topic of Opus system access occasionally raises concerns related to hacking and compromised security measures.

Opus software uses a proprietary protocol referred to as the Fox protocol used between the Opus Architect, Opus Supervisor and the Opus XCM site controllers. A Virtual Private Network (VPN) can be used to provide additional security.

The following IP port designations are the default settings. This can be configured as required by the user to fit individual security and network requirements.

- Port 1911/tcp must be open to provide the Fox communication access for Opus Architect, Opus Supervisor and the Opus XCM site controllers.

- Port 80/tcp must be open to provide HTTP access so that users accessing the Opus Supervisor and XCM site controllers can view Web pages of system data.

Optional: Port 443/tcp must be open to provide HTTPS access so that users accessing Opus Supervisor and XCM site controllers can view Web pages of system data.

- Port 3011/tcp is used for platform administration of the Opus Supervisor and/or the Opus site controllers. This includes administrative services such as software upgrades, network configuration properties and license management.

**Interconnectivity**

**Network Integration**

Leverages existing VPN architecture
Opus communication protocols can be used across 3rd party Network Address Translation devices
Ports 1911/tcp, 80/tcp and 3011/tcp are the minimum set of port numbers used for access; these can be changed to fit an end user’s individual security requirements.

**Opus Supervisor Tunneling**
The Opus Supervisor can be set up as the only Opus component exposed for network access and still provide access to the entire Opus network of deployed XCM site controllers in the enterprise. The Opus Supervisor provides tunneling capabilities on the 1911/tcp, 80/tcp and 3011/tcp port connection sessions. This allows an Opus Architect client connecting to the Opus Supervisor via a secure VPN connection to tunnel communications through this supervisor connection to a remote XCM site controller.

**System Backup**

Opus uses an Backup Service to back up the configurations maintained in the remote XCM site controllers. The Backup Service “zips” an XCM station’s entire directory of files into a WinZip®-compatible file. Opus Supervisor can be configured to backup all deployed XCM on a schedule. A user definable number of backups are stored into the supervisor local file system and are available for restoration at any time.

Backup zip files are stored within the local file system install directory of the Opus Supervisor. Each remote XCM site controller has a dedicated folder to contain the backups from that XCM. By default, the Opus Supervisor will maintain the last two backups for each XCM. This can be changed by the user.

**Viruses**

The Opus Supervisor and XCM stations operate a proprietary Web server. As part of normal XCM station operations, files are not downloaded from remote hosts. If the Opus Supervisor is installed on a computer used for non-Opus functions, end users should install virus protection. In addition, unused ports can be closed to prevent hackers from using them to access Windows-based XCM platforms.

**Network Management Tools**

The Opus application provides all the tools required to manage the XCM stations.

**History Archival Sizing**

Opus alarm history data can be archived to either a file based data store or to an MS-SQL database. The following sections provide guidelines for these archives.

**Alarms**

When file archival is specified, all alarms received by the Opus Supervisor are stored into a single file. The size of the file will vary based on the configuration of the remote XCM stations. The following can be used to calculate an approximate size of the alarm database file.
1 Alarm = ~4090 bytes

The Opus Supervisor can be configured to limit the maximum number of alarms to maintain in the local file database.

**MS-SQL Database**

Created empty database (baseline): DB File = ~2 Mb
General Overhead – added Opus tables: DB File = ~2 Mb

1 Alarm Record = ~ 1750 Bytes

(Note: this may not include additional space used by indexing.)

**Sizing Illustration:**

1 site reports 20 alarms / day = ~35 kbyte
1 site x 1 year = ~12.77 Mbyte
100 sites x 1 year = 1.277 Gbyte

**History File Database**

When file archival is specified, each Opus history extension generates a single file in the Opus Supervisor file database. The size of the file will vary based on the configuration of the remote XCM stations. The following table outlines the sizing parameters for each history extension type.

<table>
<thead>
<tr>
<th>History Point Extension type</th>
<th>file header byte size</th>
<th>bytes per history record</th>
<th>Sample=500 records (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpusNumericIntervalHistoryExt</td>
<td>1020</td>
<td>16</td>
<td>9020</td>
</tr>
<tr>
<td>OpusBooleanIntervalHistoryExt</td>
<td>781</td>
<td>13</td>
<td>7281</td>
</tr>
<tr>
<td>OpusEnumIntervalHistoryExt</td>
<td>751</td>
<td>16</td>
<td>8751</td>
</tr>
<tr>
<td>OpusStringIntervalHistoryExt</td>
<td>744</td>
<td>64</td>
<td>32744</td>
</tr>
<tr>
<td>OpusNumericCOVHistoryExt</td>
<td>963</td>
<td>16</td>
<td>8963</td>
</tr>
<tr>
<td>OpusBooleanCOVHistoryExt</td>
<td>728</td>
<td>13</td>
<td>7228</td>
</tr>
<tr>
<td>OpusEnumCOVHistoryExt</td>
<td>712</td>
<td>16</td>
<td>8712</td>
</tr>
<tr>
<td>OpusStringCOVHistoryExt</td>
<td>706</td>
<td>64</td>
<td>32706</td>
</tr>
</tbody>
</table>

**MS-SQL Database**
Created empty database (baseline): DB File = ~2 Mb
General Overhead – added Opus tables: DB File = ~2 Mb
Added 1st XCM with 175 history points x 300 records: DB File = ~5.1 Mb
Added 100 additional XCM overhead with No histories: DB File = ~5.1 Mb
Therefore the additional overhead per site is negligible.

The significant increase will come when importing histories. Histories will continue to accumulate daily unless database maintenance is performed to reduce database size.

For additional histories per site per point, you can use following formula to add to previous baseline.

**Sizing (typical configuration) Illustration:**

For 1 day logs for 1 site with 175 points x 96 intervals per day:
history table size = \(\frac{(175\times96)}{112\times8192} = 1.228,800\) bytes per day per site.

Therefore, for an example of 100 sites for a full one year without maintenance, the database size would grow to:

\[
1.228,800 \times 100 \times 365 = \sim 44,851,200,000 \text{ (44.8 GByte)} / \text{year}
\]

**Maximum Sizing (atypical configuration) Illustration:**

For 1 day logs for 1 site with 175 points x 96 intervals per day:
history table size = \(\frac{(175\times96)}{21\times8192} = 6,553,600\) bytes per day per site.

Therefore, for an example of 100 sites for a full one year without maintenance, the database size would grow to:

\[
6,553,600 \times 100 \times 365 = \sim 239,206,400,000 \text{ (239.2 GByte)} / \text{year}
\]