



# Deployment Scenarios

## Sun Cobalt™ Control Station

### Summary

The Sun Cobalt™ Control Station is a network-based appliance for managing a large number of remote servers and for deploying services to these servers. A control station is deployed according to your specific needs. You need to consider both the security and the scalability of the network configuration into which you will deploy a control station.

There are numerous ways of deploying a control station in your network and for each network configuration, there is a set of issues to bear in mind. This document provides a set of likely scenarios and the issues that you need to take into consideration for each.

***IMPORTANT:*** These scenarios represent a number of possible installations for a Sun Cobalt Control Station. Keep in mind that each network is unique and that you must follow your own security guidelines to ensure the security of your network and control-station installation.



## 1. Security Scenarios

The Sun Cobalt Control Station manages the servers through an agent; this agent is either “pushed” out to and installed on a managed server or it is pre-installed and manually enabled on a managed server. The Software Management module and BlueLinQ operations use a “pull” operation over an HTTP connection. The Control Station uses several TCP/IP ports to control the managed servers. The Control Station uses the following ports:

- **Port 27000** – used by the Control Station to communicate with the agent. This connection is authenticated and encrypted (see *Authentication Technical Details* later in this document).
- **Port 80** – used by the Health Monitoring module to send health-status data.
- **Port 80** – used to access the Control Station acting as a BlueLinQ server from a BlueLinQ-enabled client (if required)
- **Ports 80, 81 and 444** - used by the Control Station to install the Control Station agent. Once the agent is installed, access is no longer required to ports 81 and 444.

### 1.1 Configuring the Basic Firewall on the Sun Cobalt Control Station

If you enable the Basic Firewall feature on the Sun Cobalt Control Station, at a minimum, you must create these five input rules so that the control station functions properly.

To add these rules, see the section “Adding an input rule” in the user manual entitled *Administrator Manual*.

**Note:** For each rule, enter the information provided for the fields indicated. Leave all other fields blank.

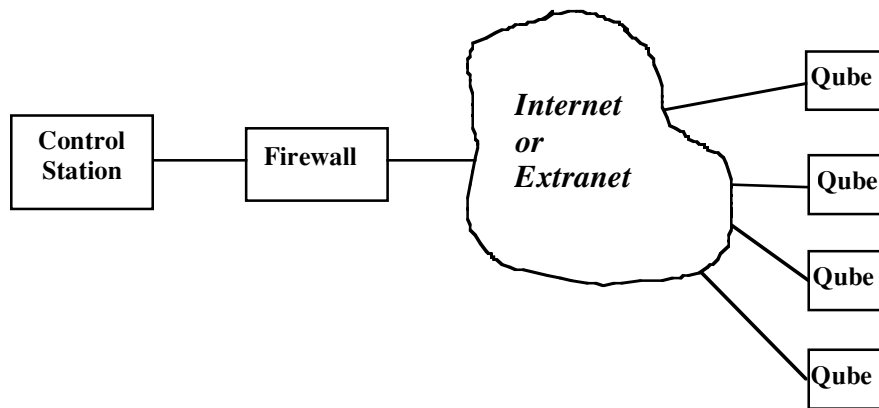
As well as these five rules, change the default Policy to “Deny”. See the section “Changing the default policy for a chain” in the user manual entitled *Administrator Manual*.

1. Rule 1
  - a. Destination Port Number(s). The low value is 1025; the high value is 65535.
  - b. Policy. Accept
2. Rule 2
  - a. Destination Port Number(s). The low value is 444; the high value is 444.
  - b. Policy. Accept
3. Rule 3
  - a. Destination Port Number(s). The low value is 80; the high value is 81.
  - b. Policy. Accept
4. Rule 4
  - a. Source IP Address (Low). 127.0.0.1.
  - b. Source IP Address (High). 127.0.0.1
  - c. Policy. Accept
5. Rule 5
  - a. Source IP Address (Low). Enter the IP address of the default gateway for the control station (see “System: Internet” in Chapter 2 of the *Administrator Manual*).
  - b. Source IP Address (High). Enter the IP address of the default gateway for the control station
  - c. Network Protocol. ICMP
  - d. Policy. Accept

Based on the ports used by the Control Station, there are several deployment scenarios. Several such scenarios are described below, along with the associated security risks and benefits. It is recommended that you make the Control Station as secure as possible for the particular deployment scenario.

## 1.2 Scenario #1 - Remote Management (for example, Sun Cobalt Qube™ appliances)

In this scenario, the Control Station is placed behind a firewall and then accesses the servers or is accessed by the servers across the Internet or an extranet.



In this configuration, the Control Station is used to manage the Sun Cobalt Qube™ appliances deployed throughout the Internet. An administrator can use the Control Station to install updates, patches and new software onto the Sun Cobalt Qube appliances. In general, BlueLinQ-enabled products (the Sun Cobalt Qube 3 appliance, Sun Cobalt RaQ™ XTR server appliance, Sun Cobalt RaQ 550 server appliance and future products) can use the Control Station as their BlueLinQ server and “pull” package files rather than having the Control Station “push” package files to them. This allows for patches and updates to be qualified at a central site before making them available to remote Sun Cobalt Qube appliances. The Sun Cobalt Qube appliances that pull package files through the BlueLinQ interface do not have to be managed by the Control Station. However, communication for BlueLinQ requests takes place on TCP port 80 so the firewall should allow HTTP requests through port 80.

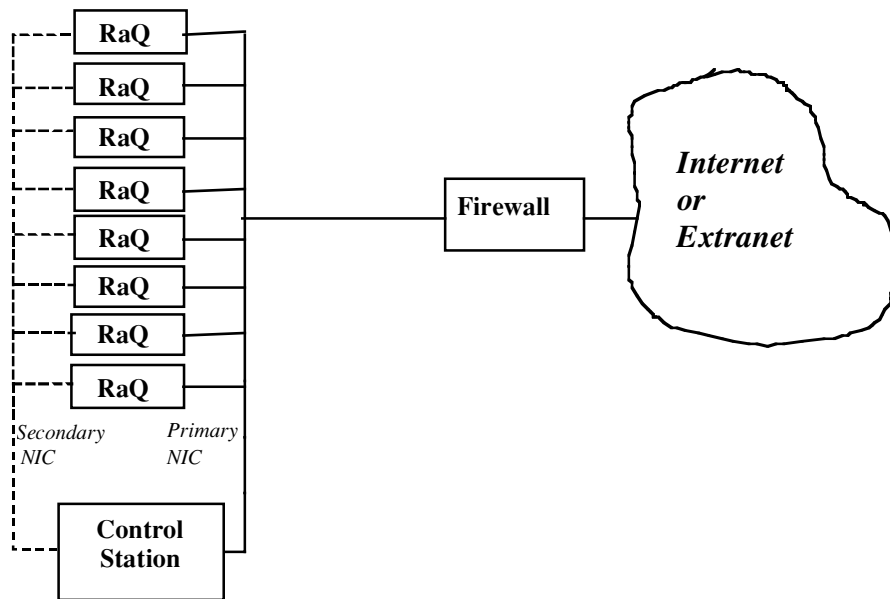
In the Remote Management scenario, the Control Station needs to be accessible via the Internet. The firewall is used to protect the Control Station and should be configured to allow only inbound connections to the Control Station on TCP port 80 (HTTP). The BlueLinQ server and the Health Monitor event collector both run on port 80 of the Control Station.

The Control Station requires outbound connectivity to TCP ports 80, 81, 444 and 27000. Ports 80, 81 and 444 are used by the Control Station to install the Control Station agent. Once the agent is installed, access to these ports is no longer required. Port 27000 is used by the Control Station to communicate with the agent.

**Note:** Access into the managed servers is both authenticated and encrypted. The applications on the Sun Cobalt Control Station DO NOT send user names or passwords across the network.

### 1.3 Scenario #2 - Data Center Management (for example, Sun Cobalt RaQ™ server appliances in a data center)

In the data center, the Control Station can be located behind a firewall close to the systems it manages. In this scenario, the Control Station can use the secondary NIC as the management interface while using the primary NIC to access the Internet. The Control Station can also be placed on the primary NIC as none of the module data travels past the firewall. This scenario is as shown below:



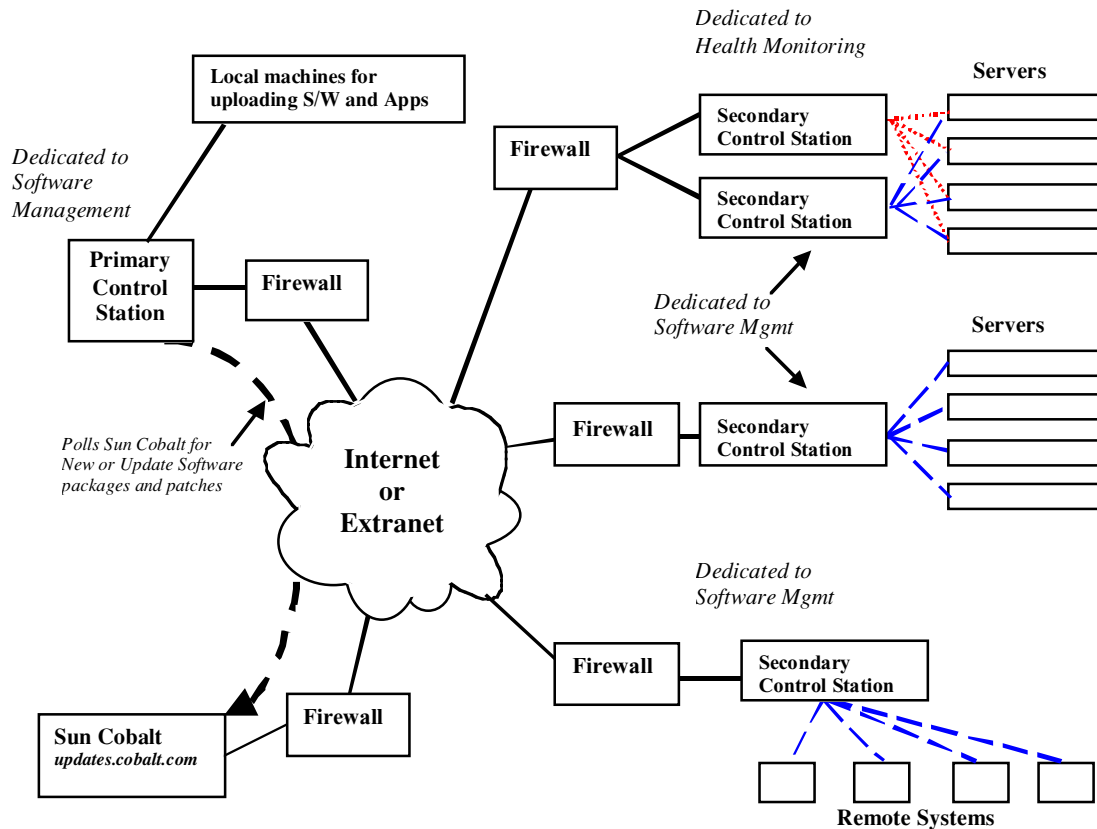
With the Control Station, you can provide health monitoring, inventory, performance and software management for the Sun Cobalt RaQ server appliances. The Control Station can be used to push updates and patches to the server appliances. For the Sun Cobalt RaQ XTR server appliance, the Sun Cobalt RaQ 550 server appliance and newer systems with a BlueLinQ client, the Control Station can be configured to act as a BlueLinQ server.

The Control Station should not be accessible from the Internet. TCP port 80 on the Control Station should be accessible on the management network for the BlueLinQ server and the Health Monitoring module to function properly.

The Control Station must be able to connect to TCP ports 80, 81, 444 and 27000 on the RaQs. Ports 80, 81 and 444 are used for installing the Control Station agent. Once the agent is installed, access to these ports is no longer required. Port 27000 is used by the Control Station to communicate with the agent. This port must be accessible on the management network only; access to port 27000 from the Internet should be filtered by the firewall.

## 1.4 Scenario #3 - Remote Distributed Data Center

In this scenario, multiple Control Stations are used to support different remote data centers or sites. The scenario is shown below.



In this configuration, a primary Control Station deployed at a central site is used for software distribution via BlueLinQ. The primary Control Station does not manage any Sun Cobalt RaQ server appliances or Sun Cobalt Qube appliances directly; the appliances are managed by the secondary Control Stations located in the remote data centers. The secondary Control Stations have managed and installed the agent on the servers they cover. The secondary Control Stations located in the remote data centers are configured to use the primary Control Station as their BlueLinQ server from which to obtain software patches and updates.

The primary Control Station is configured to use the “updates.cobalt.com” BlueLinQ server to get its updates and patches. The Firewall must therefore allow inbound and outbound HTTP connections on TCP port 80. When an update or patch is available on the “updates.cobalt.com” server, it can be downloaded to the primary Control Station and approved to be installed in the remote sites. When the update or patch is approved, it just has to be “published”, making it available to the secondary Control Stations. A secondary Control Station can now see the update or patch, and “publish” it for other BlueLinQ-enabled servers or install it on the servers it manages.

**Note:** The secondary Control Stations can be configured to query the “updates.cobalt.com” BlueLinQ server directly; this scenario, however, is intended to highlight how one primary Control Station can be used to control the distribution of software to the managed servers through one or more secondary Control Stations.



You can also create customized software packages and upload them to the primary Control Station from a local machine.

In this configuration, TCP port 80 on the primary Control Station should be accessible from the Internet. The secondary Control Station systems require an outbound Internet connection on TCP port 80 to contact the primary Control Station via the BlueLinQ protocol.

## 1.5 Other Security Notes

There are two other issues concerning security on the Sun Cobalt Control Station. These particular issues also pertain to all Sun Cobalt server appliances. Though the risk is minimal, they should be noted.

1. **Setup Wizard.** When the Setup Wizard is launched, the system prompts the user for a user name and password. When entered, this information is transferred in clear text to the server. Anyone “sniffing” the network could obtain the password for the user *admin*. It is recommended that you set up the Control Station initially on a secure network, preferably one not connected to the Internet.
2. **Initial Login.** When accessing the Sun Cobalt Control Station or any other Sun Cobalt product, initially for that session, the system prompts the user for the user name and password for the user *admin*. Again, this information is transferred in clear text to the server. Even if the “Security” check box is selected, the initial transfer of the user name and password occurs in clear text. After the initial login, all other traffic is encrypted. Again, anyone “sniffing” the network could obtain the password for the user *admin*.

## 1.6 Encryption and Authentication Technical Details

The Control Station uses an encrypted and authenticated channel to communicate with managed servers.

A connection from the Control Station to a managed server is authenticated using a scheme based on Diffie-Hellman Key Exchange (DH) and Fortified Key Negotiation (FKN). Cryptographically strong primes, between 1024 and 2048 bits, are used for DH key exchange. Keys, once generated, are stored for one hour.

Key validation and authentication is performed using FKN. SHA1 is used as the underlying hash function for FKN. Every time a new key is generated, authentication using FKN is performed. During the initial connection, the Control Station uses the *admin* or *root* password provided by the Control Station administrator as the password parameter to FKN. Subsequent connections use a randomly generated 160-bit password that is unique to each Control Station—managed server pair. This password is only used by the Control Station and cannot be used to log in to the server.

Once a connection has been authenticated, fresh encryption and message-authentication session keys are derived using AKEP2. Connections are then encrypted using ARC4. Messages are authenticated using HMAC. SHA1 is used as the underlying hash function for HMAC.

Diffie-Hellman Key Exchange, Fortified Key Negotitation, AKEP2, ARC4 HMAC and SHA1 are in the public domain. The implementations of DH, FKN, ARC4 and SHA1 used by the Control Station are derived from examples given in [1]. The implementation of AKEP2 is derived from [2]. The implementation of HMAC is derived from [3].

[1] *Applied Cryptography*, B. Schneier, John Wiley & Sons, 1996.

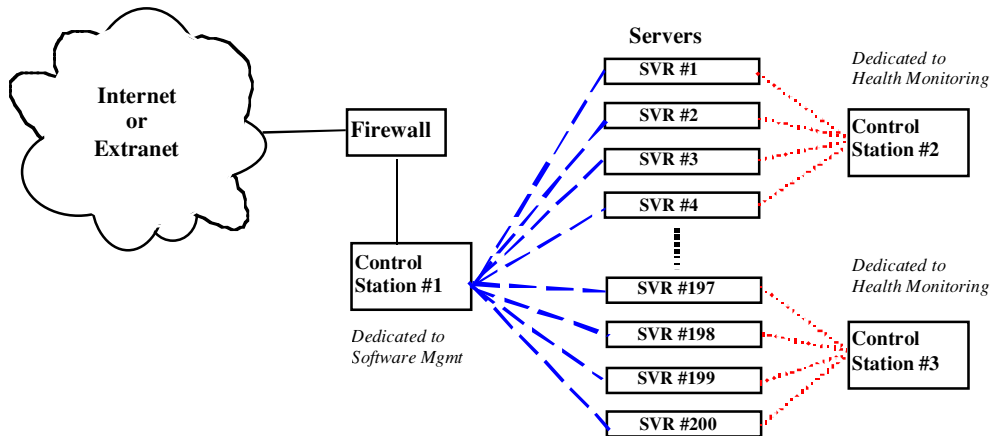
[2] *Entity Authentication and Key Distribution*, Mihir Bellare and Phillip Rogaway, CRYPTO 93, Lecture Notes in Computer Science Vol. 773, D. Stinson, Ed. Springer Verlag 1994.

[3] *HMAC: Keyed-Hashing for Message Authentication*, H. Krawczyk, M. Bellare, R. Canetti, RFC 2104, February 1997.

## 2. Scalability Scenarios

### 2.1 Scenario 1: Multiple Control Stations control a single server

The scalability of the Control Station is not defined in hardware but is more based on the deployment scenario chosen. The Control Station agent is designed to allow multiple Control Stations to manage a single server. With this capability, several Control Stations can be deployed to manage a large set of servers for different reasons. The scenario below illustrates the multiple Control Station deployment.



In this scenario, Control Station #1 performs only the Software Management function. It has an external connection to the Sun Cobalt BlueLinQ server and acts as a staging area for updates and patches. Control Station #1 manages all of the servers and can have its own server groups. For example, on Control Station #1, you can create groups for the different types of managed server, such as all Sun Cobalt Qube 3 appliances or all Sun Cobalt RaQ 4 server appliances. You may also want to group the server according to their physical locations, such as Building 21, Building 22 and so on.

As another option, you may want to dedicate a control station specifically to the Health Monitoring function. In this scenario, Control Station #2 monitors the managed servers 1 through 100, while Control Station #3 monitors servers 101 through 200.

**Note:** A server can be managed by more than one control station; in this case, only one agent is installed on the managed server. The agent keeps track of the IP addresses of the control stations that are managing the server.

This also allows you to have a backup control station in place, should the primary control station fail.

## 2.2 Scenario 2: A Control Station accesses different repositories for different types of package files

In your network, you may have specific BlueLinQ servers on which reside certain types of packages or files. For example, the Sustaining department might have their own server for software patches, the Professional Services department might have their own server for customized software, and so on. A Control Station dedicated to the Software Management function would poll each of these different BlueLinQ servers for new or updated package files.

In the following example, one Control Station performs only the Software Management function. It polls the Control Stations for the Sustaining, Development and Media Team BlueLinQ servers respectively for any software patches, new modules or applications, or content files.

