Intricloud Network Setup

Thank you for your purchase of Intricloud data protection solutions!

When deploying Intricloud's feature-rich management and automation solutions for offsite backup and disaster recovery, please ensure to complete the following configuration on your networking infrastructure prior to implementation.

Stratus Backup Cloud

Stratus LAN/Network Communications

The following port(s) are required in order to back up roaming PCs and remote offices outside your network for each Stratus Appliance. These ports should not be open to public access:

Direction	Port	Protocol	Purpose
Inbound	995	TCP	Ensures secure Stratus communications for monitoring, alerts and updates.
Inbound	873	TCP	Provides global synchronization of files.

Nimbus Disaster Recovery Cloud

Nimbus LAN/Network Communications

The following port(s) are required for administrative access to the portal on each Nimbus High Availability Appliance and for alerts, updates, and licensing. These ports should not be open to public access:

Direction	Port	Protocol	Purpose
LAN-only Inbound	80 & 443	TCP	Nimbus Portal access. Needed internally on private network LAN only. No Internet access recommended.
Inbound	443	TCP	https from Nimbus HA Appliance IP needed to the Internet for licensing and alerts
Outbound	443	HTTPS	Access for alerts (httpsalerts.onqcentral.com), updates and licensing (updates.onQcentral.com).

Inbound & Outbound	123	UDP	Communication with NTP (ntp.org).

Nimbus High Availability to Protected Node Communications

Generally, HA-to-PN communications are over a LAN that is not secured. In the event that there are any filtering devices between the PN and the HA Appliance, the following ports need to be accessible on the PN:

Direction	Port	Protocol	Purpose
Outbound	3000	TCP	Allows squirtcopy communications
Inbound	5000	TCP	For FLR processing, allows WVhds for Windows and Netcat for Linux to receive data from Nimbus Manager
Inbound	5990	TCP	Allows DCRM to accept connections from Nimbus Manager
Inbound	5990	UDP	Allows LAMD to communicate with Nimbus Manager
Inbound	5991	UDP	Allows LAMD to monitor the PN
Inbound	5992	UDP	Allows LAMD to send PN heartbeat

High Availability Appliance to Disaster Recovery Communications

The following ports must be accessible between the HA Appliance and the DR Appliance pairs across WAN or LAN:

Direction	Port	Protocol	Purpose
Inbound & Outbound	22	TCP	Allows secure TCP connections between Nimbus Appliances. May be remapped.
Inbound & Outbound	81	TCP	Allows inter-appliance link monitoring. May be remapped.

WAN-DR Site Communications

The following ports must be accessible or inaccessible between your WAN and DR site:

Direction	Port	Protocol	Purpose
Inbound & Outbound	22	TCP	<DR IP> to <HA IP>
Inbound & Outbound	81	TCP	<DR IP> to <HA IP>
Inbound	80	TCP	Deny ANY PUBLIC / External / Internet to <DR IP> (HTTP protocol)

Inbound	443	TCP	(https) Allow <DR IP> outbound to Public / External / Internet
Outbound	443	SSL, SMTP, & SSH, TCP	Access for alerts (alerts.onqcentral.com), updates (updates.onqcentral.com), and licensing (lic.onqcentral.com).

Glossary of Terms

HA = High Availability, is the Nimbus appliance residing locally at client.
DR = Disaster Recovery, is the recovery site hosted on Intricloud's infrastructure.
PN = Protected Node, identifies each server or workstation being protected.
Portal = Web-based console for managing Intricloud solutions.
DCRM = Distributed Computing Resource Management, originally developed for military applications the DCRM platform is the engine inside Nimbus for monitoring and managing both virtual and physical computing resources.

