Kofax eCopy ShareScan
6.2
High Availability and Load Balancing Deployment Guide

KOFAX

Licensing, Copyright, and Trademark Information

1 - Introduction

This document describes how to deploy eCopy ShareScan to achieve High Availability and / or Load Balancing and details its advantages.

To get information about how to set up a Load Balanced cluster, refer to the relevant Microsoft Knowledge Base articles:

– When using Microsoft Network Load Balancer: (http://technet.microsoft.com/en-us/library/cc739506(v=ws.10).aspx)

– When using a hardware load balancer or other solution hosted in a server other than the ShareScan servers: Installation and configuration guide of your hardware load balancer and the ShareScan Reference Setup Guide respective to the hardware load balancer.

Important!
Different network appliances offering load balancer features have plenty of modes and options to configure, also affected by the circumstances and policies of the hosting IT infrastructure. To find a way for enabling the installation of ShareScan behind a (hardware) load balancer, we provide compatibility testing of ShareScan in a certain configuration, enabling proper ShareScan operation. Obviously, this testing / compatibility declaration does not cover all the modes and features of the load balancer (network appliance), but until the necessary requirements are met, an expert administrator of the given network appliance will most probably also be able to configure the system in other / extended ways.

The basic feature / mode ShareScan requires from a load balancer:

– TCP requests (including HTTPS request) reaching the ShareScan server nodes behind the load balancer MUST preserve the source IP address of the client initiating the request.

– TCP connections must be persisted in a client IP basis.

Please check the support portal for the latest set of Reference Setup Guide documents available for supported / recommended load balancers.

About eCopy ShareScan 6.2

eCopy ShareScan 6.2 is an MFP document capture solution that enables MFP users to engage their business systems and processes by completely automating document capture processes. As a result, eCopy ShareScan simplifies MFP capture workflows and enables users with advanced imaging capabilities.

The eCopy ShareScan software extends the capabilities of digital copiers and scanners. When installing and setting up a ShareScan system, you must be familiar with the scanning devices that you will use with ShareScan, the ShareScan software components, and the basic installation and configuration workflow.

This document is written on the assumption that readers are familiar with working in a server-client architecture and environment.

If you are about to **install or upgrade to ShareScan 6.2** , consult the **eCopy ShareScan 6.2 Installation Guide**..

High availability deployments

eCopy ShareScan 5.2 SP2 introduced high availability and better scalability features. Since v5.2 SP2, eCopy ShareScan can be deployed in a Microsoft Network Load Balancing Cluster (abbr. as **MSNLB Cluster** throughout this document) solution in such a way that it provides:

– high availability

– Central device management to simplify working with a sizeable fleet of MFPs

For ShareScan 6.2, compatibility testing for certain hardware load balancer solutions were performed. For the list of these third party load balancer systems /appliances, consult the ShareScan support portal.

Load balancing across multiple ShareScan servers

Multiple ShareScan 6.2 servers with a common database and a shared work folder can be configured (as part of a NLB Cluster or without it) to provide load balancing features, regarding the document building and OCR phases of the workflow.

This guide is intended for system administrators who are responsible for carrying out such a deployment. On ShareScan (pre-) installation requirements, MFP model specific guidance, installation procedure and configuration help, see the relevant items in product documentation.

2 - Cluster and Host Topology

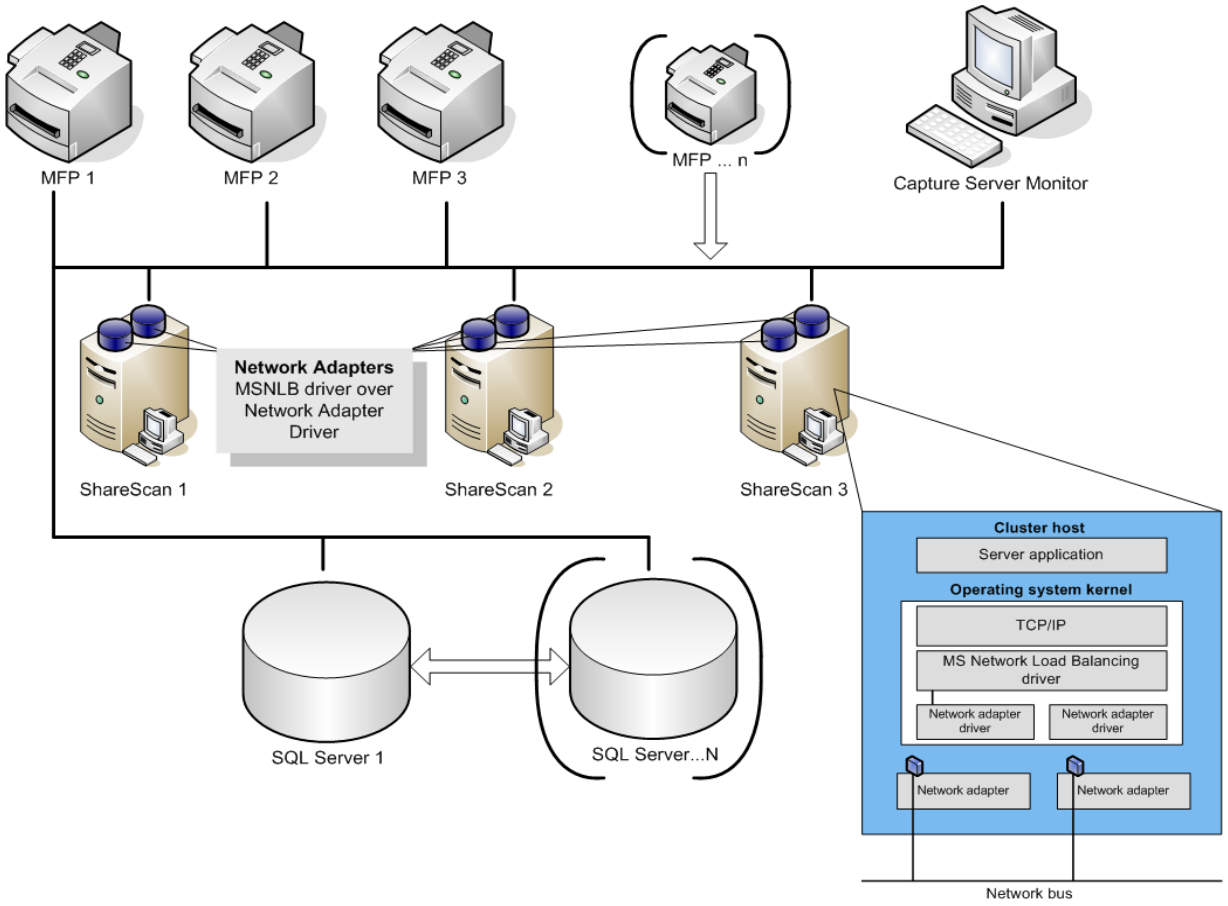


Figure 1: System diagram with MS NLB

The same figure properly depicts the different supported scenarios from the point of view of high availability and load balancing, because the server / network topology is the same, but different configuration settings are applied to achieve the desired behavior.

If a hardware load balancer is used instead of MS NLB, the system diagram changes as shown below:

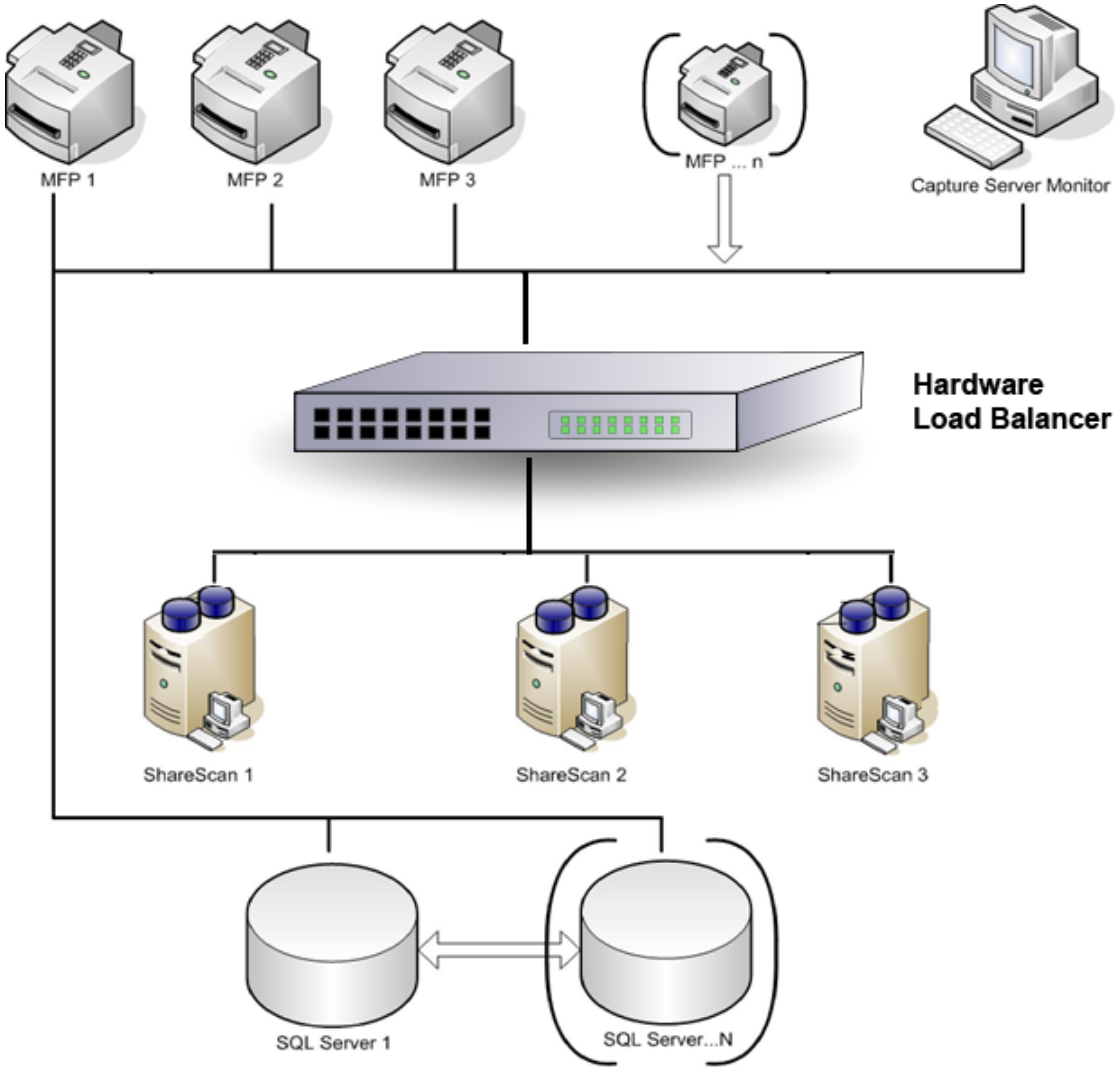


Figure 2: System diagram with a hardware load balancer

The SQL Server Cluster (SQL Server 1, SQL Server N) is visible to the ShareScan servers as a single SQL Server. See the Microsoft SQL Server documentation for details.

1. **High availability is enabled via a network load balancing cluster**
   In this case, servers ShareScan 1...N (node) form a network load balancing cluster.

This basically means that the cluster is seen by the devices behind the same cluster IP address (in terminology of different vendors it is often referred as Virtual IP) and the ShareScan configuration database contains only a single ShareScan Manager entry - all the ShareScan Managers (1...N) use the same configuration data.

When an MFP is added to the system, its configuration points to the common cluster IP address; when the ShareScan application is started on the MFP, the requests are sent to the cluster IP address.

With the proper configuration option used (in MS NLB it is called single node affinity mode) for the particular communication ports, NLB Cluster makes a static assignment between the MFP and one of the ShareScan servers (1..N), based on its internal algorithm, aiming to evenly distribute the devices across the nodes.

This assignment is in effect until a node is taken away from the cluster or a node is added (back) to the cluster.

A node is taken away, for example, when the load balancer or the Capture Server Monitor detects that the OS, the network or ShareScan is non-functional on a particular node.

Also, this setup enables simplified management of a bigger fleet of MFP devices: since the cluster is stored as a single Manager in the ShareScan database, all the devices connected to the multi-manager cluster can be managed in a single Administration Console.

2. **ShareScan Document creator and OCR Load Balancing**
   This feature ensures that the document creation and OCR processes are executed on multiple servers, distributing the jobs across all the available ShareScan Manager PCs. This happens via using a common job queue and a shared work folder. This feature can be enabled in any case when multiple Managers are connecting to the same SQL Server Database.

   Whenever a workflow execution reaches the point when the final document (PDF, DOC, DOCX etc.) is to be produced, data describing the document (source file paths, metadata, document format, etc.) are put into a job queue, stored in the database, and a notification is sent to the Managers in the system. One of the Managers with a free document creator fetches a job from the database job queue, processes it and then it sends a notification to the originator about the job completion.

   Note:
   The Shared Output Creator does not work in a Workgroup environment. This scenario is not supported due to the limitations of the Windows operating system when used in a workgroup.

3. **Both #1 and #2 are enabled**
   This setup is able to provide high availability and optimal resource usage at the same time.

Reference setup of Citrix Netscaler 10.5 with Policy Based routing

High availability mode setup was introduced with ShareScan 5.2 SP2. The only QA certified setup of that version was based on Microsoft Network Load Balancer.

With ShareScan 5.4 SP2 a compatibility testing was performed with other load balancer products, like Citrix Netscaler 10.5.

Different network appliances offering load balancer features have plenty of configurable modes and options, also affected by the circumstances and policies of the hosting IT infrastructure. To find a way to enable installation of ShareScan behind a (hardware) load balancer, we provide compatibility testing of ShareScan in a certain configuration, enabling correct ShareScan operation. This testing / compatibility declaration will not cover all the modes and features of the load balancer (network appliance), but until the necessary requirements are fulfilled, an expert administrator of the given network appliance will most probably be also able to configure the system in other / extended ways.

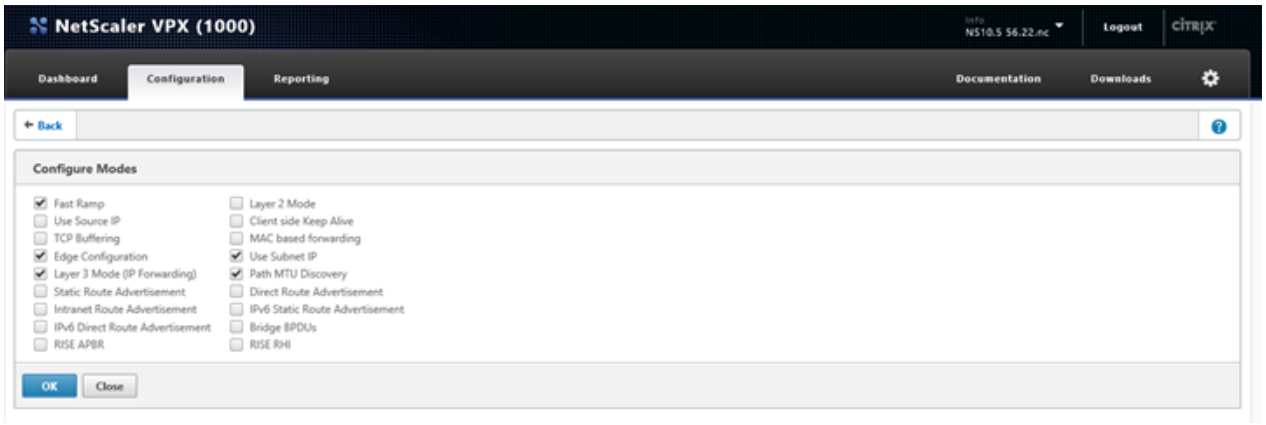
The basic feature / mode ShareScan requires from a load balancer:

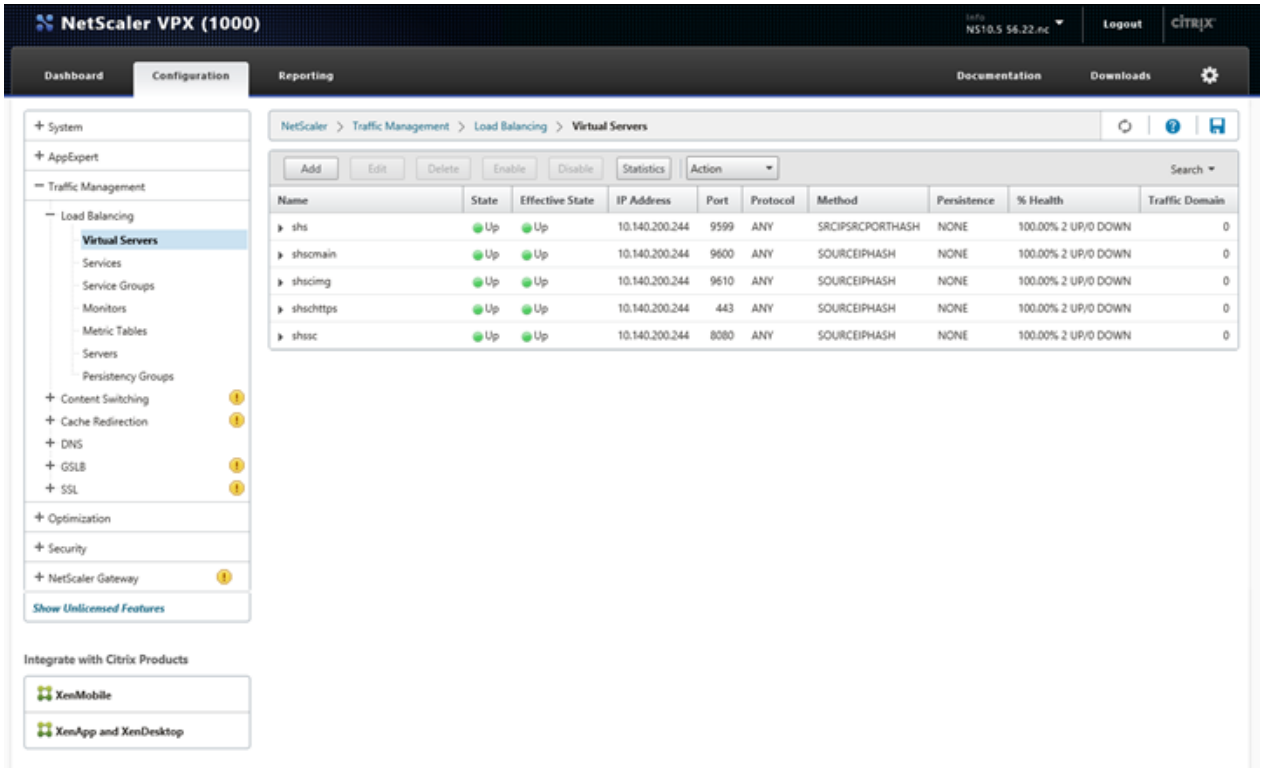
– TCP requests (including HTTPS request) reaching the ShareScan server nodes behind the load balancer MUST preserve the source IP address of the client initiating the request.

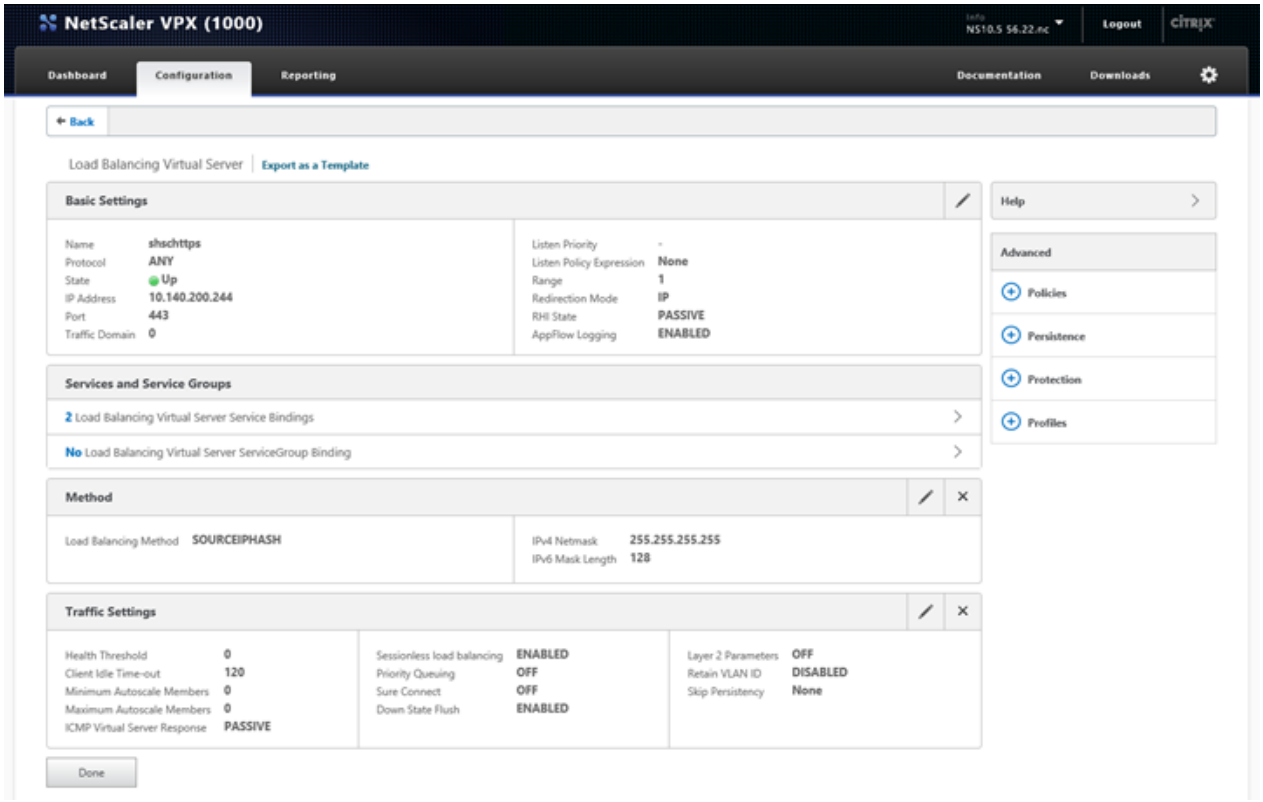
– TCP connections must be persisted on a client IP basis. (This means that until the number of ShareScan server nodes is the same, TCP connections from a given client should go to a certain ShareScan server node – this method is called SOURCEIPHASH in the Netscaler terminology.) It is NOT a requirement that the “Persistence” feature of NetScaler or any other load balancer should be used.

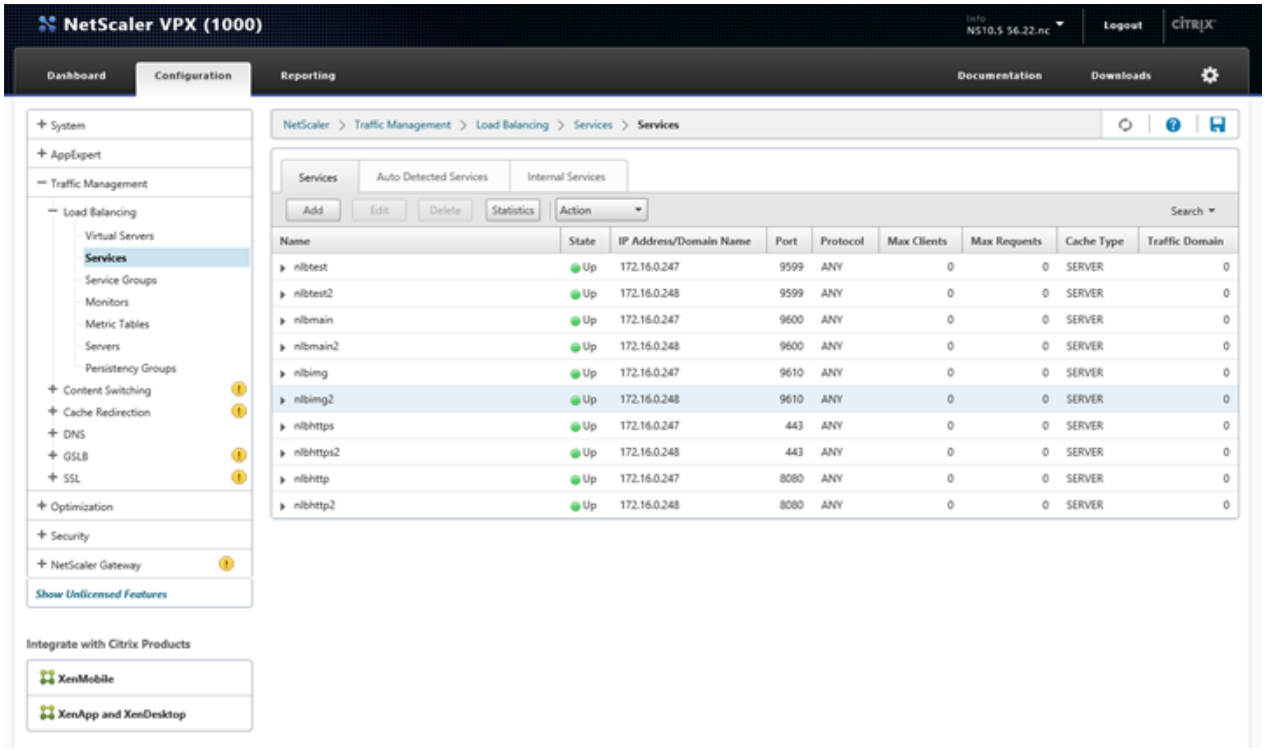
The following screenshots indicate the settings used in the reference environment:

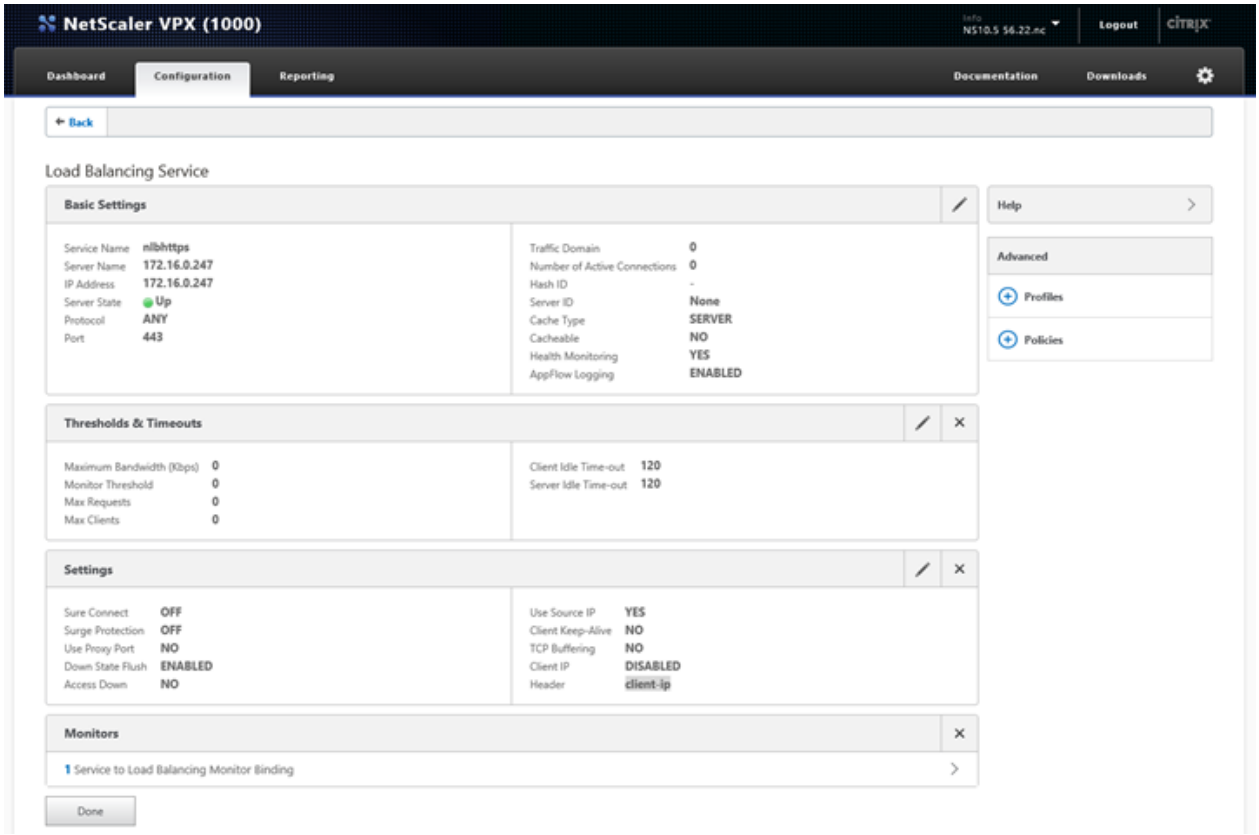
(The below settings are about the service called ‘shschttps’ on port 443, and this is basically enough to be used for a web based – like HP - device when the secure communication is enabled, but basically the other services on other ports have the same settings.) For the complete port list necessary to configure for a particular device vendor, consult eCopy ShareScan 6.2 High Availability and Load Balancing Deployment Guide (this document).

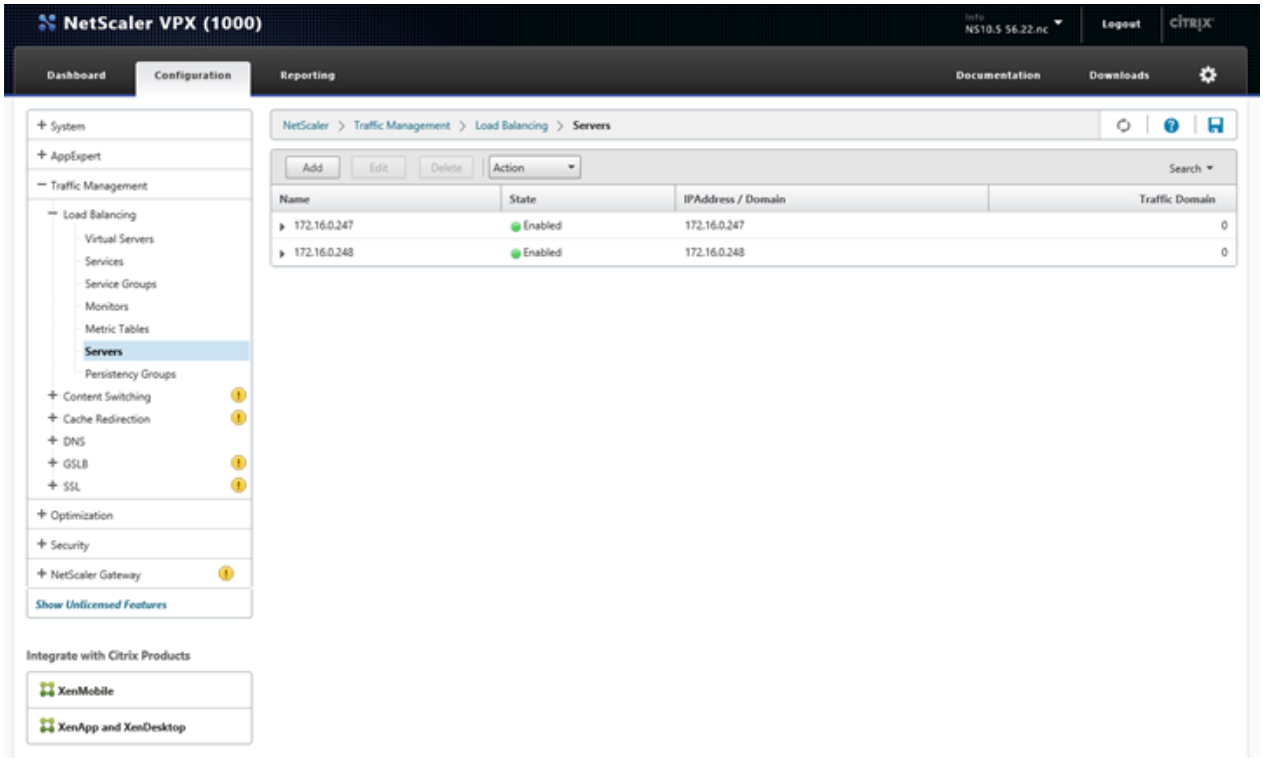


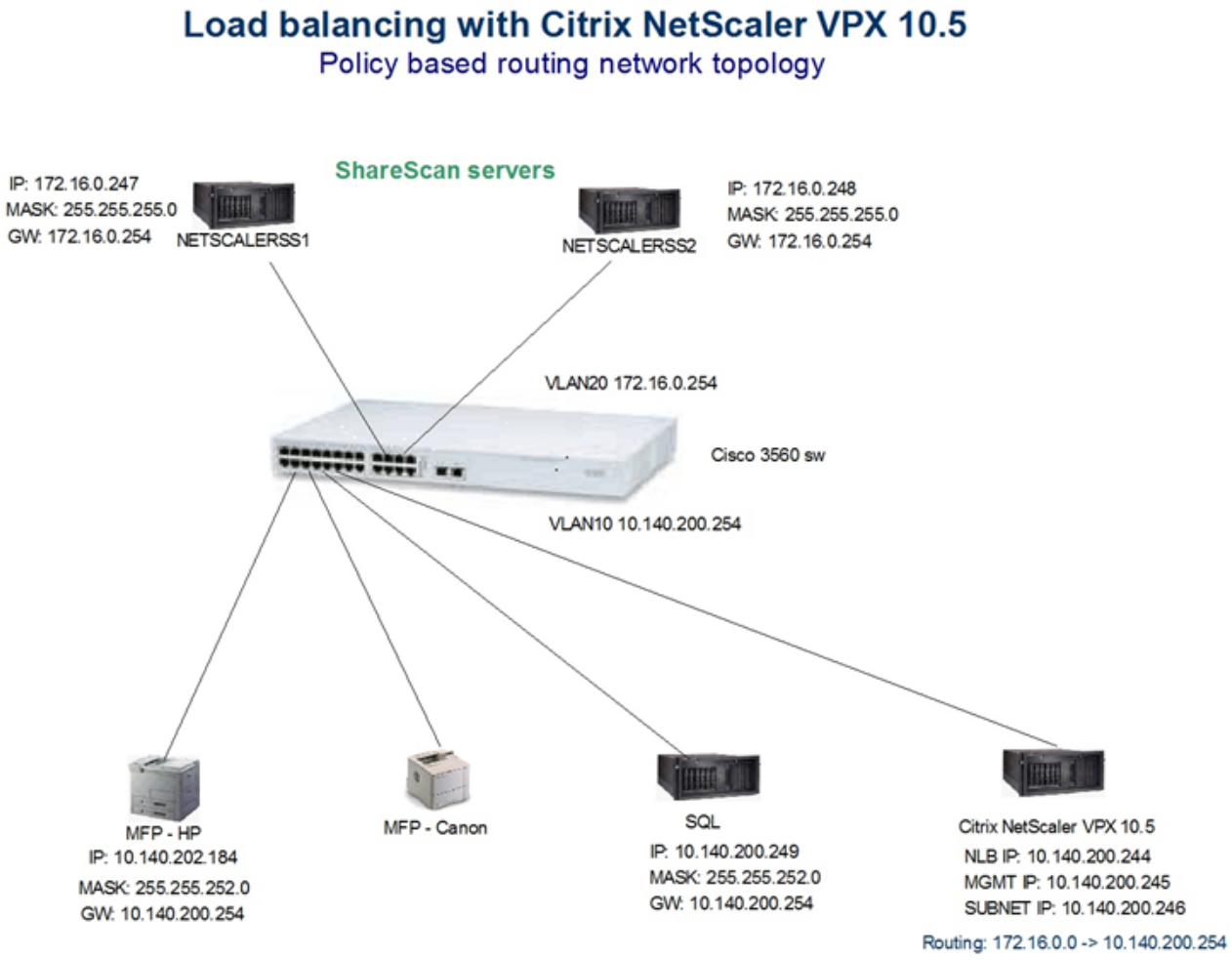

NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Content Switching
Cache Redirection
DNS
GSLB
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
Integrate with Citrix Products
XenMobile
XenApp and XenDesktop
NetScaler > Traffic Management > Load Balancing > Virtual Servers
Add
Edit
Delete
Enable
Disable
Statistics
Action
Search
Name
State
Effective State
IP Address
Port
Protocol
Method
Persistence
% Health
Traffic Domain
shs Up Up 10.140.200.244 9599 ANY SRCIPSRCPORTHASH NONE 100.00% 2 UP/0 DOWN 0
shscmain Up Up 10.140.200.244 9600 ANY SOURCEIPHASH NONE 100.00% 2 UP/0 DOWN 0
shscimg Up Up 10.140.200.244 9610 ANY SOURCEIPHASH NONE 100.00% 2 UP/0 DOWN 0
shschttps Up Up 10.140.200.244 443 ANY SOURCEIPHASH NONE 100.00% 2 UP/0 DOWN 0
shssc Up Up 10.140.200.244 8080 ANY SOURCEIPHASH NONE 100.00% 2 UP/0 DOWN 0


NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Back
Load Balancing Virtual Server
Export as a Template
Basic Settings
Name shschttps
Protocol ANY
State Up
IP Address 10.140.200.244
Port 443
Traffic Domain 0
Listen Priority -
Listen Policy Expression None
Range 1
Redirection Mode IP
RHI State PASSIVE
AppFlow Logging ENABLED
Help
Advanced
Policies
Persistence
Protection
Profiles
Services and Service Groups
2 Load Balancing Virtual Server Service Bindings
No Load Balancing Virtual Server ServiceGroup Binding
Method
Load Balancing Method SOURCEIPHASH
IPv4 Netmask 255.255.255.255
IPv6 Mask Length 128
Traffic Settings
Health Threshold 0
Client Idle Time-out 120
Minimum Autoscale Members 0
Maximum Autoscale Members 0
ICMP Virtual Server Response PASSIVE
Sessionless load balancing ENABLED
Priority Queuing OFF
Sure Connect OFF
Down State Flush ENABLED
Layer 2 Parameters OFF
Retain VLAN ID DISABLED
Skip Persistency None
Done


NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Content Switching
Cache Redirection
DNS
GSLB
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
Integrate with Citrix Products
XenMobile
XenApp and XenDesktop
NetScaler > Traffic Management > Load Balancing > Services > Services
Services
Auto Detected Services
Internal Services
Add
Edit
Delete
Statistics
Action
Search
Name
State
IP Address/Domain Name
Port
Protocol
Max Clients
Max Requests
Cache Type
Traffic Domain
nlbtest Up 172.16.0.247 9599 ANY 0 0 SERVER 0
nlbtest2 Up 172.16.0.248 9599 ANY 0 0 SERVER 0
nlbmain Up 172.16.0.247 9600 ANY 0 0 SERVER 0
nlbmain2 Up 172.16.0.248 9600 ANY 0 0 SERVER 0
nlbimg Up 172.16.0.247 9610 ANY 0 0 SERVER 0
nlbimg2 Up 172.16.0.248 9610 ANY 0 0 SERVER 0
nlbhttps Up 172.16.0.247 443 ANY 0 0 SERVER 0
nlbhttps2 Up 172.16.0.248 443 ANY 0 0 SERVER 0
nlbhttp Up 172.16.0.247 8080 ANY 0 0 SERVER 0
nlbhttp2 Up 172.16.0.248 8080 ANY 0 0 SERVER 0


NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Back
Load Balancing Service
Basic Settings
Service Name nlbhttps
Server Name 172.16.0.247
IP Address 172.16.0.247
Server State Up
Protocol ANY
Port 443
Traffic Domain 0
Number of Active Connections 0
Hash ID -
Server ID None
Cache Type SERVER
Cacheable NO
Health Monitoring YES
AppFlow Logging ENABLED
Help
Advanced
Profiles
Policies
Thresholds & Timeouts
Maximum Bandwidth (Kbps) 0
Monitor Threshold 0
Max Requests 0
Max Clients 0
Client Idle Time-out 120
Server Idle Time-out 120
Settings
Sure Connect OFF
Surge Protection OFF
Use Proxy Port NO
Down State Flush ENABLED
Access Down NO
Use Source IP YES
Client Keep-Alive NO
TCP Buffering NO
Client IP DISABLED
Header client-ip
Monitors
1 Service to Load Balancing Monitor Binding
Done


NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
System
AppExpert
Traffic Management
Load Balancing
Virtual Servers
Services
Service Groups
Monitors
Metric Tables
Servers
Persistency Groups
Content Switching
Cache Redirection
DNS
GSLB
SSL
Optimization
Security
NetScaler Gateway
Show Unlicensed Features
Integrate with Citrix Products
XenMobile
XenApp and XenDesktop
NetScaler > Traffic Management > Load Balancing > Servers
Add
Edit
Delete
Action
Search
Name
State
IPAddress / Domain
Traffic Domain
172.16.0.247
Enabled
172.16.0.247
0
172.16.0.248
Enabled
172.16.0.248
0



Failure Trigger Events

Detecting failures

MS NLB detects the hardware, OS and network level issues basically by sending and checking internal network messages to the cluster nodes (so-called heartbeat messages). In case of not receiving the proper messages, it brings the failing node offline. (Stopped state)

Hardware load balancer systems are able to detect the network issues and often able to perform basic level check like opening a port on the monitored server, or sending a test request and check the response and the like.

The Capture Server Monitor (if installed), performs a basic level functional check of the ShareScan Manager Service, by executing simple simulated scanning and document creation workflow and storing the result document in a local folder.

It is not able to detect any issues with:

– Session Logon Service (e.g. domain controlled or AD problem)

– Cost Recovery or ID services

– Any issues with connecting backend systems (e.g. a document management backend or Exchange server being down)

System Failure Operation

When the system fails on a node, another node takes over its role. The failed node does not automatically return to the cluster, but the administrator must manually set it back online in the administrative tool of the network load balancer.

Detection of the failure can happen by:

– the network load balancer system itself (network errors, in case of MS NLB, sever OS level errors)

– if the load balancer has some monitoring features, it can detect if a service behind a port is not responding properly

– CSM, it is able to perform basic level ShareScan functional test: if ShareScan services are not responding in a timely manner or errors are detected, this triggers the failure event.

Failure Symptoms

Failure symptoms on the device connected to a server that has a problem include:

– stopped scanning

– device screen refreshed to Main screen

– device screen refreshed to the Session Logon Screen (if SSO is enabled)

– displaying ShareScan error messages

– displaying a Connection Error or Communication Error screen

Any error messages that appear need to be acknowledged by clicking the **Connect** button, which causes a device to reconnect to a properly working server node.

Successful reconnection can be completed if the failing node is detected and brought offline by the Capture Server Monitor (if installed) or by the network load balancer.

This detection process may take some time (from 10 seconds to several minutes), so repeated click on the **Connect** button may be necessary.

Occasionally, all data processed on the particular server regarding the currently processed job may be lost, depending on workflow phase where the failure happened.

If Cost Recovery or ID Services integration is also in place, a system failure may trigger an automatic logoff and a repeated login process and workflow restart may be necessary.

Functional Advantages

– even distribution of the MFP devices across multiple managers, providing static load balancing

– single Administration Console to manage the whole fleet connected to the cluster, no need to maintain several Managers separately

– Capture Server Monitor installation and configuration inside / outside the cluster

– convergence time insured by NLB driver to complete ongoing jobs

Configuration Checklist

The following high availability function requirements must be fulfilled for proper operation:

1. installed and configured NLB Cluster
2. installed and configured ShareScan in cluster mode
3. **RECOMMENDED**: installed and configured Capture Server Monitor to ensure that the whole ShareScan server is verified periodically; at least one CSM Agent outside the cluster.

Note:
The high availability behavior of the cluster remains available even without the ShareScan Capture Server Monitor, as the OS, hardware and network related issues trigger a failure event without it.

System Requirements

– at least two server machines with supported server operating systems (same version on all nodes) with MSNLB Cluster support

Important!
High availability functionalities do not work if the server operating systems are hosted in VMware Workstation.

– When MS NLB is used
  – Two Network Interface Cards - unicast/multicast mode (multicast is the preferred protocol); **single NIC is not supported**

  – IPv4 is supported only (IPv6 is recommended to be disabled on all network adapters used for the cluster) QoS is recommended to be disabled on all network adapters used for the cluster purposes

  – MSNLB Cluster driver must be installed overthe network adapter driver (i.e.: the MSNLB Cluster feature must be enabled in the Windows Server OS)

– MSNLB Cluster can be configured by Network Load Balancing Manager tool that is part of the Windows server OS

– When the Capture Server Monitor is installed onto a cluster node, additional static IP addresses will be necessary on the NIC used for non-cluster purposes (2nd NIC). For details, see the **Capture Server Monitor Configuration Guide**

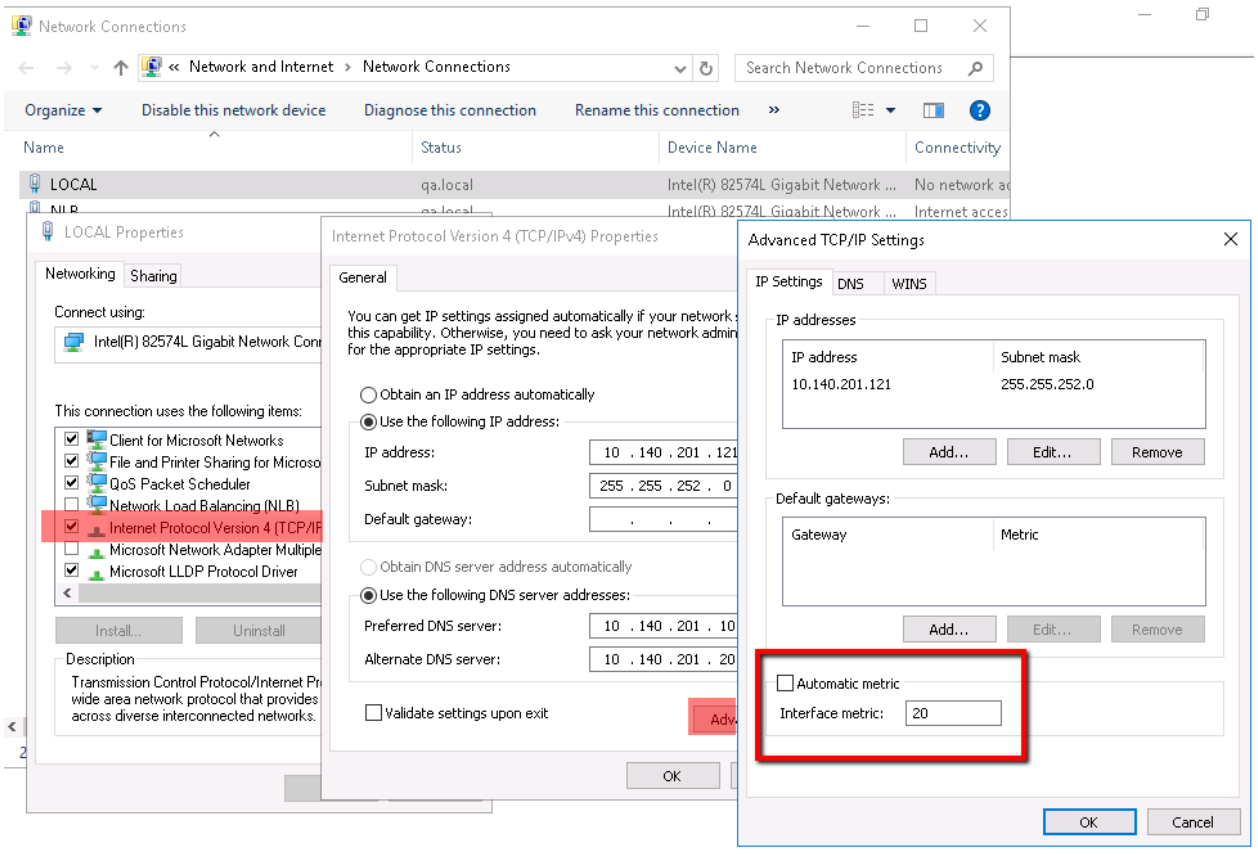
– after the MSNLB Cluster setup is ready, the IP / name of the cluster shall be added to the DNS as well

– having a proper DNS entry for the fixed IPs of the nodes used on the NIC which is used for the cluster.

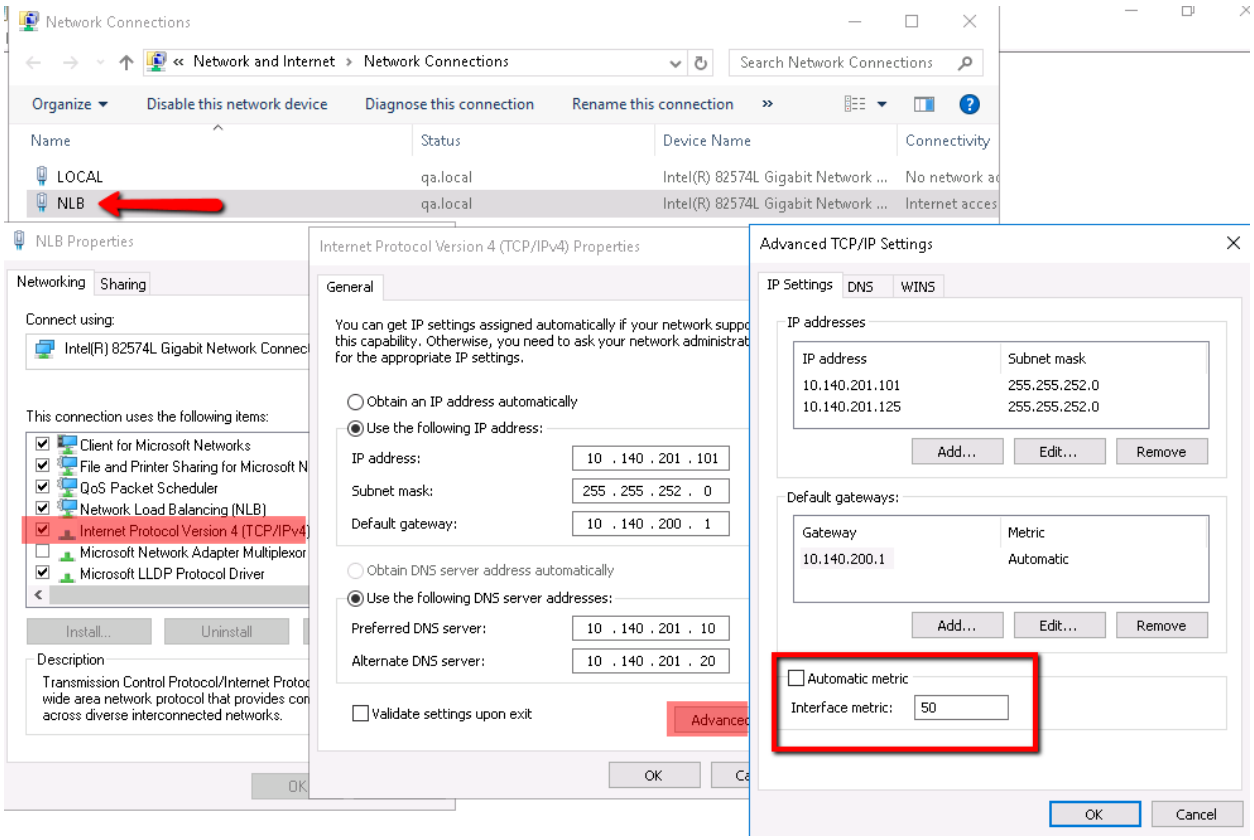
Consult with the ShareScan Reference Setup guide for the hardware load balancer.

The following interface metric values must be specified in Microsoft Windows 2016 NLB and Microsoft Windows 2012 NLB server environments:

NON-NLB – 'LOCAL' connection: Interface metric=20



NLB – 'LOCAL' connection: Interface metric=50



Note:
Changing MSNLB Cluster properties may cause unexpected results and full system unavailability. In case of any change, make sure the new settings are supported, and in case of unexpected behavior the original values can be reset. Some of the cluster setting changes may take effect only after some minutes of delay.

Note:
Make sure you add the cluster IP / name to the DNS **after** the cluster configuration, as it may cause issues in the process. Registering the cluster by its name to DNS is optional, because ShareScan uses only the IP address of the cluster.

ShareScan Requirements

– ShareScan 6.2 (or higher), same version on all nodes

– centralized common SQL database residing on a server which is not functioning as a ShareScan Manager node in the cluster. For information on supported SQL database versions, see the ShareScan 6.2 Compatibility Matrix.

Note:
It is recommended to have a SQL cluster instead of a single SQL server, as a single SQL server would be a single point of failure. For full system high availability, a SQL cluster is required (but it is not enforced by ShareScan; for testing purposes a single SQL server is appropriate). ShareScan is able to support MS SQL clusters, with no limitation (any number of nodes).

Note:
Parallel editing of Administration Console data from several Manager PC-s connecting to the same database is not recommended. Since all the configuration settings are stored for the 'virtual server' represented by the cluster IP (and cluster host name) all the Administration Consoles (on the disctinct server nodes) manage the same settings. Therefore there is no point to manage the settings from multiple Administration Consoles.

Capture Server Monitor Requirements

For details, see the **Capture Server Monitor Configuration Guide**.

Network Environment Recommendations (in case of MS NLB)

The network switch the cluster nodes directly connect to should be able to handle the amount of network traffic caused by the image transfer between the MFPs and the cluster nodes.

If the number of cluster nodes is higher and the MFPs are used intensively (concurrently), a proper network system design is recommended to avoid packet flooding (or switch flooding). Depending on the selected NLB setup, packet flooding can be avoided by:

– adding a network hub between the switch port and the NLB server nodes (when Unicast mode is used)

– in case of Multicast (preferred), different network devices / vendors have specific recommendations to configure their devices properly for this type of usage.

In any case, consult the network switch documentation and the vendor’s recommendations for the Microsoft NLB setups.

Note:
On the actual switch it may be necessary to enable Multicast mode. Consult your network device documentation and involve the network administrator of your system in the planning of the cluster deployment.

Note:
High Availability for Fuji-Xerox devices is only supported with Unicast enabled.

General Recommendations to Support High Availability

– For high availability implementation, a fully set up and configured MS SQL cluster environment is recommended

– In Windows Service Control Manager, you can enable different actions for the ShareScan Manager and ShareScan Agent service. (On the **Recovery** tab of the dialog opening when you right-click the) While unexpected service stoppage is not a probable scenario, it is recommended to enable the automatic service restart in case of a failure with a 1 minute delay since the services are highly fault-tolerant

– In concordance with your system policy, you may decide also to use the **Run a program** option of the **Recovery** tab (e.g. to send a notification email or to perform other action)

High Availability Prerequisites (in case of MS NLB)

Multicast UDP traffic must be enabled / supported on the subnet to which the non-cluster enabled network adapter (NIC) connects (UDP port 9650).

It is required to provide a notification mechanism between the cluster nodes.

Benefits of an eCopy ShareScan High Availability Deployment

Deploying eCopy ShareScan with a high availability has a number of advantageous functions:

– In case of failure, no immediate manual intervention is needed; failing servers are automatically put offline

– With the CSM installed:

- automatic notification of server failure

- possibility of integration with system management software (via action command scripts) features become available as well.

Note:
The high availability setup in a NLB environment does not ensure that the jobs being processed at the time of the failure will be recovered and finished after the successful failover. However, scanned files are preserved for these incomplete jobs to prevent data loss, and can be accessed via the Job Monitor web application.

3 - Deployment Overview

MFP Fleet

Before you start, ensure that MFP devices in your fleet are supported by eCopy ShareScan 6.2.

Ensure that your MFP fleet is ready for an eCopy ShareScan 6.2 deployment - determine what device vendors are represented in your fleet and consult the corresponding vendor-specific **eCopy ShareScan 6.2 Pre-Installation Checklist and Sizing Guide (s)**. Depending on your model(s), a **Device Configuration Guide** may also be available to help you prepare your MFPs for working with eCopy ShareScan. Feel free to consult these as well.

Note:
Only the necessary ports used by the MFP devices are to be open as clustered ports. See section 9.4 (Port Rules) of Appendix A for details.

Server Setup

MSNLB Cluster Setup for High Availability

1. Ensure that you have the eCopy ShareScan 6.2 installer ready with the proper licenses.
2. Have at least two *physically different* computers ready for a ShareScan 6.2 installation in a standard MSNLB Cluster environment with unique, fixed IP addresses. These machines (your dedicated ShareScan Manager PCs) must meet the following requirements:

   - ShareScan deployment / system requirements, since they make up the nodes in your cluster,

   - MSNLB Cluster PC requirements (http://technet.microsoft.com/en-us/library/hh831698.aspx)

   Note:
   For more information on clusters, see the relevant Microsoft resources and guidance: http://technet.microsoft.com/en-us/library/cc770558.aspx. For information on ShareScan system requirements, see either the vendor specific **eCopy ShareScan 6.2 Pre-Installation Checklist and Sizing Guide** or the **eCopy ShareScan 6.2 Installation Guide**.

Important!
A new registry setting HASecureDeviceCommunicationIP is introduced. It should be created manually and configured on all NLB nodes.

– Type: REG_SZ

– Default value: ''

– Hive: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan\ShareScanManager

– Description: If this value is defined, then the manager will be listening on this IP address in case the ClusterName is defined in the NLB environment.

Note:
If the virtual server nodes of the cluster reside on the same physical host (VMWare or Hyper-V) the setup is possible and the system will be operational. However, in case of a hardware failure it may happen that all nodes hosted on the same hardware stop, resulting in an inoperable system. For that reason it is recommended to have nodes at least on two physical hardware.

3. Have a failover-capable Microsoft SQL cluster (recommended) ready to provide the database for your ShareScan installation (a single SQL server instance with proper backup can be sufficient for disaster recovery solutions, but for a hot failover solution you may need a SQL cluster with at least 2 nodes).
4. Ensure that the MSNLB Cluster server feature is installed on all would-be nodes (servers). (This is an essential part of the supported Windows Server versions)
5. Set up your cluster in a standard way using the MSNLB Cluster server feature. Consult the MSNLB Cluster product documentation on how to do this: http://technet.microsoft.com/en-us/library/cc732149.aspx
6. **RECOMMENDED**: Use the ShareScan TroubleShooter Tool to run a pre-installation check on all (would-be) Manager PCs.
7. Install eCopy ShareScan 6.2 on each server.
8. After a successful installation, you have to specify three registry settings in order for eCopy ShareScan 6.2 to work in cluster mode; the `ClusterName` should be specified as the Fully Qualified Domain Name (FQDN):

   - `ClusterName`: needs to be created and set to cluster name as registered in DNS; open `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan\ShareScanManager` and create a new string key under this hive called `ClusterName` and specify the name of the cluster in this key

   - `ManagerIP`: needs to be set to cluster IP (registry path: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan`);

   - `ClusterNodeIP`: always needs to be set to the IP address of the physical network card which is NOT assigned to the MSNLB driver (usually the second network card); the registry hive is:`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan\`.

   Note:
   It is recommended to arrange the NIC handling the clustered traffic (cluster IP, devices connecting to these) and the other NIC (Management NIC) in two subnets, where possible
   – Possible problems:
   – in most cases, the device IP is used for printing as well, hence it should not be an easy task to address this issue in the target system; the goal should be to have the least necessary traffic between the cluster NIC-s and the switch in multicast mode
   – If separated network cannot be set up, it is by all means recommended to determine the binding priority of the network adapters in such a way that non-clustered NIC is set to be the primary one
   In order to set up / change the binding of network adapters, navigate to **Control Panel -> Network and Sharing Center**. Click **Change adapter settings**, then **Alt+N**, **Alt+S** to open the **Advanced Settings** dialog.

Make sure the NIC representing the cluster IP is ***NOT*** the first in the list.

9. Restart all ShareScan services under Windows Service Control Manager:

   - ShareScan Agent

   - - ShareScan Manager

   - - ShareScan WatcherService

   - - ShareScan Web Admin Host

   - - Capture Server Monitor (applies only if CSM is installed on the node)

Note:
After setup, it is recommended to run the troubleshooter to delete configuration data from the ShareScan database related to the originally used manager IPs to prevent any later confusion. This way, after deleting the "unused managers" from the database via the Troubleshooter tool, there will be only one IP address visible in the list of the Troubleshooter tool, on the dialog of the **Remove unused manager data** option.

You will see the same server from any Administration Console instances. Use any Administration Console instance to add devices and your system will act as a single unit.

MS NLB

UDP discovery during device addition works ONLY on the node that has value **1** set in the **Priority (unique host identifier)** field of the **Host Parameters** dialog of the Network Load Balancing Manager tool, therefore it is best to use that node to run the Administration Console if you plan to use UDP device discovery when adding devices to the ShareScan system.

Hints

To change cluster IP (in MS NLB), the recommended process is the following:

1. Delete all the devices from ShareScan
2. Stop all ShareScan related services, see section 3.2.1 / 9
3. Change the IP in the **MS NLB Manager**, and in the `ManagerIP` registry setting
4. Without starting any of the ShareScan services, start the **Administration Console**, and confirm that there was an IP change
5. Perform the necessary modifications in the network device (switch) configurations, if needed
6. Re-add the devices to ShareScan

As the process is complex, we recommend performing a fleet deployment only if the cluster IP is decided and considered to be final.

NLB Environment setup when using a hardware load balancer

Consult the white paper / ShareScan Referece Setup Guide respective to your load balancer, published via the eCopy support web site.

Upgrading eCopy ShareScan in a High Availability Environment

If you want to upgrade eCopy ShareScan in a High Availability environment without any downtime, follow the below directions:

Step 1

– choose a time period when the ShareScan system is not heavily loaded,

– use the node drain stop (or equivalent) option in the NLB manager tool to take the selected node offline,

– make sure that all jobs are successfully completed (by using the ShareScan Job Monitor web application),

– Stop all ShareScan services,

– upgrade via the **Copy current catalog to perform the upgrade on the following one:** option of the installer on the current node and specify a name for the new (version 6.2) ShareScan database (e.g. eCopyShareScan_6.2),

– test functionality with the local simulator,

– do NOT bring the node in the NLB Manager tool online / active.

Step 2

Use the following directions on the other nodes:

– use the node drain stop (or equivalent) option in the NLB Manager tool to take the selected node offline,

– make sure that all jobs are successfully completed (by using the ShareScan Job Monitor web application),

– Stop all ShareScan services,

– upgrade via the **Use a different exisiting ShareScan catalog** option of the installer on the current node and select the catalog name specified during the upgrade of the first node (above),

– test functionality with the local simulator,

– do NOT bring the node in the MS NLB Manager tool online / active.

Repeat Step 2 on the remaining nodes until half of the nodes are upgraded to 6.2.

If the first half of the nodes are upgraded, the old nodes (still on on earlier ShareScan version) should be stopped via node drain stop (in MS NLB Manager tool). When all earlier ShareScan version nodes are in drainstop / stopped state, turn on the 6.2 nodes, making sure that each of them works without any issues.

Afterwards, the rest of the nodes can be upgraded according to Step 2.

Important!
Restoring the database stops the ShareScan Agent service on all the nodes except the node where database restore is done. In this case, all Agent services must be stopped manually, and then restarted manually.

HTTPS Communication on Web-based Devices

For successful HTTPS communication on web-based devices, a Self Signed Server Certificate must be generated, exported and imported on all other nodes.

Creating Self Signed Server Certificates

Since ShareScan uses a Self Signed Server Certificate based on the IP address of the server and this certificate is of an unknown Certification Authority, certain vendor MFPs may display warning messages after an SSL Communication is initiated. To avoid these messages, create a self-signed certificate based on the Fully Qualified Domain Name (FQDN) of the server and install it as a root certificate on the MFP device.

Certificate Manager

The Certificate Manager is an addon tool for eCopy ShareScan, which allows you to manage the certificates required by some devices.

The Tool is installed in the **Tools** folder of the ShareScan installation (**%programfiles%\Kofax\ShareScan6.2\Server\Tools** when using the default installation path), and can be launched by double-clicking on the `CertificateManager.exe` file.

When started, the Certificate Manager displays the following buttons in its window; depending on your configuration, the first option (Configure Tomcat server.xml may not be available):

– **Configure Tomcat** `server.xml`: this option allows you to customize the cryptographic protocols and ciphers used by ShareScan on a port-by-port basis via editing the server.xml file used by the Tomcat component of eCopy ShareScan. Clicking this button displays a new window, listing all ports currently used by eCopy ShareScan, and the cryptographic protocols assigned for the specific port, if that port uses SSL or TLS. You can use the `server.xml` dropdown item in the top-left corner to create a backup of the server.xml file you are using, or you can load a previously saved server.xml.
To modify the protocols and ciphers assigned to a port, do the following:

1. Click on the port whose properties you want to modify.
2. Click the **Edit** button on the upper-right part of the window. A new screen is displayed, showing the currently used protocols and ciphers.
3. Under **Enabled protocols**, select the cryptographic protocols you want to use.
4. Under **Enabled Ciphers**, select the ciphers you want to use. For ease of use, a number of filter options are included with the tool, and can be accessed via button push (for example, **Remove weak ciphers**, **Select Java 6 ciphers**, **Remove ciphers using CBC encoding**, and so forth).
5. Click **OK** to save the changes.

– **Re-generate certificate**: this option allows you to recreate your digital certificate. To create the certificate, you have to enter either the IP address (**Discover IP** button) or Fully Qualified Domain Name (**Discover FQDN** button) to the displayed field under Certificate Common Name, then click the **Generate** button on the lower-right part of the window.

– **Backup certificate**: click this button to create a backup of your existing certificate. A **Browse** window is displayed, where you can select the location and filename of the certificate to be saved. Back up your certificates if you have imported your certificates manually to your Konica Minolta devices (to prevent the warning from popping up), and do not want to repeat the process.

Also, the recommended workflow when upgrading from an earlier ShareScan version is to back up your certificate, perform the upgrade of ShareScan, then restore the certificate.

– **Restore certificate**: click this button to restore a certificate. A **Browse** window is displayed, where you can locate the certificate to be restored.

How to create HTTPS certificates for your High Availability setup

Perform step 1-3 on one of the ShareScan nodes:

1. Use the **Re-Generate Certificate** option of the Certificate Manager tool. Use the MS NLB cluster IP or the FQDN that is registered in the DNS for the cluster.
2. Use the **Backup certificate** option to save the newly created certificate.
3. Restart the Apache Tomcat service.
4. Copy the created backup file to all the other ShareScan nodes or to a shared network folder accessible from all the other nodes.

Perform step 5-6 on the remaining ShareScan nodes

5. Use the **Restore certificate** feature of the Certificate Manager tool.
6. Restart the Apache Tomcat service.

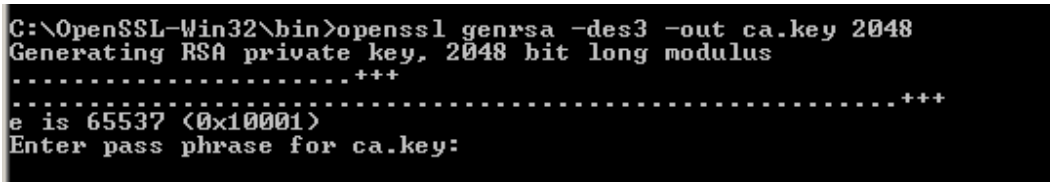
With the above steps, the same certficate will be installed on all ShareScan nodes.

How to generate certificate and install it under Tomcat

1. Generate your Certification Authority (CA)

a. Create a 2048-bit key to be used when creating your CA

– In command prompt, type `openssl genrsa -des3 -out ca.key 2048`

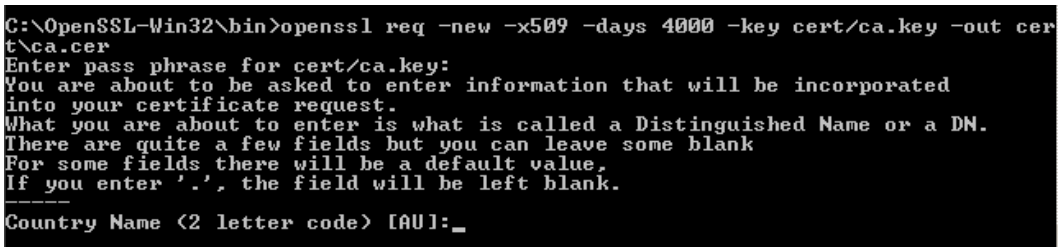


– You will be asked to supply a pass phrase for ca.key. The pass phrase will be requested whenever you use the CA certificate.

– This will create a file called `ca.key`, containing your certificate authority private key.

b. Create the CA certificate request

– In command prompt, type `openssl req -new -x509 -days 4000 -key ca.key -out ca.cer`



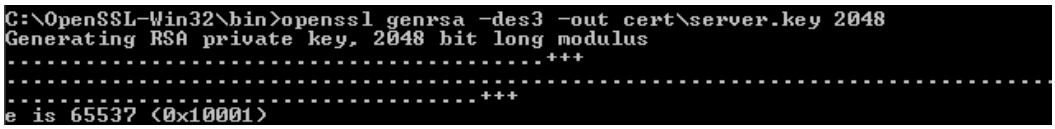
– You will be asked to enter a pass phrase. Make sure you enter the pass phrase used in the previous step. Also, you will be asked to complete certain fields: e.g. country, locality name. Please, do not forget to complete the **Common Name** field, that must be an FQDN (Fully Qualified Domain Name).

– The output CA certificate will be generated in `ca.cer` file.

2. Generate a Server Certificate

a. Create a 2048-bit key to be used when creating server (Tomcat) certificate.

– In command prompt, type `openssl genrsa -des3 -out server.key 2048`



– You will be asked to supply a pass phrase. The pass phrase will be requested whenever you use this certificate so make sure you remember it.

– This will create a file called `server.key` containing your server private key.

b. Create the server certificate request

– In command prompt, type `openssl req -extensions ssl_server -new -key server.key -extensions usr_cert -out server.csr`

– You will be asked to enter a pass phrase for `server.key`. Make sure you enter the pass phrase used in 1.a.

– Important: The `Common Name` has to match the FQDN/IP of the web server.

– This openssl command will create the server certificate request `server.csr`

c. Sign the certificate signing request with the self-created certificate authority that you made earlier.
In command prompt, type `openssl x509 -req -startdate -days 365 -in server.csr -CA ca.cer -CAkey ca.key -extensions usr_cert -out server.crt -CAcreateserial -CAserial ca.srl`

```
C:\OpenSSL-Win32\bin>openssl x509 -req -startdate -days 365 -in cert\server.csr
-CA cert\ca.cer -CAkey cert\ca.key -extensions usr_cert -out cert\server.crt -CA
createserial -CAserial cert\ca.srl
```

– You will be asked to enter a pass phrase for `ca.key`. Make sure you enter the pass used in step 1.a.

– This will create the server certificate `server.crt`

– The first time you use your CA to sign a certificate you can use the `-CAcreateserial` option. This option will create a file (`ca.srl`) containing a serial number. You are probably going to create more certificates, and the next time you will have to do that use the `-CAserial` option (and no more `-CAcreateserial`) followed by the name of the file containing your serial number. This file will be incremented each time you sign a new certificate. This serial number will be readable using a browser (once the certificate is imported to a `pkcs12` format). And we can have an idea of the number of certificate created by a CA.

– Important: By using the `-startdate` parameter, you are singing the certificate against the current date/time. Make sure that your environment has the correct date/time and timezone setup.

d. Generate a `.PFX` file / `PKCS#12` certificate
– In command prompt, type `openssl pkcs12 -export -in server.crt -inkey server.key -certfile ca.cer -name` FQDN/IP defined in the server **Common Name** field `-out serverCert.pfx`

```
C:\OpenSSL-Win32\bin>openssl pkcs12 -export -in cert\server.crt -inkey cert\serv
er.key -certfile cert\ca.cer -name 10.140.26.200 -out cert\serverCert.pfx
Enter pass phrase for cert\server.key:
Enter Export Password:
Verifying - Enter Export Password:
```

– You will be asked to enter a pass phrase for `server.key`. Make sure you enter the pass phrase used in step 1.a.

– You will also be asked to supply an export password.

– This will create the `serverCert.pfx` file.

3. Install the Server Certificate in Tomcat
– Copy the `serverCert.pfx` under **Tomcat8\conf** directory

– Convert `pfx` file to `jks` file

In command prompt, type `keytool -importkeystore -srckeystore serverCert.pfx -srcstoretype pkcs12 -destkeystore eCopy.key -deststoretype JKS`

```
C:\apache-tomcat-8.0.30\conf>keytool -importkeystore -srckeystore serverCert.pfx
 -srcstoretype pkcs12 -destkeystore eCopy2.key -deststoretype JKS
```

– create certificate

- In command prompt, type `keytool -export -alias` the Common Name used in 2.b `-keystore eCopy.key -file "..\webapps\ROOT\eCopy.cer"`

```
C:\apache-tomcat-8.0.30\conf>keytool -export -alias 10.140.26.200 -keystore eCop
y.key -file "..\webapps\ROOT\eCopy.cer"
```

- then type `keytool -export -alias` the Common Name used in 2.b `-keystore eCopy.key -file "..\webapps\ROOT\eCopy.der"`

- and finally type `keytool -export -alias` the Common Name used in 2.b `-keystore eCopy.key -rfc -file "..\webapps\ROOT\eCopy.pem"`

4. Upload the CA certificate `ca.cer` to the device.
5. Configure `server.xml`.

Certificate installation on ShareScan Manager PC

Prerequisites:

- Certificate for ShareScan manager PC:
- CA certificate
- Server certificate file (Manager-hostname.p12) – and password for accessing the private key
- WinHTTP Certificate config tool installer, winhttpcertcfg.msi, downloadable from Microsoft
- `winhttpcertcfg.msi`
- https://www.microsoft.com/en-us/download/details.aspx?id=19801

1. Install SS Manager certificate on the SS manager PC
   Start MMC / Certificates

i. Start MMC.
ii. Select File/"Add/Remove snap-in".
iii. Select "Certificates", press "Add".
iv. On "Certificates snap-in" panel, select: "Computer account".
v. On "Select Computer" panel select: "Local computer: (the computer this console is running on)", "Finish".

Import <CA certificate>

vi. Select "Trusted Root Certification Authorities" container.
vii. Click on "Certificates" sub-container.

viii. Right-click / All tasks / Import….
ix. Browse/Select “<CA certificate>” – Click Next, Next, Finish.
x. Do not change the “Certificate store” = “Trusted Root Certification Authorities”.
xi. Finish certificate addition and click OK on the notification popup.

Import Server certificate file (e.g. “managername.qa.local.p12”)

xii. Select “Trusted People” container.
xiii. Right-click / All tasks /Import…
xiv. Browse/Select the Server certificate file.
xv. Enter the password of the certificate.
xvi. Do not change the “Certificate store” = “Trusted People”.
xvii. Finish certificate addition and click OK on the notification popup.

2. Create a registry setting “SslCertificateThumbprint” for ShareScan, with the certificate`s thumbprint

The SslCertificateThumbprint identifies the certificate which the ShareScan manager should use.

Obtain server certificate thumbprint.

i. Using MMC, navigate to “Trusted People”/”certificates” container
ii. Click on the certificate, which you imported in step 1.
iii. Select “Details” tab.
iv. Click on “Thumbprint” field.

v. Copy the Thumbprint value.

vi. Paste to Notepad – remove all spaces from the thumbprint value (replace all space to <nothing>).

vii. Start Regedit.

viii. Navigate to “HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan\ShareScanManager”.

ix. Create new string value, Name = SslCertificateThumbprint.

x. Set Value= <*Thumbprint value without spaces*>.

3. Grant access right to certificate, for “Network Service" or for the account, which runs the ShareScanManager service

i. Install `winhttpcertcfg.msi`

ii. Open a Command Prompt as Administrator.

iii. Navigate to C:\Program Files (x86)\Windows Resource Kits\Tools\.

iv. Execute the following command: `WinHttpCertCfg.exe -g -c LOCAL_MACHINE\TrustedPeople -s "<SS server host-name FQDN>" -a "Network Service"`

Or if the ShareScan Manager service running account is customized, e.g “Domain\SSManager”, then use this account name in the command: `WinHttpCertCfg.exe -g -c LOCAL_MACHINE\TrustedPeople -s "W2k8x64R2-XY-QA.qa.local" -a "Domain\SSManager"`

v. Restart ShareScan Manager.

4 - Certificate creation for ShareScan

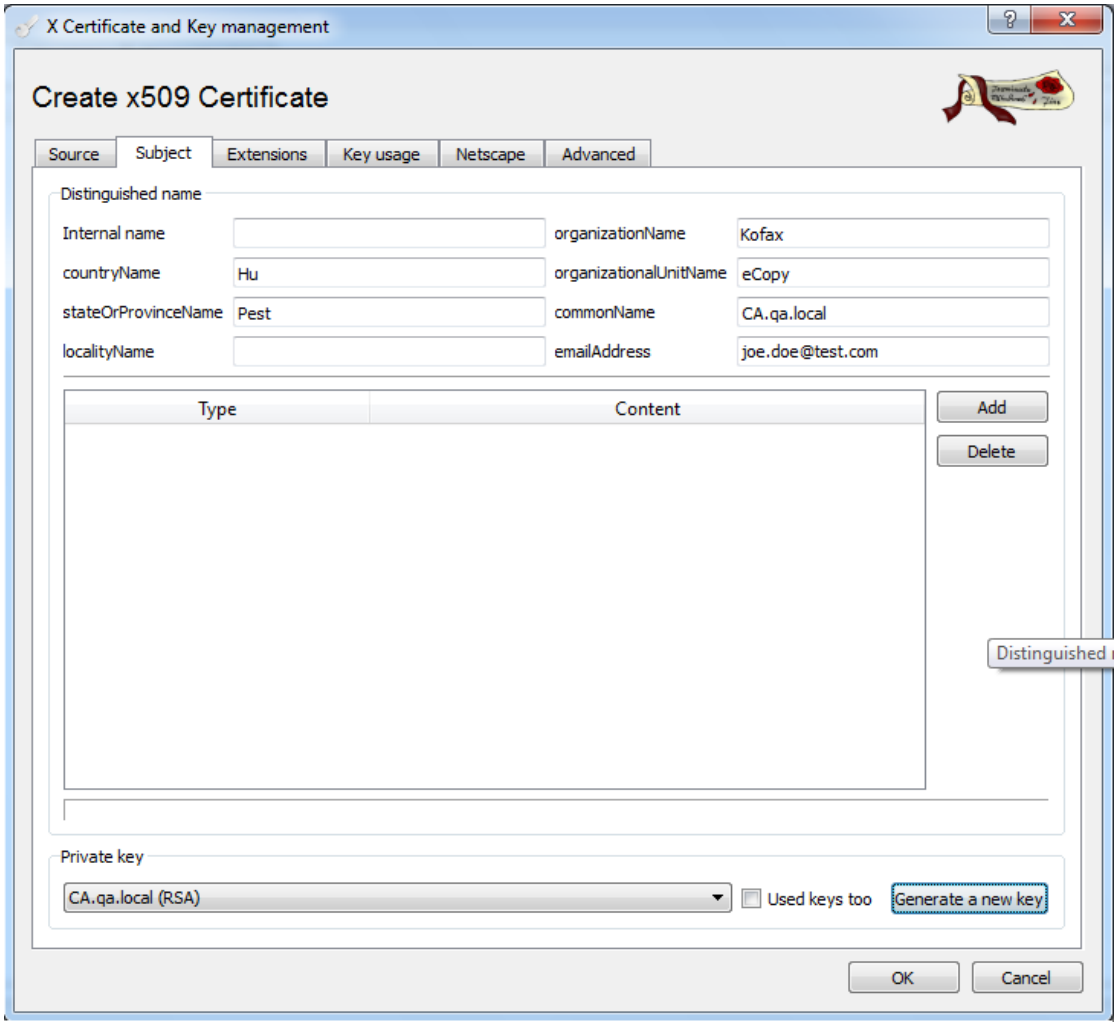
XCA software installation

1. Install XCA software (http://sourceforge.net/projects/xca/).
2. Launch XCA.
3. Create a new database.

Creating the CA Certification

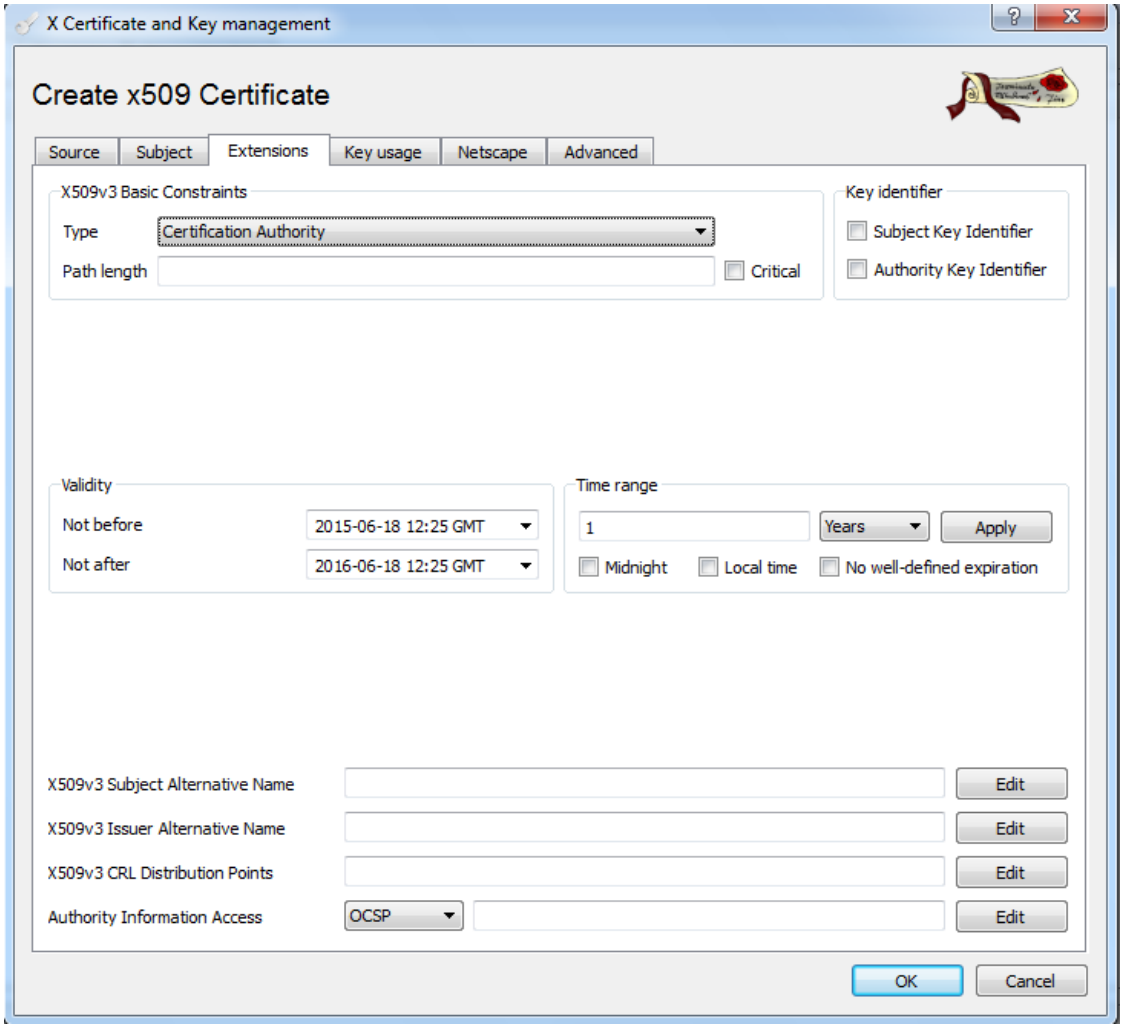
1. Select **Certificates** tab.
2. Select **New certificate**.
3. Fill the following fields.

4. Click the **Generate a New Key** button (RSA, 2048 bit).



5. Select **Extensions** tab.

6. Select **Certification Authority** as **Type**.

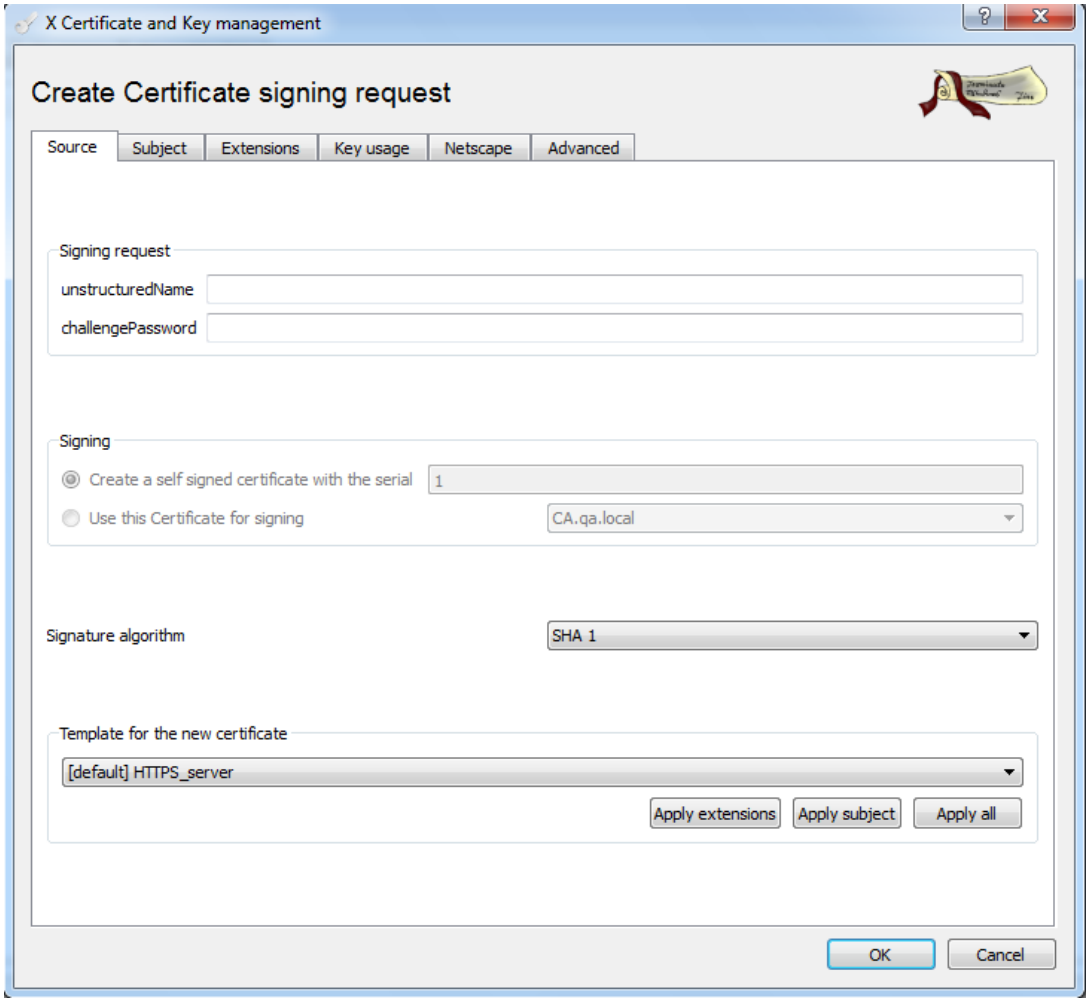


7. Click **OK**.

Creating Certificate for the ShareScan Manager

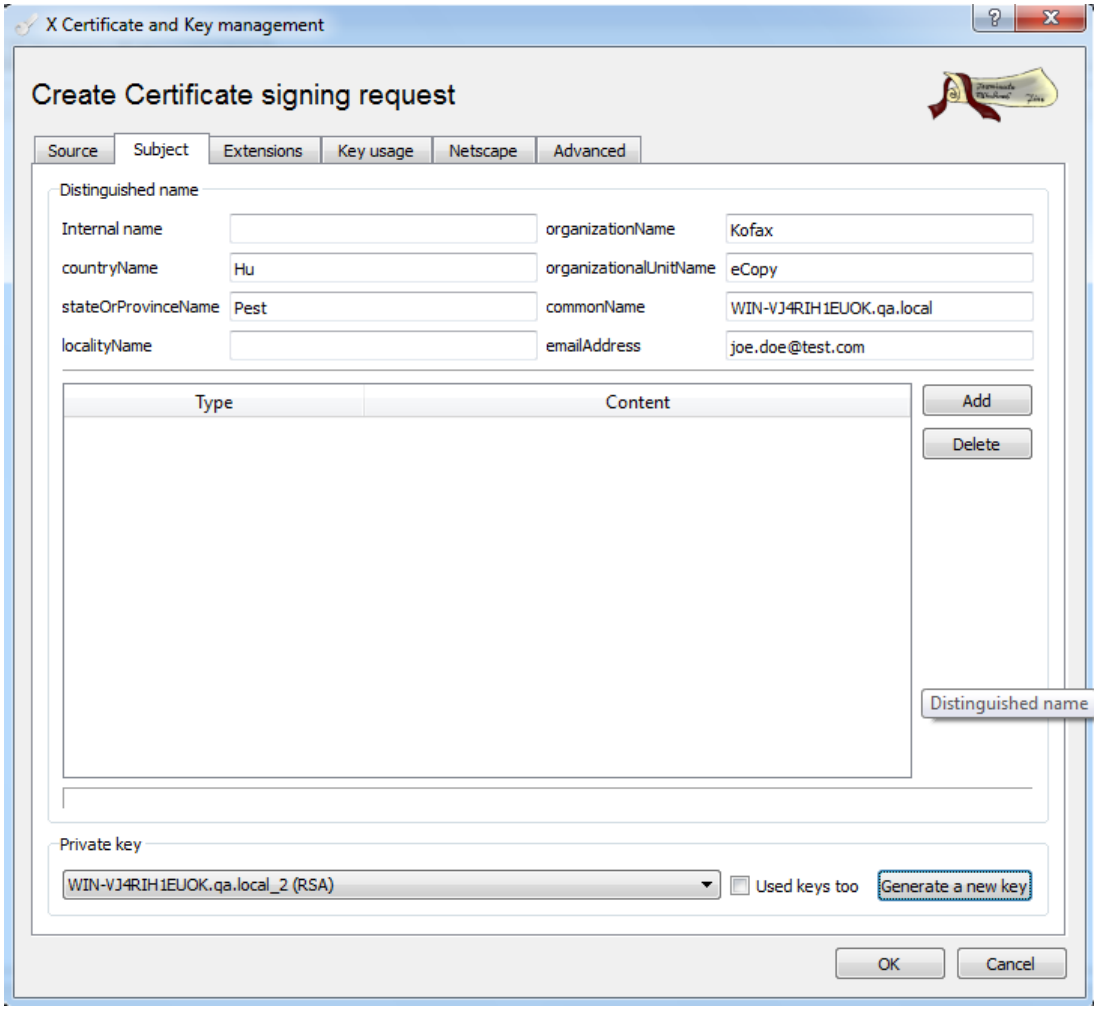
1. Go to the **Certificate signing requests** tab.
2. Click **New Request**.

3. Select **HTTPS_Server** as **Template for the new certificate** on the **Source**.



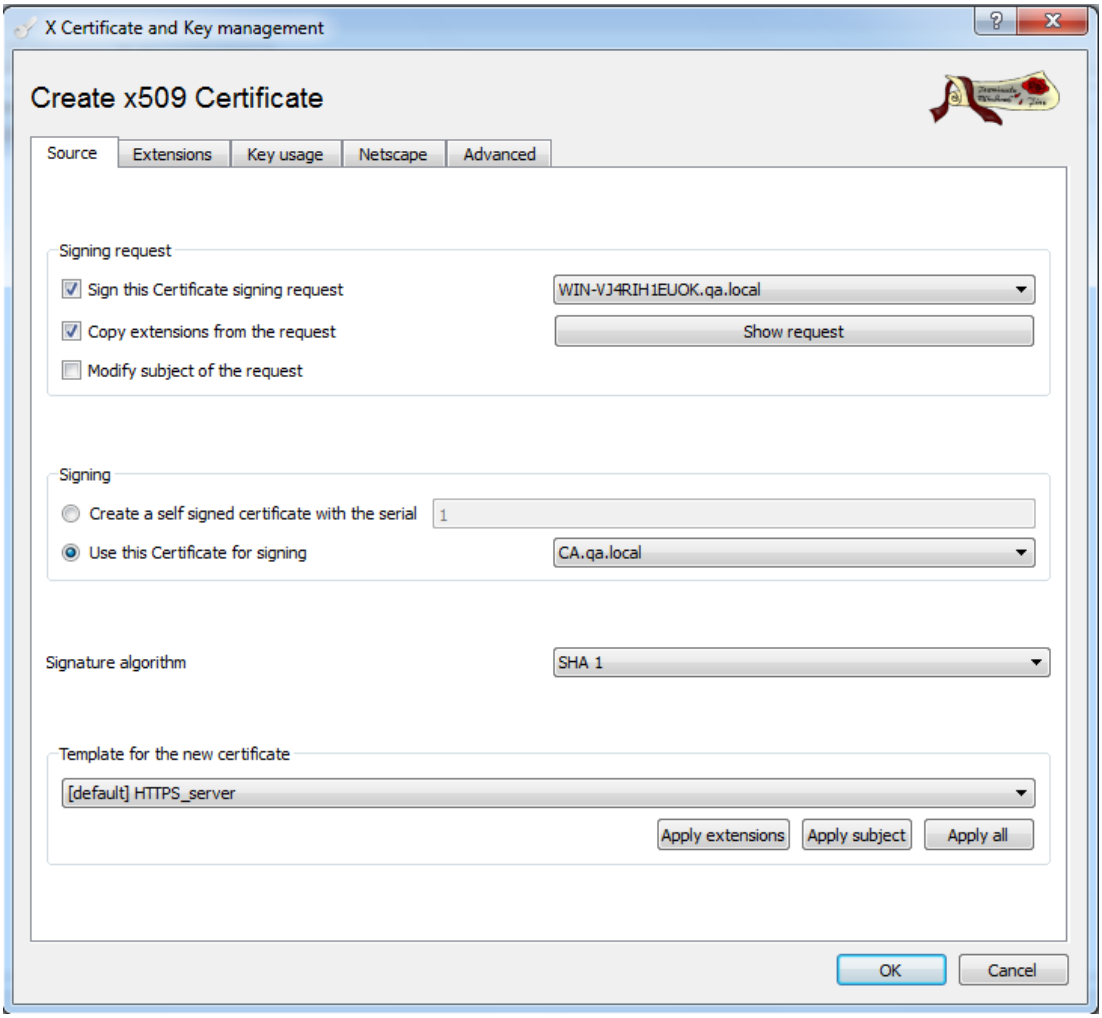
4. Fill the following fields.
5. **Important:** You have to define the computer host name in the **commonName** field. (where the ShareScan manager runs)

6. Click the **Generate a New Key** button (RSA, 2048 bit).



7. Click **OK**.
8. The certificate appears in the **Certification signing request** window.

9. Right-click on that and choose **Sign**.



10. Select **HTTPS_server** Template and select your CA for signing (**Use this Certificate for signing**).
11. Your signed certification will appear in the **Certificates** window as well (Under your CA).

Exporting certificate for the ShareScan Manager

1. Go to the **Certifications** tab.
2. Select your certificate for the ShareScan Manager (created in steps 11 – 21).
3. Click **Export**.
4. Select a destination folder and use `PKCS #12` export format.

5. Enter a password for using the private key – you will need this password when the certificate will be imported to the ShareScan machine.

Exporting CA

1. Go to the **Certifications** tab again.
2. Select your CA certificate.
3. Click **Export**.
4. Select a destination folder and use `DER` export format.

5 - High Availability Considerations

In case of eCopy ShareScan deployment with a high availability support, hardware and software failures are the two major failure categories.

Hardware Failure

Hardware failures prevent the network card from sending heartbeat messages to the cluster. Typical hardware failure scenarios include electric power loss, mainboard /CPU malfunction, memory error and the like. These types of issues are detected by the MSNLB Cluster technology through the loss of network connectivity.

When a node misses five consecutive heartbeat messages, the MSNLB Cluster manager detects the lack of signal and starts a convergence process. During convergence, the MSNLB Cluster re-assigns all connections between the healthy nodes and clients, the same way it happens when a client wants to connect to a node for the first time. The state of all the servers in MSNLB Cluster Configuration Utility is changed to 'Convergence' which means that distribution procedure of devices is started from scratch. This is an automatic process.

When convergence is finished, users can continue working.

To ensure that the operations / workflows happen (on healthy nodes) at the very moment of the convergence process, there is a configurable delay preserving connections. Only after the pre-set delay is configured are the active connections re-arranged. (The setting referred is on the **Port rule** dialog, and the recommended value is 5 minutes).

Similarly, hardware load balancers are able to detect the basic availability of the server hardware and networking infrastructure by pinging the server and opening TCP connections, as configured in the load balancer (typically these checks are called 'monitoring').

Software Failure

Software failures are ShareScan related errors; network load balancers (both MS NLB and hardware load balancers) are unable to detect higher software (ShareScan) level errors hence the need for the Capture Server Monitor, which is able to send commands to the MS NLB Cluster and alert the administrator via email.

When using a hardware load balancer, the CSM enables integration with these (to let CSM turn off a server node if necessary) is possible by running a custom command script.

Risks and Limitations

eCopy ShareScan 6.2 has the following limitations:

Folder or Email watch*	Not Supported via Capture Server Monitor
ScanStation**	Not Supported for HA; LB (without HA) is supported on ScanStation
High Availability via NLB clustering	Not supported if Cost Recovery v2 integration is used

* Watcher workflows are fail-safe by design, if more than one ShareScan Managers are installed and watching the same folder or email inbox. In this setup, jobs are restarted when they are not completed within a preset time window.

** ScanStation is not supported in cluster environment

6 - Load Balancing of Document Building/OCR

Document creation and OCR are the most resource-consuming phases in a scanning, document processing and storing workflow.

To ensure the shortest delivery time of the documents, distribution of the document processing tasks on multiple servers is a recommended technique, also called load balancing.

To enable this feature in ShareScan, follow the below steps:

Note:
It is recommended to install ShareScan 6.2 in a custom installation mode, specifying custom accounts to run the Manager and the Agent services. If you do so, you can avoid the cumbersome process deatiled below in step 2 – you only have to follow the instructions in step 1, and grant full read / write access to these custom (domain) accounts on the shared work folder specified in the `ScannedFilesLocation` advanced setting (detailed below)

1. Launch the **ShareScan Administration Console** application. For the particular configuration tasks your deployment requires, press F1 in the Console window to access product Help. Should you wish to take advantage of load balancing capabilities, specify the following three advanced settings:
    a. Select the **Home** tab in the Administration Console and click **Settings** in the **System** group.

    b. Scroll down to the **Advanced** header, select the field **Advanced ShareScan Settings** and click the '**...**' button on the right.

    c. Click **OK** in the Warning window and proceed with care.

    d. Expand the node **Shared manager settings**. Scroll down to `WorkerQueueManagerShareJobs`, and set its value to `TRUE` (if set to `TRUE`, all the Managers running on different servers check the common job queue, stored in the shared database if there is a document to process / OCR. Click **Save and close** and then **OK** on the warning message.

    e. Collapse this node and expand the one that shows the name and IP address of the Manager. Locate the setting `ScannedFilesLocation` and specify a valid path. Specify a UNC path representing a shared network folder. Mapped drives (with a drive letter) are NOT possible to use here. All servers in system must have access to this shared folder (Read/Write access for the account running the ShareScan Manager and Agent service).To change the default (local) service accounts to a domain account, see next list item.

    f. Locate the `OutputCreatorReuseWorkerProcess` setting: it should be set to `False`. You might also want to consider to review or set the `MaxNumberOfOutputCreators` value. Its value can be an integer number to specify how many parallel processes can be used for OCR / document creation. The scaling / recommended hardware documentation has some proposed values for different configurations. If not specified by this registry setting, the default values are the following (Number of CPU Cores - Number of output creators): 1 - 1, 2 - 2, 4 - 6, 8 – 12.

    Note:
    Once these three advanced settings are specified, the services (Agent and Manager) must be restarted on ALL the servers / nodes.

2. Follow the steps below only if your installation uses the default NETWORK SERVICE and Local System accounts to run the ShareScan Manager and the ShareScan Agent services. If you have an installation with custom (domain) account to run these services, then see the **Note** before step 1.

   To run the ShareScan Manager as a non-local (domain) user, you need to:

   d. create a domain user having the following rights
      – same privileges enabled as the NETWORK SERVICE built-in account, namely (see privileges listed in Local Policy Editor, User rights Assignment):
      – Bypass traverse checking
      – Create global objects
      – Impersonate a client after authentication
      – Log on as a service

   e. The account must have full (read/write) access to the network share used as a shared work folder

   f. The account must have read access to the local ShareScan installation folder

   g. The account must have full control to the `Program Data\Nuance\ShareScan` folder (usually on drive `C:\`)

   h. The account must have full control to the registry hive `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance`

   i. Start the Windows Service Control Manager

   j. Stop the ShareScan Manager service and double click the service in the list. On the opening dialog, click on the **Log On** tab

   k. Select the **This account:** radio option, and specify the account name and the corresponding password.

   l. Click **OK**

3. If you plan to use Folder or Email watcher features or the Scan To Desktop connector, the service account needs to be changed in the same way as it is described for the ShareScan Manager.

4. Similarly to the change of the account running the Manager Service, you also need to change service account of the ShareScan Agent Service. As this service performs some system-level operations, it requires different privileges than the ShareScan Manager Service. To run the ShareScan Agent as a non-local, but domain user, you need to:

   a. create a domain user that has the following rights - same privileges enabled as the Local System built-in account, namely (see privileges listed in Local Policy Editor, User rights Assignment):
      – Generate security audits
      – Bypass traverse checking
      – Create global objects
      – Create page file

– Create permanent shared objects

– Impersonate a client after authentication

– Increase scheduling priority

– Lock pages in memory

– Act as part of the operating system

– Log on as service

b. The account must have full (read/write) access to the network share used as a shared work folder

c. The account must have read access to the local ShareScan installation folder

d. The account must have full control to the **Program Data\Nuance\ShareScan folder** (usually on drive **C:**)

e. The account must have full control to the registry hive `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance`

f. Start the Windows Service Control Manager

g. Stop the ShareScan Manager service and double click the service in the list. On the opening dialog, click on the **Log On** tab

h. Select the **This account:** radio option and specify the account name and the corresponding password.

i. Click **OK**

5. Make sure the service account is changed to the domain account on ALL server nodes.

6. Once these two advanced settings are specified and the service accounts are changed to the domain accounts, the ShareScan services (Agent and Manager, and optionally the ShareScan Watcher Service, if you use email or folder watcher functionality) must be restarted on ALL the servers / nodes.

7. Pay particular attention to specifying the same `ScannedFilesLocation` folder for all server nodes in the Advanced Setting editor.

8. Add devices to managers:

   – If a high availability setup is used: it is recommended to use one Administration Console and then there is only one clustered virtual Manager in the system. Devices can be added to the system in that one Administration Console.

   – If only Document Building/OCR Load Balancing is configured as in 3.2.2: (without MSNLB high availability Cluster): there is no Manager clustering; there are only separate Managers. This time adding devices to the Managers must happen separately. It is recommended to connect to every Windows Server via Remote Desktop and add the devices in the given Manager Administration Console or use the Remote Management feature of the Administration Console. This Document Building/OCR Load Balancing feature is independent from the high availability setup implemented on the MSNLB Cluster - they can also be used together or any of them can be used on its own.

7 - Additional Documentation

Besides this current deployment guide, the following documentation is available for your perusal with eCopy ShareScan:

– **Pre-installation Checklist and Sizing Guide** (PDF) – provides info on the issues to be addressed before deploying ShareScan.

– **Installation Guide** (PDF) - contains information on installing eCopy ShareScan, including hardware and software prerequisites.

– **Administration Console help** – the integrated help of the application, covering the use of ShareScan beyond installation, and provides configuration information. The help is accessible by pressing F1 on the ShareScan Administration Console.

– **Troubleshooter User Guide** (PDF) – contains information on how to use the ShareScan Troubleshooter, a built-in diagnostic tool of the product.

– **Release Notes** (PDF) – contains an overview of the changes for the given ShareScan release.

– **eCopy ShareScan Capture Server Monitor Configuration Guide** (PDF) - contains information on how to use the Capture Server Monitor tool for monitoring ShareScan instances.

– In case of using a hardware load balancer: ShareScan Reference Setup guide (white paper) released for your hardware load balancer. This contains the pre-requisites and configuration parameters ShareScan is compatible with.

To view the PDF documentation, you must have a PDF reader application installed.

8 - Glossary

For a full understanding of this current document, knowledge of the following terms is essential.

Node

A node is a PC or a virtual PC, the base unit of a cluster. Nodes are members of the cluster.

Cluster

A group of nodes configured as a single server computer. A cluster consists of at least two nodes; they usually represent a server computer. For maximum level of availability and fail-safe operation, it is recommended to run the nodes on at least 2 physical hardware. A cluster is transparent for the user; it is represented by a separately assigned IP address on the network, different from any nodes' IPs.

Heartbeat

A message sent by the NLB driver in a cluster in regular intervals to detect node failures.

High availability support

The main purpose of this function is giving an option to keep the system alive when a node goes down. (e.g.: memory, HDD or CPU failure, electric power loss or unrecoverable software error)

Load Balancing support

The main purpose of this function is to distribute the load between available nodes in real-time.

Capture Server Monitor

A utility that monitors the ShareScan managers, stops any node and sends email notification to a predefined email address when ShareScan stops working on a node.

Drainstop

The drainstop command can be executed in the **Network Load Balancing Manager**: **right-click selected node/cluster > Control Host > Drainstop**. The MSNLB Cluster manager disables the affected node when a job queue becomes empty. Due to drainstop, the MSNLB Cluster waits a specified time before shutting down the node. Waiting time can be configured between 1-5 minutes.

Convergence

Convergence means that the MSNLB Cluster re-assigns all connections between remaining nodes and MFPs just like it happens when an MFP wants to connect to a node for the first time.

Virtual device

The state of ShareScan is monitored by the Capture Server Monitor through virtual devices. Each node has a separately registered virtual monitoring device.

9 - Configuration, Troubleshooting and Testing

– Always complete a successful and working setup before enabling Capture Server Monitor. If High Availability setup is created, make sure that the MS NLB system works properly with ShareScan, (i.e. different MFP devices are connected to different server nodes.

Note:
As the MS NLB system uses its own internal algorithm to assign devices to servers, it is NOT guaranteed that randomly selected two devices connect to different server nodes. However, this algorithm is designed to ensure that in case of a high number of connections (devices), the distribution is close to the even distribution.

To test whether multiple different devices connect to different ShareScan server nodes, the easiest way is to create a ScanToFile connector profile with a local folder destination. This saves the output document into a local folder on the node that handles the actual device connection.

By checking the content of the folders in Windows Explorer on all the nodes, you should see that by using multiple devices, the output documents keep appearing on different servers. Note that a scan initiated on a particular device results in an output document always on the same server until the number of the server nodes changes (server node was taken away because of failure or if a new node is added or a node is added back to the cluster). To perform such a test, you have to use as many multiple devices as you can.

– Enable Capture Server Monitor server only after the proper functionality is tested. Make sure the time windows the Capture Server Monitor uses are specified correctly, as too short windows may result in false alerts or false failure triggers (turning off a node). It is recommended NOT to enable the High Availability mode in the CSM immediately, but only the email alerts. After some time of normal system usage, the CSM settings (testing interval and evaluation window) can be tuned to ensure that no false failure email alerts are sent. Afterwards the High Availability mode can be enabled (with evaluation window not shorter than the email alert evaluation window).

– In case of using the High Availability deployment option and integration with a Cost Recovery server or ID Services server, the cluster IP should be used when you configure the **ShareScan server IP** in the CR or ID service software.

– After configuring MS NLB for ShareScan High Availability mode:

– make sure the MS NLB Manager indicates that all the cluster nodes are marked with a green icon

– use a computer that is on the same subnet as the MFP devices, open a command window, and issue the following commands:

- `arp –d`
- `ping <cluster IP>` (ICMP protocol should be enabled on the computers / networks / firewalls)
- ping should succeed
- `arp –a`

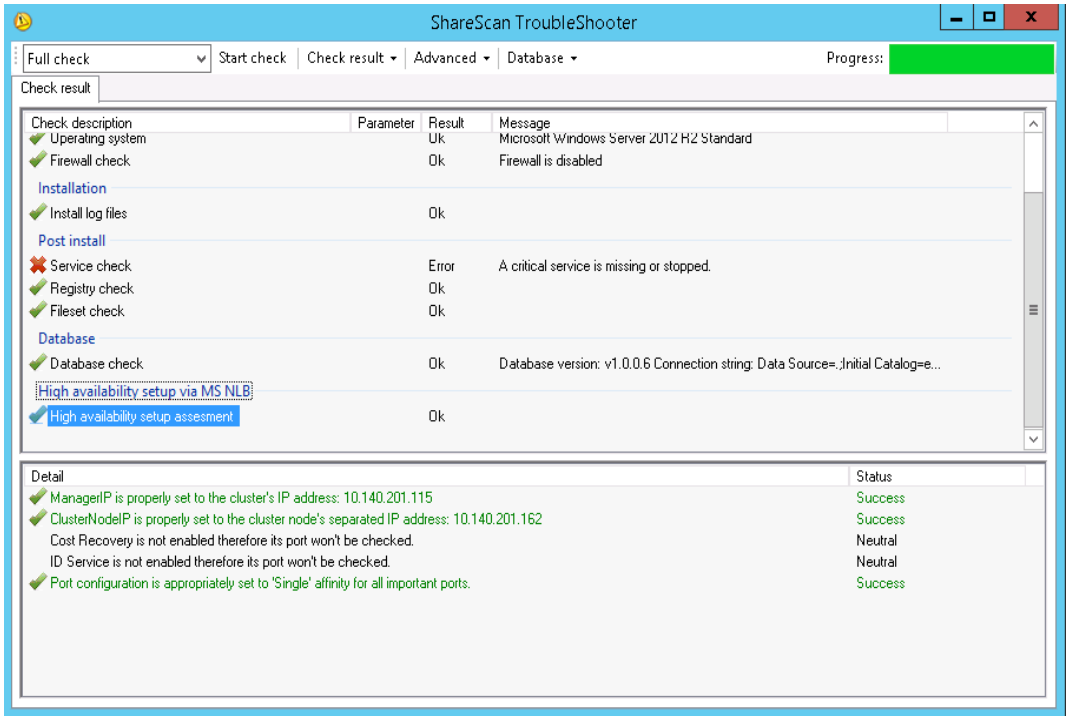
– use the ShareScan TroubleShooter tool to test the core MS NLB functionality:

Verify/Troubleshoot the High Availability Setups by the ShareScan Troubleshooter

The ShareScan Troubleshooter has the following new options to help to verify / troubleshoot the High Availability setups built on the Microsoft Network Load Balancing infrastructure.

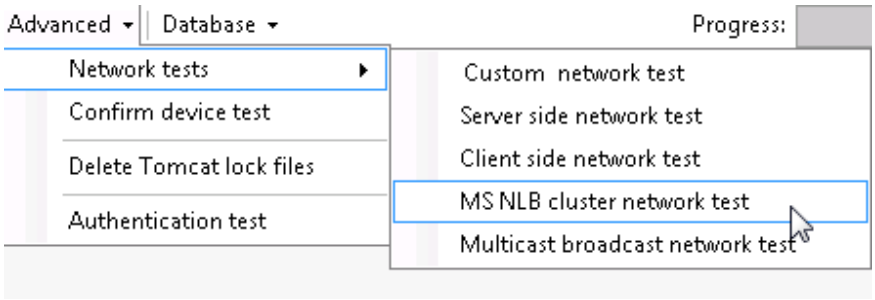
Before testing, make sure the MS NLB and the ShareScan registry settings are set properly, in accordance with the **High Availability and Load Balancing Deployment Guide**.

1. The Full Check option (started by the **Start check** button) on the menu bar performs a check to determine if the MS NLB based cluster is configured.
   The checker adds a last section to the report, with a section named **High Availability setup via MS NLB**.



If there is an inconsistency / missing item in the configuration settings (`ManagerIP`, `ClusterName` and `ClusterNodeIP` settings in the registry) or if these are not in sync with the actual settings of the Microsoft NLB system or the network adapters, then alert lines in red appear in this section.

2. There are two new menu items:



– MS NLB cluster network test
This is a client-server communication test, to see if MS NLB is set up properly and the requests from the outside of the cluster (the part of the network where the devices exist) are dispatched to one of the server nodes in the cluster. During multiple repeated connection tests, the routing of the individual request should vary sometimes (once the response should arrive from server node X, next time from server node Y, etc.), proving that NLB 'spreads' the requests across the server nodes.

Note:
This test is performed on TCP port 9599, which should be configured with **Node affinity: None** option in the Port Rule editor of the MS NLB Manager as it is documented in the **High Availability and Load Balancing Deployment Guide**, allowing the new TCP connections to assign to a server node randomly. This mode is NOT used for the normal ShareScan device-server connections, but for Cost Recovery and Identification services. However, the test is useful to prove the proper configuration of the MS NLB system.

Note:
As mentioned previously, the ShareScan Load Balancing feature does NOT rely on the load balancing capability of MSNLB (i.e. it is able to dispatch the requests to different nodes to enable even load); we use MSNLB only for High Availability. However, to test if MSNLB functions properly, we test the dispatching feature on port 9599, configured specially for this type of test.

How to set up and perform a test:

1. Start the ShareScan Troubleshooter tool on all of the tested cluster nodes – these instances of the Troubleshooter tool will be called "server agents".
2. Copy the following files to a folder on a PC connecting to the same network to which the MFP devices are connected (or will be connected), and launch the ShareScan Troubleshooter tool – this instance is called "client agent".
3. Select the **MS NLB cluster network test** menu option (on all nodes).
4. A dialog appears.
5. Click the **Start listening** button on the dialog on all the "server agents".

6. On the “client agent” instance enter the IP address of the cluster (the IP address used in the `ManagerIP` registry entry) into the text field.
7. Click the **Connect** button on the “client agent”.
8. If the request sending / response receiving is successful, then you should see 3 lines:
   – **Local / Connect / Cluster IP:9599** (in green)

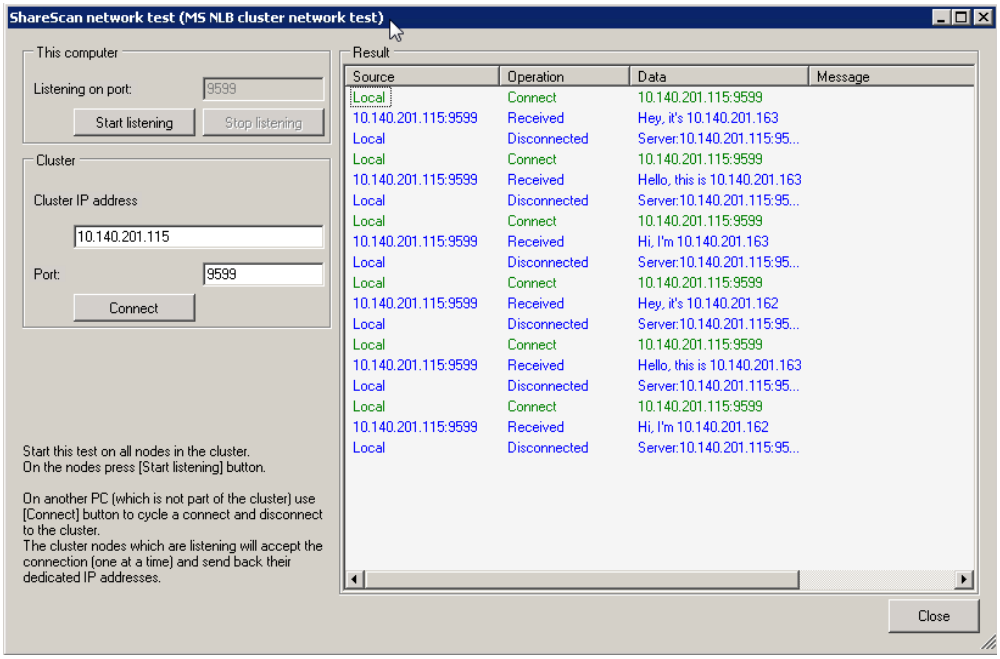
   – **Cluster IP:9599 / Received / Hey, it’s X** or **Hi, I’m X** or **Hello, this is X** (in blue), where X is the `ClusterNode IP` of the responding server node

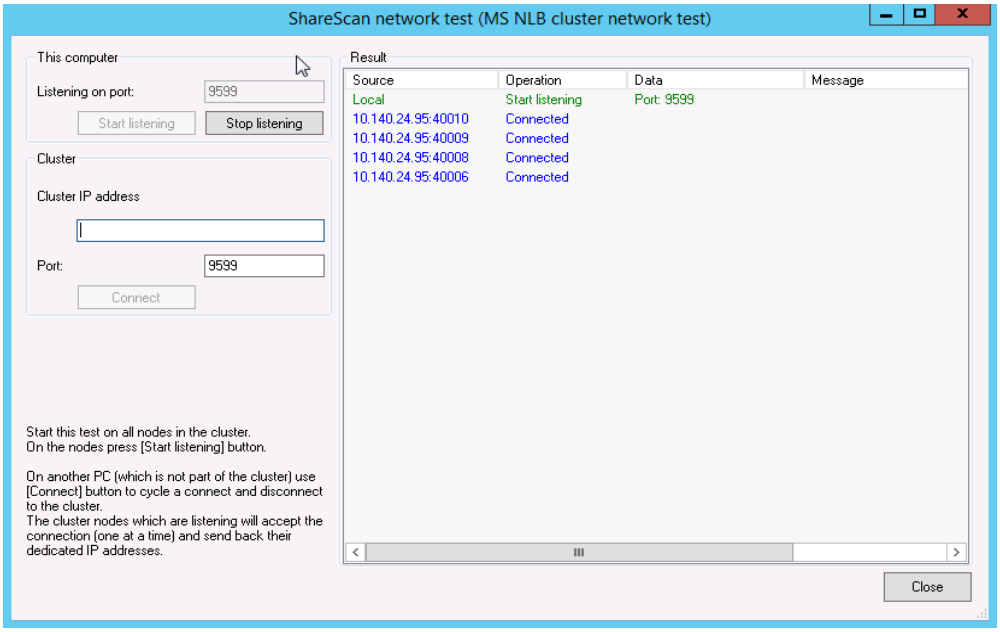
   – **Local / Disconnected / ClusterIP:port**
9. In the console of the “server agents” (always only in the instance that actually gets the request) you should see lines appearing saying **<IP:port> Connected** in blue, where **<IP:port>** should correspond to the “client agent”.

If you click the **Connect** button several times (wait until all the 3 lines are listed) you should see different IP addresses in place of X, representing the different server nodes.

If you can see the `ClusterNodeIP` of all of the nodes at least once, then the entire test is successful.

Note:
One should not expect that the server nodes are hit by the requests in a round-robin manner. As the TCP connection-server node assignment is decided by the MS NLB based on the client IP and the source port (which is selected randomly by the “client agent”) it is not guaranteed that the next server node is hit next, nor that the requests are spread evenly – this is out of scope for this simple test tool.

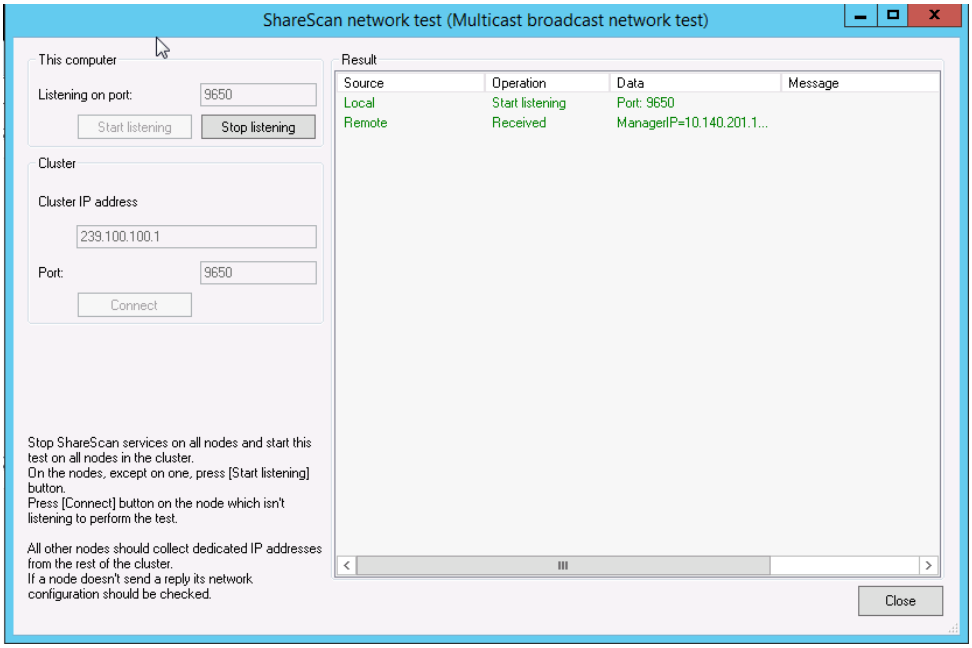




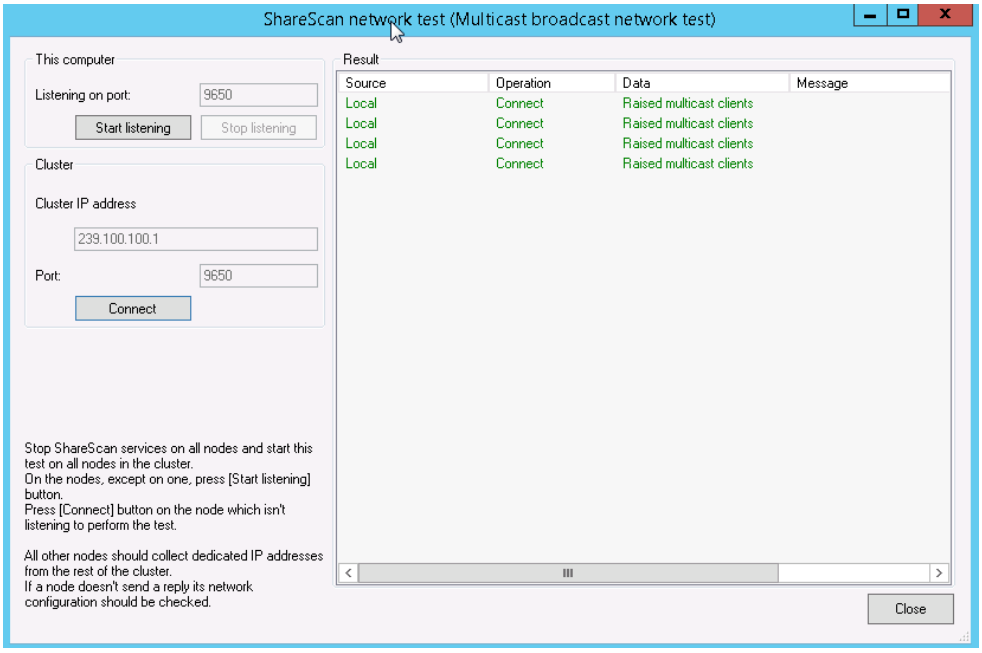
– Multicast broadcast network test

To test the Multicast broadcast functionality of the network, click the **Advanced > Network tests > Multicast broadcast network test** menu item on all ShareScan server nodes.

On the dialog that appears, click the **Start listening** button on all the server nodes (these will be the test servers), except one (which will be used as the message sender).



On the single node you use as a message sender, click the **Connect** button:



When you click the **Connect** button, a broadcast message is sent to all the test servers, listening on UDP port 9650.

If these test servers receive the message, they write out a line into the right-hand list, with the text **Receive** also indicating the IP address of the sender.

This line should be shown on all the servers where the network test dialog was started with the **Start listening** button.

If the test was successful, it should be repeated on all nodes, so all of the nodes should act as a message sender once, while the others are listening.

Determine actual device request

To check which Manager serves the actual device request, a diagnostic feature is included.

If you create a registry setting: `HKEY_LOCAL_MACHINE\SOFTWARE\Nuance\ShareScan\ShowClusterNodeIP` (string value, true/false) then the `ClusterNodeIP` value (which can be used to uniquely identify the Manager, and is set by the registry settings at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nuance\ShareScan\ClusterNodeIP`) of the Manager serving the request will be displayed on the Main screen, in the section where usually the "**Place a document into the feeder…**" instruction appears. This can be used to determine if the devices are connected to a specific Manager.

Another method to determine the MFP-Manager assignments is detailed below:

– Turn on verbose tracing on the Manager – if the High Availability system is already set up via MS NLB, then it is enough to turn on the tracing on a single Administration Console instance

– Use the devices

– Export the traces (from all server nodes)

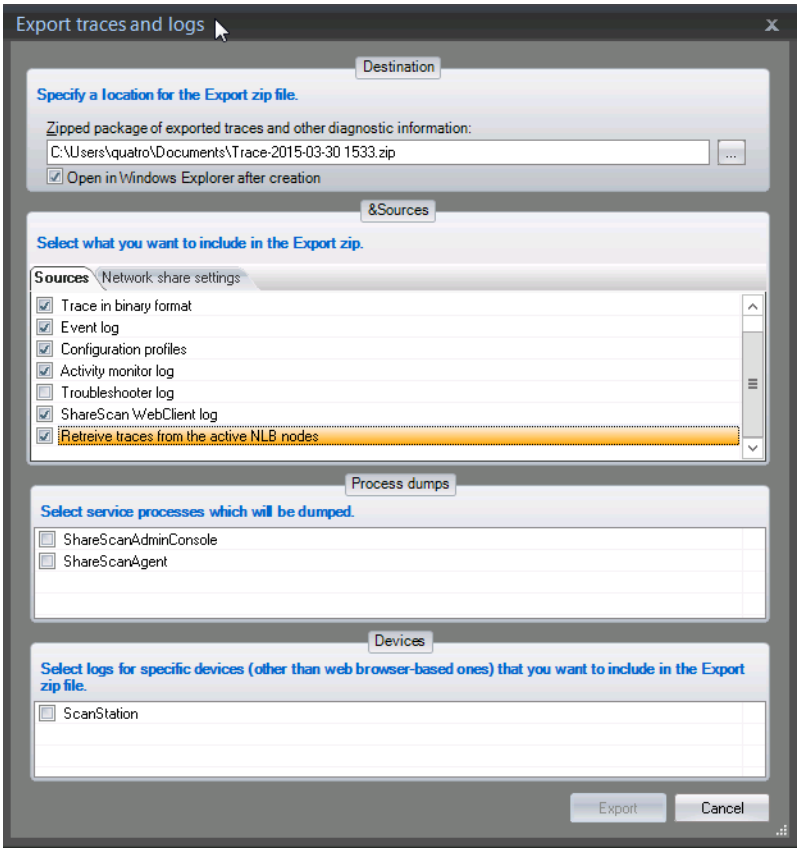
– Open the `Trace.txt` file of a given Manager, and search for **\xxx.yyy.zzz.www** where **xxx.yyy.zzz.www** is the IP address of the device you need.

If the string is found, then the MFP is served by that Manager.

Note:
The MFP – Manager node assignment is constant only until a Manager node is removed or added to the cluster – in case of a change, the device-Manager node assignments are recalculated by MS NLB.

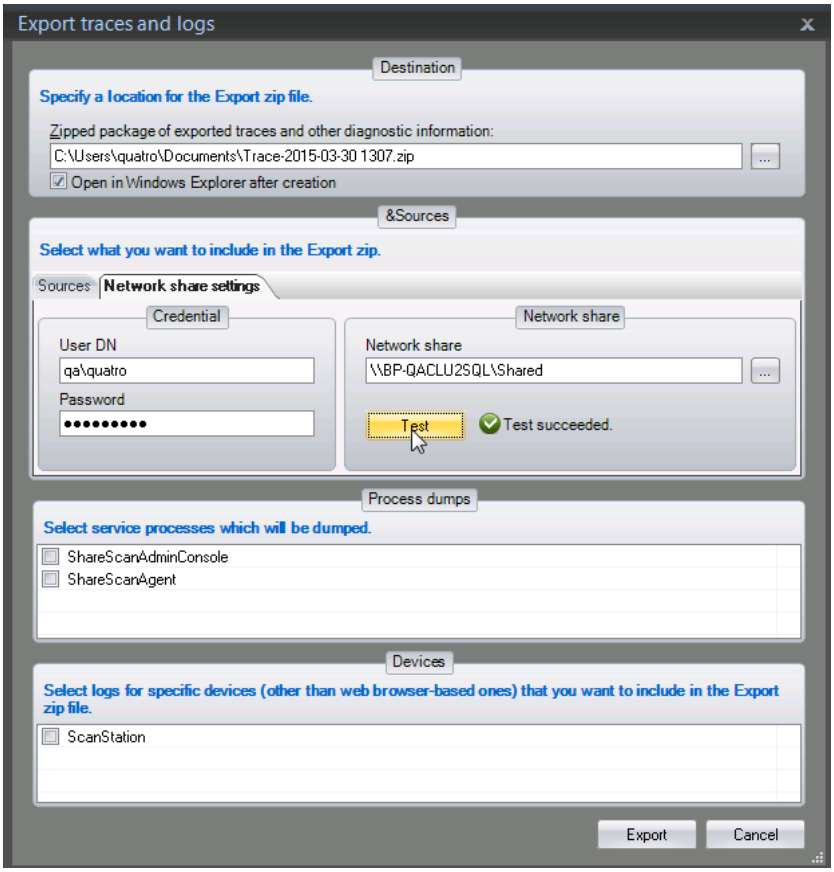
Exporting trace in a High Availability environment

When a trace export is needed in case there are multiple nodes set up in a High Availability environment, mark the **Retrieve traces from the active NLB nodes** checkbox to display the **Network share settings** tab next to the **Sources** tab in the **&Sources** section of the **Export traces and logs** dialog.



When this checkbox is selected, before clicking the **Export** button, the user should configure the network share settings (by selecting the **Network share settings** tab next to the **Sources** tab). After configuration, click the **Test** button to make the Export button active. It becomes active only if the test is successful.

Note:
The **Retrieve traces from the active NLB nodes** checkbox appears only in a Network Load Balancing environment.



This network folder is used to collect the trace export from all the server nodes.

Using the ShareScan Troubleshooter tool with hardware load balancers

The tool can be used for checking environments with hardware load balancers as well, with the following differences:

– In **Full check** mode, the MS NLB test will not succeed, since it is not required when using a third party hardware load balancer

– For network tests and to see if the hardware load balancer is properly configured, the **Custom network menu** option should be used. The other test described in 8.1 is specific to MS NLB, therefore they may not provide useful results when using with a third party load balancer.

When testing a hardware load balancer, after setting it up:

– make sure all ShareScan services are stopped on the server nodes

– Start the **Custom network test** of the troubleshooter tool (**Advanced menu > Network tests**) on all the servers

– Specify the port you want to test and click the **Start listening** button (on all servers)

– On a PC which is not part of the NLB cluster, start the Troubleshooter tool (simply copy the **Tools** folder to another PC, no installation is required; or, you can run a **Complete installation** on a PC, with a local database- it will install the Troubleshooter tool as well), use the **Custom network test** option, and anter the NLB cluster IP ('Virtual IP') into the **Address** filed of the **Remote computer** panel, and specify the port you want to test (and what you specified when you started the test dialogs on the servers), and click **Connect**.

– If the NLB system is working correctly, the connection should be successful

– Enter some text into the payload input field and click **Send**

– The message should appear in the dialog box of one of the servers

– To see if the failover mechanism is working, turn of the network adapter of the server where the message arrived successfully

– Repeat the connect / send message steps above – you should see that the connection / message arrives to another server node.

10 - Frequently Asked Questions

Q: How to set up MFP IP addresses to ensure the device-server node assignments happen evenly?

A: It is recommended to use a continuous range, if possible. If a wider IP range is used and it is not possible to assign continuous range(s), an evenly spread random IP assignment is a also a good choice. A device IP is a factor in the algorithm how the devices are assigned to a server node of the cluster, so this influences how many MFP devices are assigned to a particular node.

A strict control on the assignments is not supported due to the nature of the algorithm Microsoft NLB operation is based on.

Q: Is it possible to recover lost jobs /documents?

A: Recovering lost jobs / documents is possible via the Job Monitor Web UI – the jobs in failed state can be downloaded (scanned pages, or, if the final document creation was successful, but the storing operation failed, the final document(s) will be downloadable.

However, if there was a server (node) failure when the workflow was still in a processing phase, data loss might not be fully avoided.

Appendix

11 - How to install and configure NLB cluster on Windows 2008

Installation of NLB feature on all NLB nodes

Installation should be done on ALL NODES in the NLB Cluster. In this below sample, installation is performed on 2 nodes, the computer (host) names are PL2008-01 and PL2008-02, and the FQDN is **pintolake.net**.

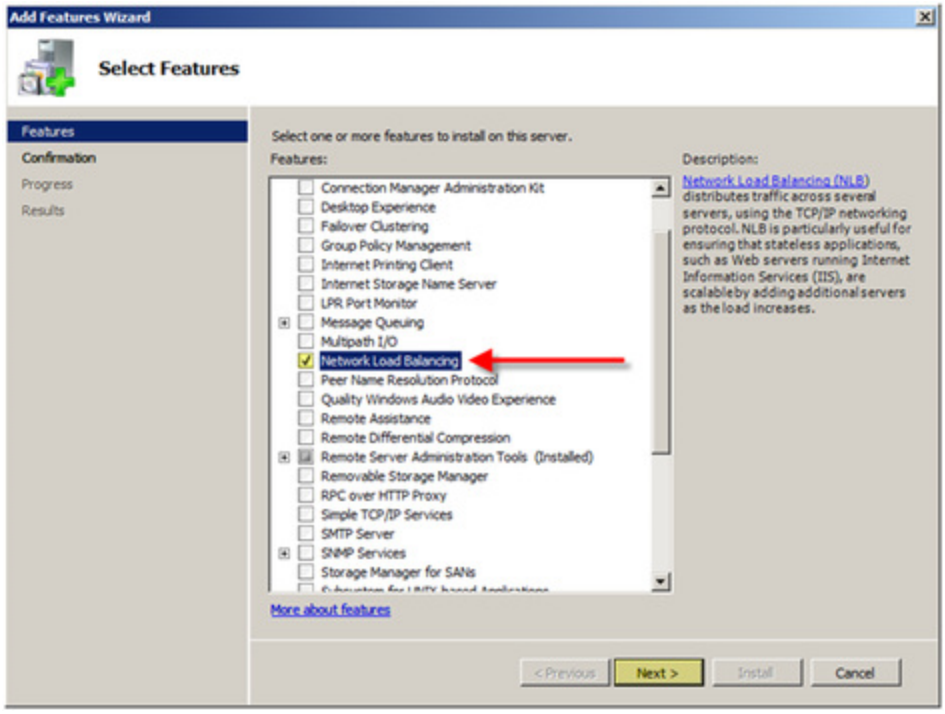
Open Server Manager - you can open it in several different ways in Windows Server 2008. For the quickest way to open Server Manager right-click **My Computer** and choose **Manage**. You can also open it via **Control Panel -> Program and Features -> Turn Windows features on or off**. Opening it from **Server Manager** option under **Administrative Tools** is also an option.

Select **Features** from the Server Manager menu on the left.

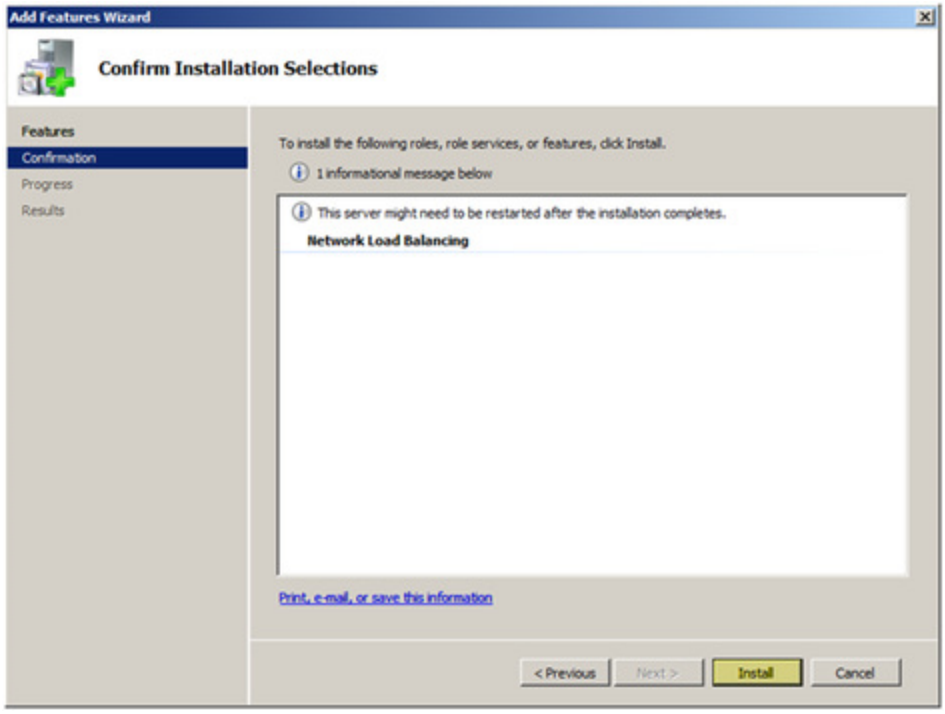
Click **Add Features**.

Select the checkbox next to **Network Load Balancing**

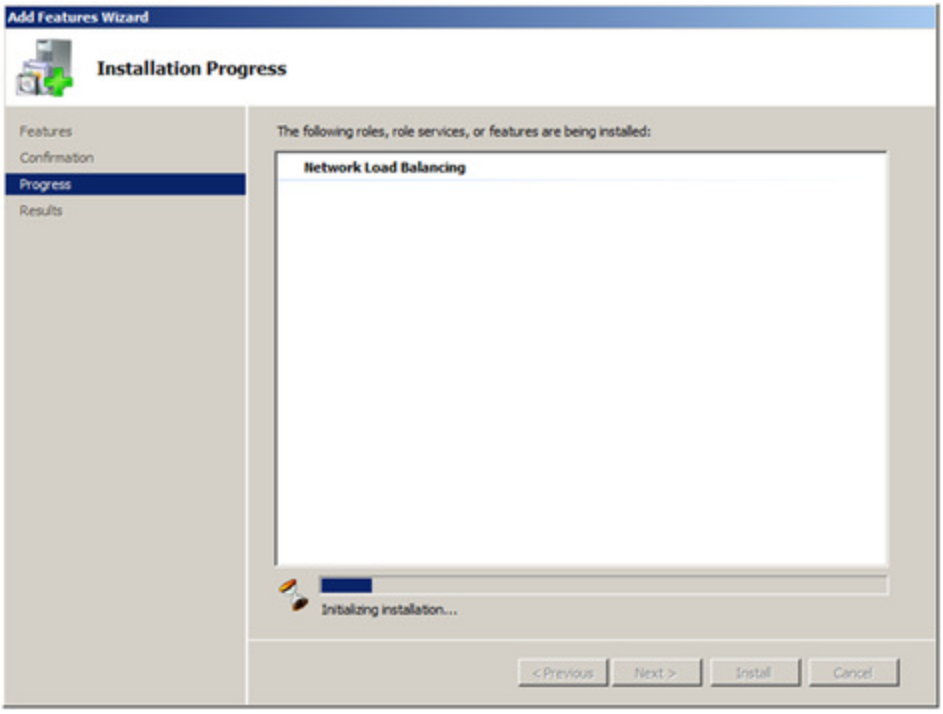
Click **Next**.



Click **Install**.

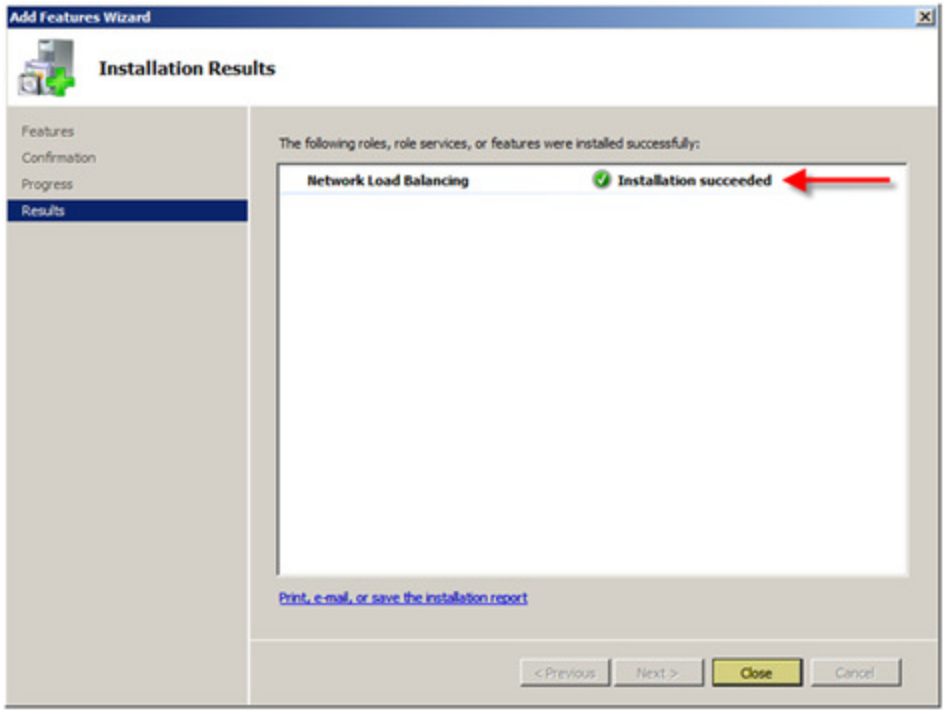


Installation proceeds with copying the required components.



Installation succeeds. It is highly recommended that you repeat this process on all nodes in the NLB cluster at this point before continuing with configuration

Click **Close**.



Note:
Network Load Balancing may also be installed from a command prompt with elevated privileges (right-click on the command prompt in the **Start menu** and select **Run as administrator**) by running the `servermanagercmd -install nlb` command.

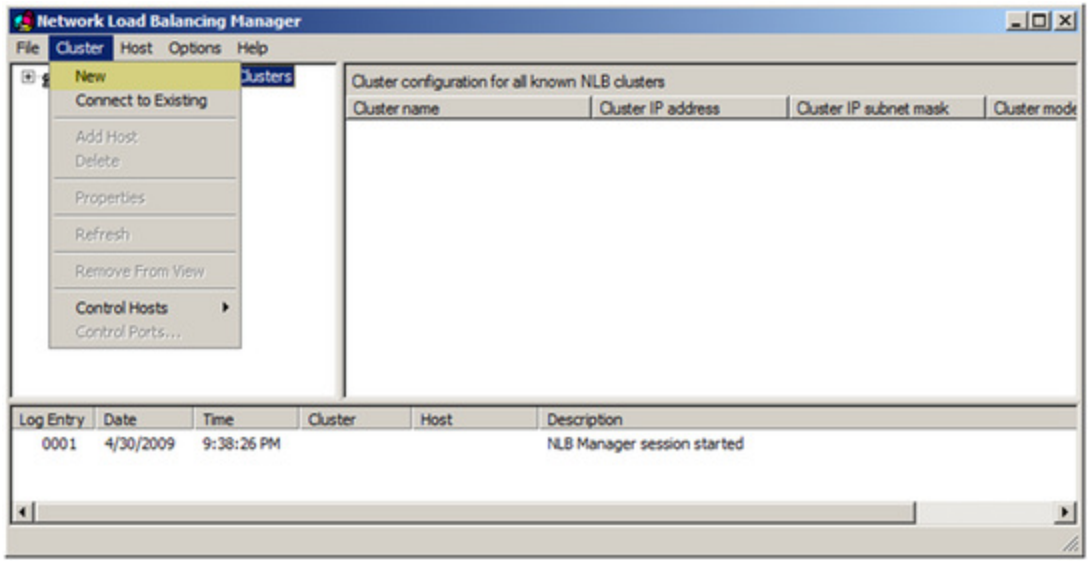
For example:

```
C:\Windows\system32>servermanagercmd -install nlb

......

Start Installation...

[Installation] Succeeded: [Network Load Balancing].

<100/100>

Success: Installation succeeded.
```

Configuring NLB on NODE 1 (PL2008-01)

Network Load Balanced clusters are built using the Network Load Balancing Manager. You can launch it via **Start -> All Programs -> Administrative Tools** menu or from a command prompt by executing `nlbmgr`.

Under the **Cluster Menu** option select **New**.



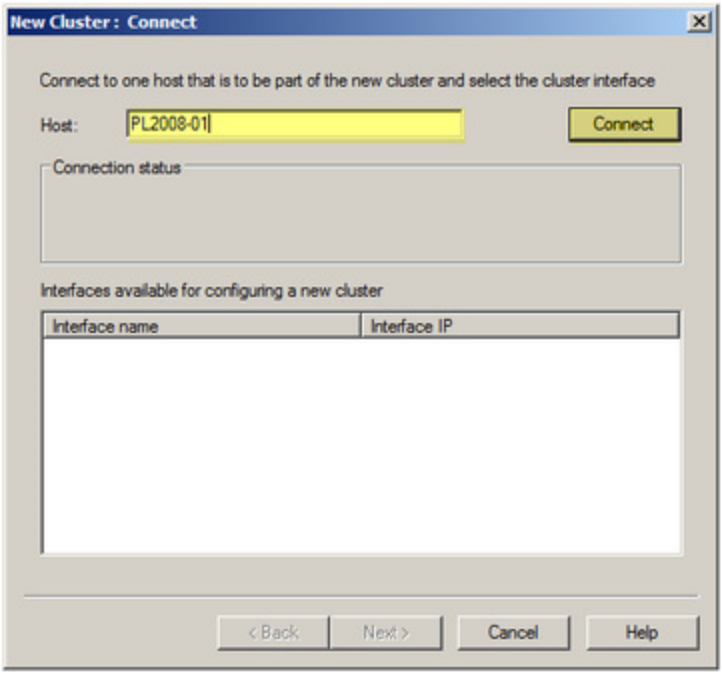
Enter the first node in the cluster which is **PL2008-01**.

Click **Connect**.

Note:
Before starting to install the cluster nodes, make sure

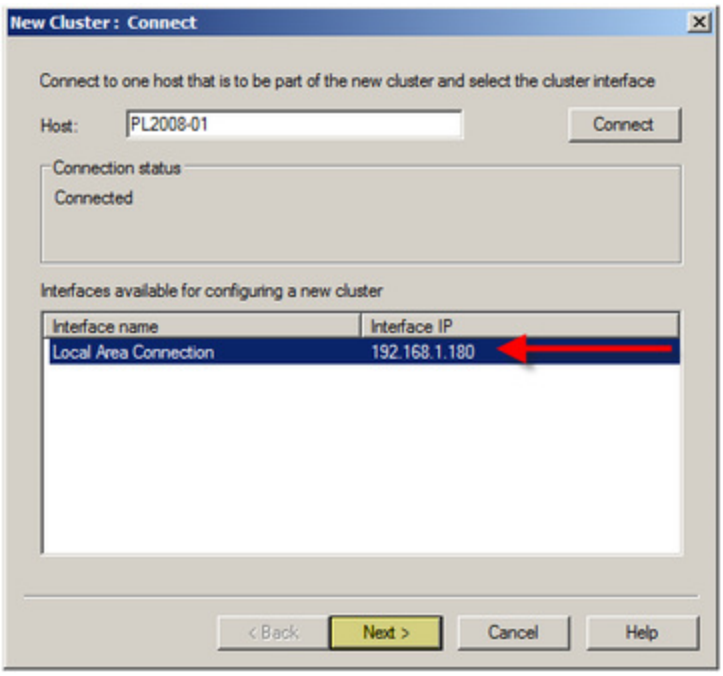
– the IP addresses are fixed (not DHCP enabled) on the 2 NIC cards you need to have in the servers

– the cluster IP address is registered in the network DNS server - in the sample, PL2008-01 and PL2008-02 are registered with the fixed IP of the two servers (192.168.1.180 and 192.168.1.181, respectively)



You can choose which network adapter you want to use; the NIC should be on the same subnet as the other servers in the NLB cluster.

Click **Next**.



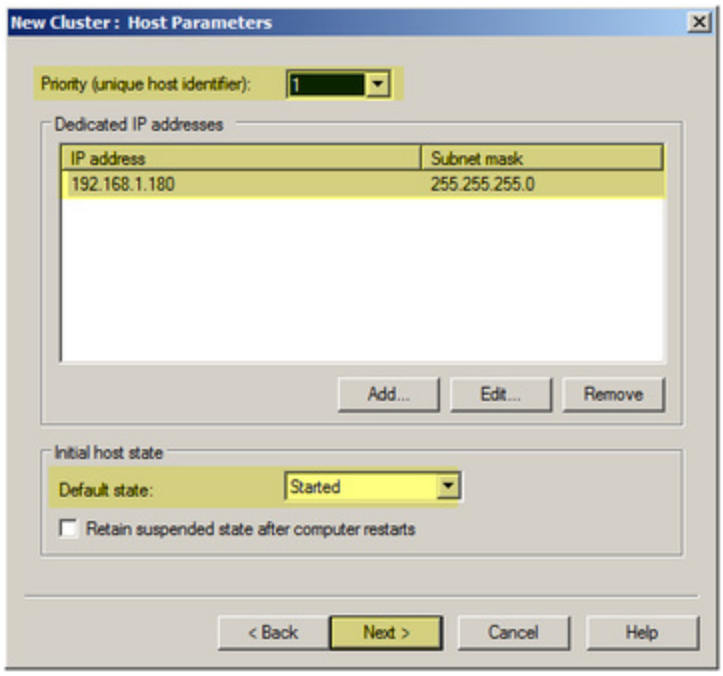
Note:
In this sample only one Interface IP is shown, for the sake of simplicity. For a ShareScan HA setup you need TWO distinct Network Interface Cards on each server, and the Interface shown in this Appendix always means the adapter that is used for the MSNLB cluster. In a real life setup, you should see two adapters, and it is important that you select the proper one as a host adapter of the cluster.

Select **1** as the **Priority ID** from the drop-down list (each node in the NLB cluster should have a UNIQUE ID)

Make sure the correct adapter was selected under **Dedicated IP Address**.

Select **Started** for the **Initial host state** (this tells NLB whether you want this node to participate in the cluster at startup).

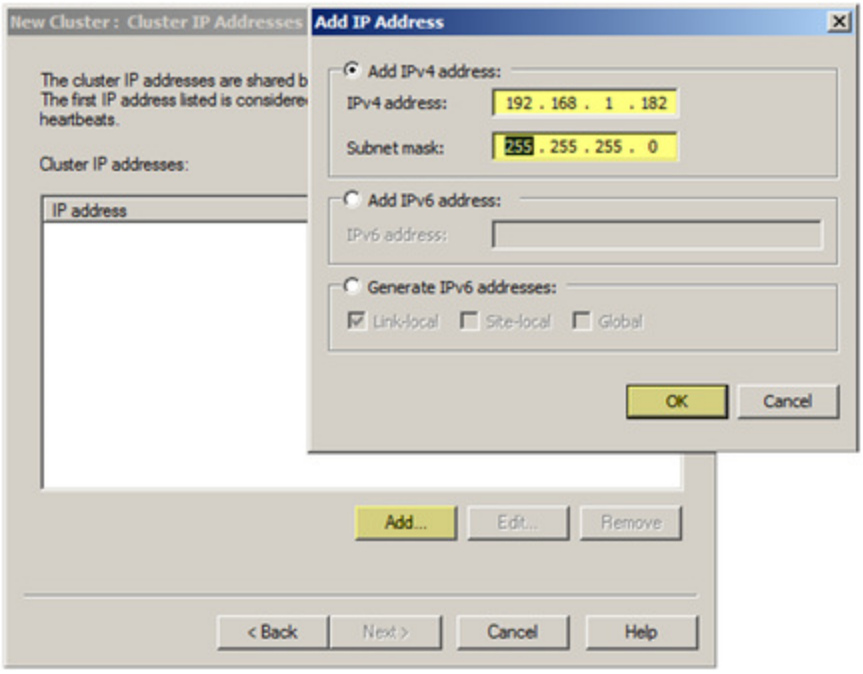
Click **Next**.



Click **Add**.

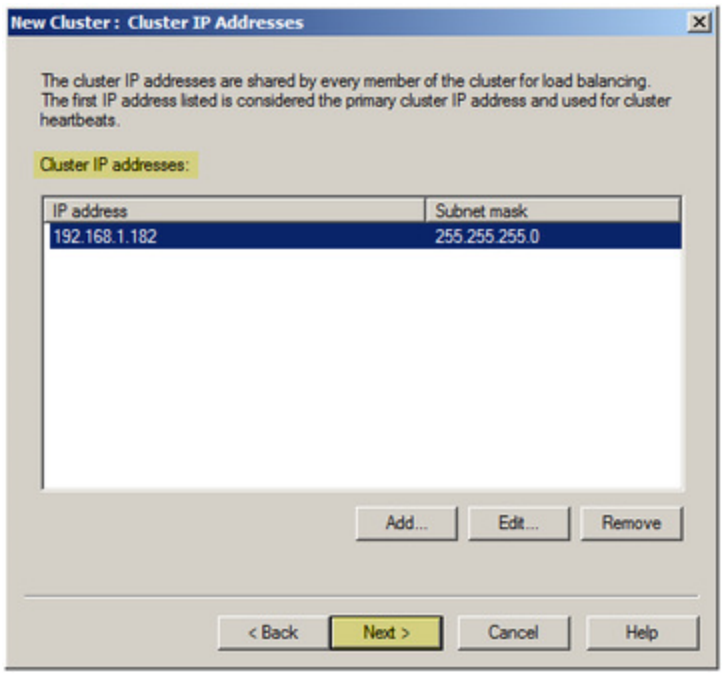
Fill in the **Cluster IP** and **Subnet mask** fields.

Click **OK**.



Make sure the **Cluster IP addresses** are correct. This IP address is used for all traffic from the devices to the ShareScan High Availability cluster.

Click **Next**.

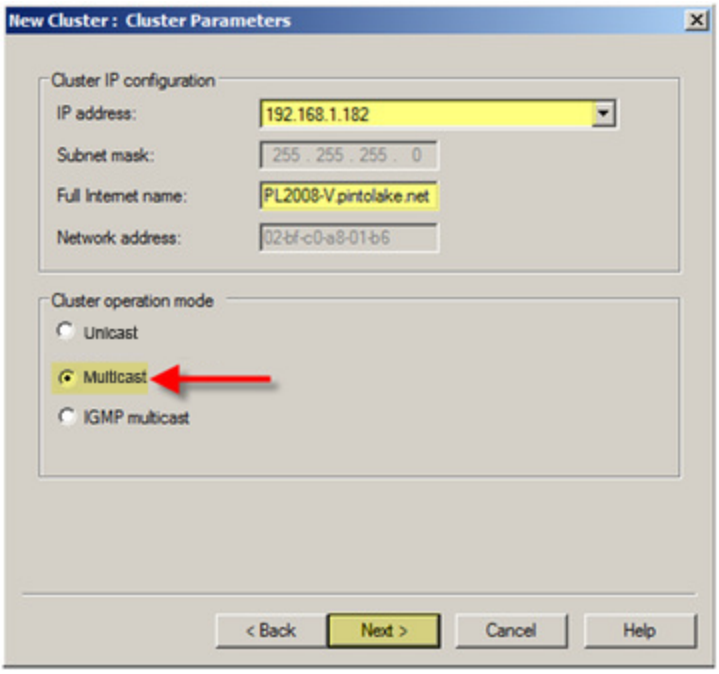


Select the **IP Address** for this cluster from the drop-down list.

Enter the NLB address: **PL2008-V.pintolake.net**

Select **Unicast** or **Multicast** (preferred) as the **Cluster operation mode**, according to your preference – this value is determined by the Network Administrator of the local network system.

Click **Next**.



Unicast vs Multicast

Unicast/Multicast determines the way the MAC address is presented to the routers for the Virtual IP (cluster IP). Multicast is preferred.

In the unicast method

The cluster adapters for all cluster hosts are assigned the same unicast MAC address.

The outgoing MAC address for each packet is modified, based on the cluster host's priority setting, to prevent upstream switches from discovering that all cluster hosts have the same MAC address.

In the multicast method

The cluster adapter for each cluster host retains the original hardware unicast MAC address (as specified by the hardware manufacture of the network adapter).

The cluster adapters for all cluster hosts are assigned a multicast MAC address.

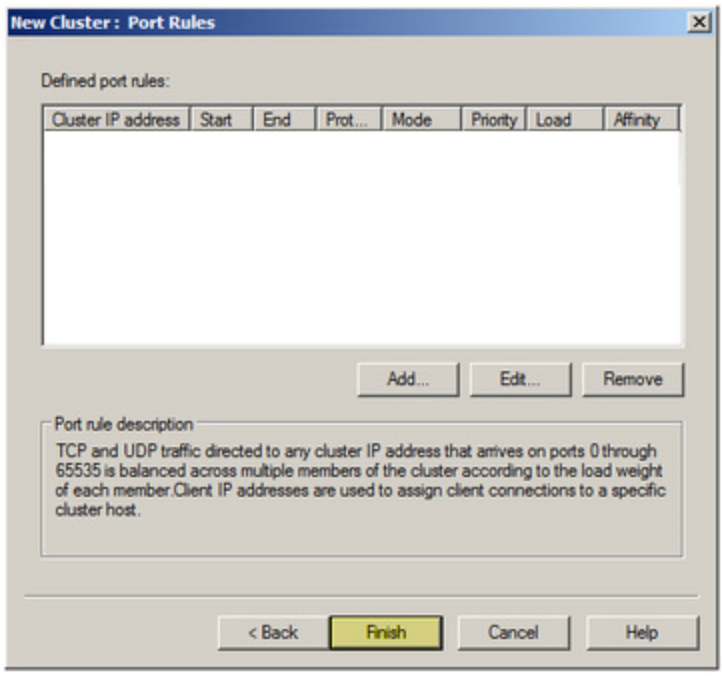
The multicast MAC is derived from the cluster's IP address.

Communication between cluster hosts is not affected, because each cluster host retains a unique MAC address.

See Selecting the Unicast or Multicast Method of Distributing Incoming Requests.

Click **Finish**.

Port rules



The port rules for the different vendors are detailed in the tables below. Each of these port numbers must be added one by one in the **Port rules** dialog (see above).

Xerox (or mixed fleet, including Xerox)

Port	Protocol	Filtering mode	Timeout (in minutes)	Comment
8080	TCP	Single	5	
443	TCP	Single	5	
9325	TCP	None	0	only required for Cost Recovery integration
9425	TCP	None	0	only required for ID Services integration
9599	TCP	None	0	only required for testing/troubleshooting purposes
9600	TCP	Single	5	only required if Canon / Ricoh is also in the fleet

KM (or mixed fleet, including KM)

Port	Protocol	Filtering mode	Timeout (in minutes)	Comment
8080	TCP	Single	5	
443	TCP	Single	5	
9325	TCP	None	0	only required for Cost Recovery integration
9425	TCP	None	0	only required for ID Services integration
9599	TCP	None	0	only required for testing/troubleshooting purposes
9600	TCP	Single	5	only required if Canon / Ricoh is also in the fleet
50002	TCP	Single	5	

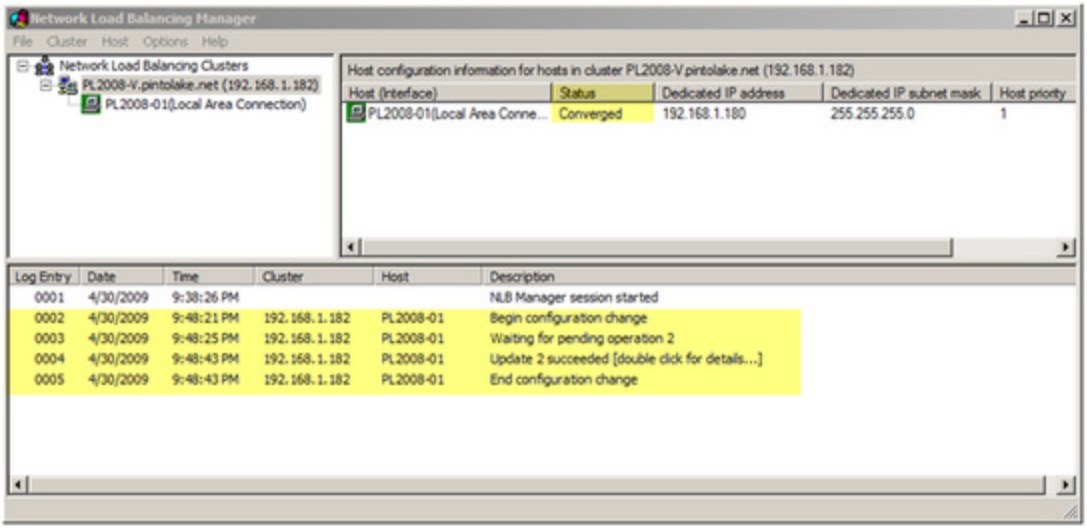
Other (not including Xerox or KM)

Port	Protocol	Filtering mode	Timeout (in minutes)	Comment
8080	TCP	Single	5	
443	TCP	Single	5	
9325	TCP	None	0	only required for Cost Recovery integration
9425	TCP	None	0	only required for ID Services integration
9599	TCP	None	0	only required for testing/troubleshooting purposes
9600	TCP	Single	5	only required if Canon / Ricoh is also in the fleet
9610	TCP	Single	5	only required if Canon / Ricoh is also in the fleet

The NLB Manager lists a number of items which lets you know whether this node successfully converged on your new PL2008-V.pintolake.net NLB Cluster.

Make sure the node's status changes to **Converged**.

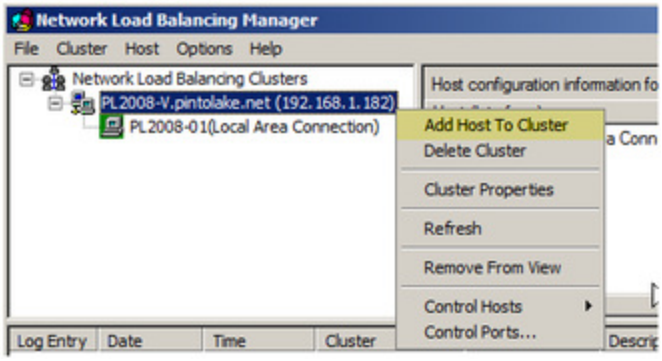
Make sure you see a **succeeded** message in the log window.



Configuring NLB for NODE 2 (PL2008-02)

Perform the NLB setup of the second node (PL2008-02) by logging in to that server. Doing so, you need to connect to the existing cluster first.

Right-click the cluster name **PL2008-V.pintolake.net** and select **Add Host to Cluster**.



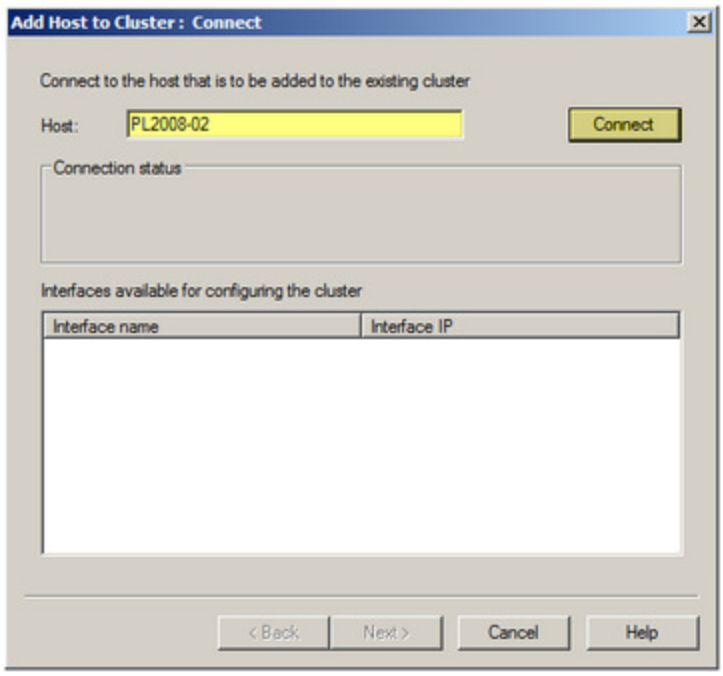
If you cannot see the cluster you have set up successfully on the other node, then most probably:

– there is a network connectivity problem between the two would-be-nodes

– the two would-be-nodes are not on the same subnet

– you are using an account that does not have the proper administrative privileges

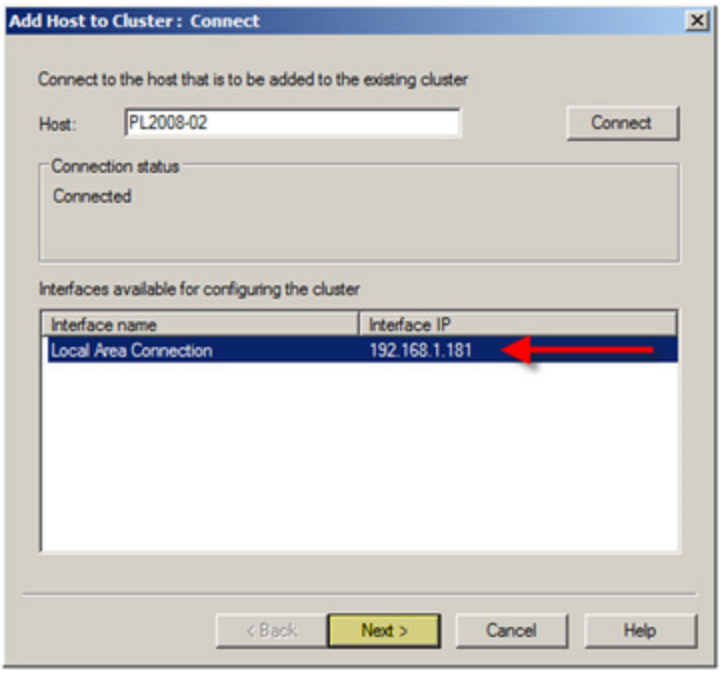
Enter **PL2008-02** in the **Host** field and click **Connect**.



A list of Network adapters shows up.

Select the network adapters that show up on **PL2008-02**.

Click **Next**.



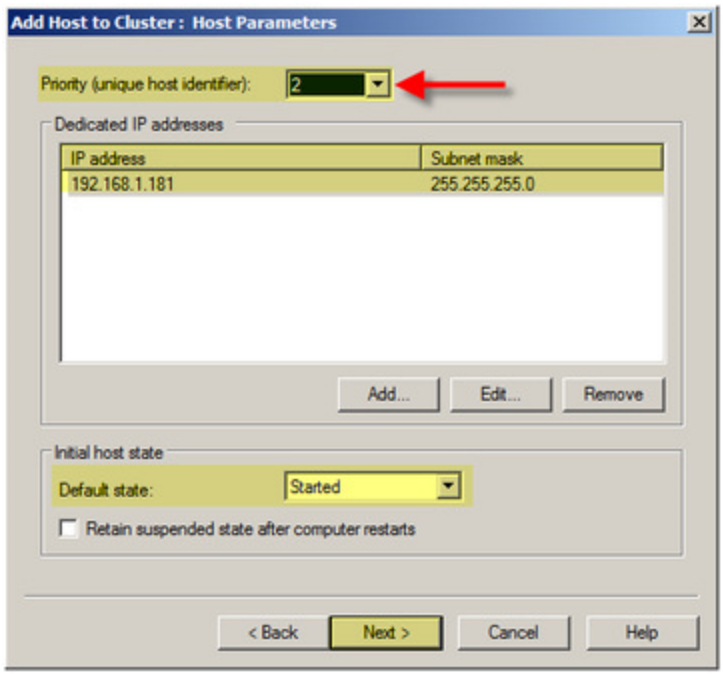
This step is very important; each node in the NLB cluster should have a unique identifier. This identifier is used to identify the node in the cluster.

Select **2** as the **Priority ID** from the drop-down list (each node in the NLB cluster should have a UNIQUE ID)

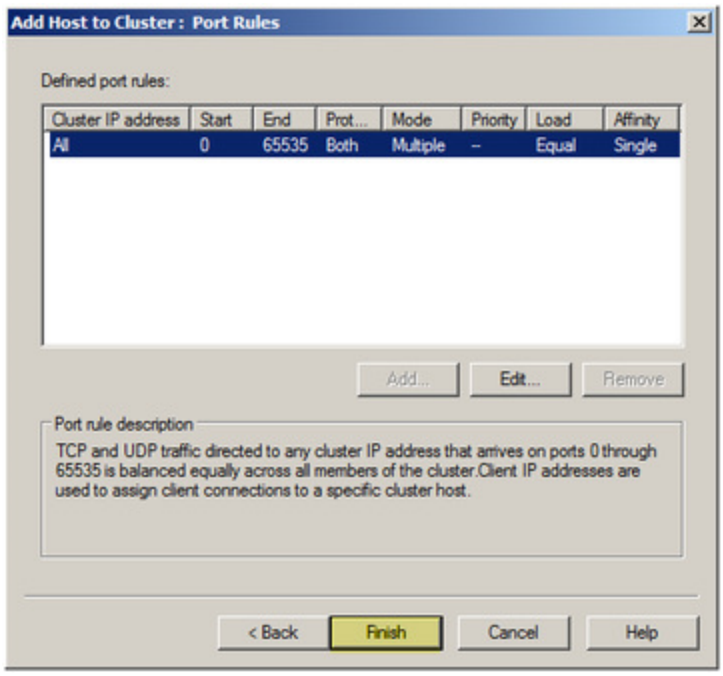
Make sure the correct adapter is selected under **Dedicated IP Address**.

Select **Started** for the **Initial host state** in the drop-down list (this tells NLB whether you want this node to participate in the cluster at startup).

Click **Next**.



Click **Finish**.



For actual port values, see tables above.

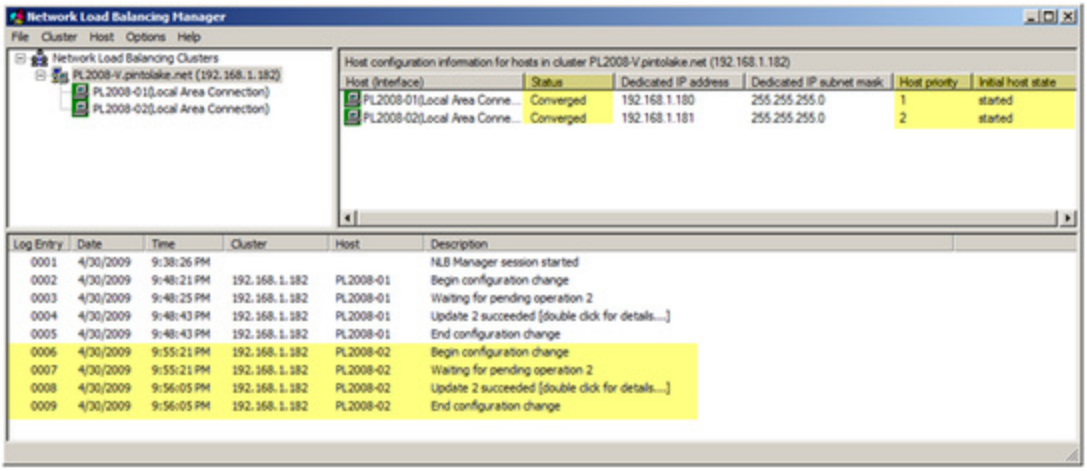
The NLB Manager lists a number of items which let you know that both nodes successfully converged on your new **PL2008-V.pintolake.net** NLB Cluster.

– Make sure that both nodes' status changes to **Converged**.

– Make sure each node has a unique **host priority** ID.

– Make sure each node shows **started** under **initial host state**.

– Make sure you see a **succeeded** message in the log window for the second node.



Testing

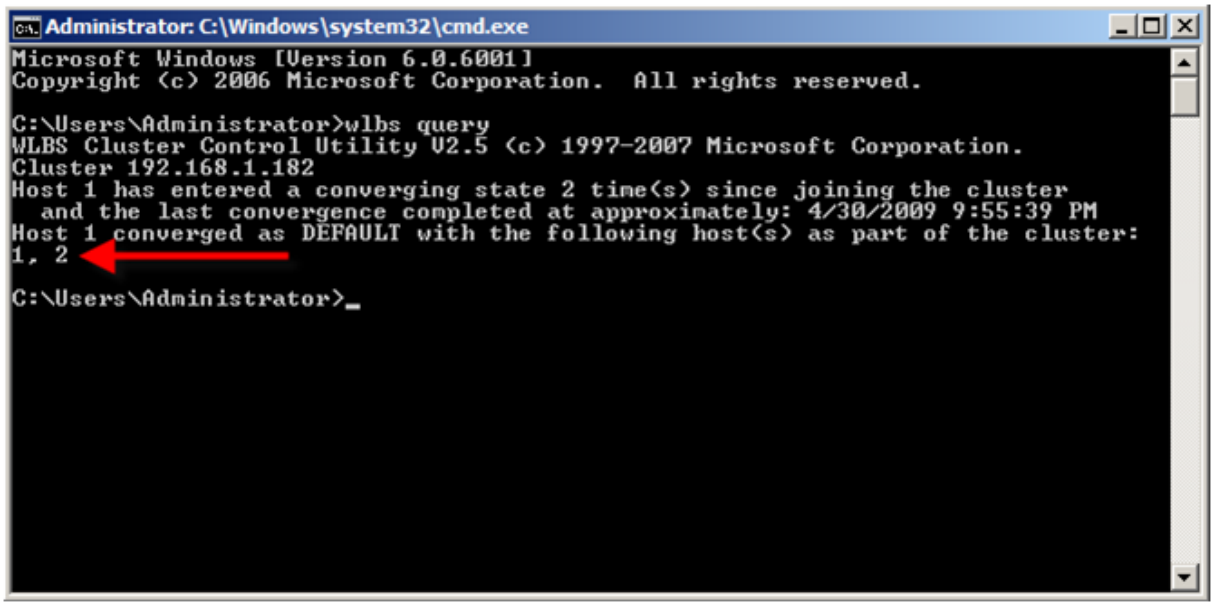
Open the command prompt, type `wlbs query` and then hit **Enter**; as you can see HOST 1 and HOST 2 converged successfully on the cluster.

Ping the virtual IP locally and remotely – you should do this three times from each location. If you cannot ping remotely you may need to add a static ARP entry in your switches and/or routers where the host machines reside.

1 – Both nodes up

2 – Node 1 down

3 – Node 2 down



As a final step, a DNS record might added to allow resolving Network Load Balanced resources via a URI.

After successfully enabling NLB, configuring the cluster IP properly, it is recommended to disable DNS auto-registration.

To do this, open **Control Panel->Network and Sharing Center / Change Adapter settings**. Right-click on the network adapter exposing the cluster IP, click **Properties**. Select **Internet Protocol Version 4 (TCP/IPv4)** on the displayed dialog and click the **Properties** button. Click the **Advanced** button on the displayed dialog and click the **DNS** tab and then uncheck the **Register this connection's addresses in DNS**.

Since ShareScan uses IP (the cluster IP) only, the **Register the cluster IP in DNS** should be removed; it is better not to register the cluster into the DNS, to reduce the unnecessary traffic towards the cluster.