ZENworks 11SP3 Remote Management - Using Join Proxy

February 2014

Novell

Typically, when you want to remote control a device that is in a private network or on the other side of a firewall or router that is behind NAT (Network Address Translation), you need to install a remote management proxy server on the same NAT environment that the device is in. This requires an interface machine. This creates a challenge when a managed device is moved to a new off-site location, because each off-site location is a NAT environment and you cannot have a single remote management proxy for devices across different NAT environments.

ZENworks 11 SP3 introduces a new satellite role called Join Proxy that removes this limitation. The Join Proxy satellite server allows Windows managed devices located in various private networks to be remotely managed.

- Section 1, “Prerequisites,” on page 1
- Section 2, “Configuring the Join Proxy Role,” on page 1
- Section 3, “Remote Controlling the Managed Device - Join Proxy,” on page 3
- Section 4, “Workflow Diagrams,” on page 4
- Section 5, “Legal Notices,” on page 6

1 Prerequisites

Ensure that you have the following:

- A Linux or Windows managed device with public IP address.
- At least one Primary Server to update the Join Proxy connection status in the database.
- The administrator should define certain locations as private.

2 Configuring the Join Proxy Role

In ZENworks, Join Proxy is a role that is by default assigned to Primary Servers; you can also assign this role to Satellites.

You can add the Join Proxy role to a ZENworks 11SP3 Windows or Linux managed device to make it a Join Proxy server in order to perform remote management operations on Windows managed devices that are in a private network.

To configure the Join Proxy Role, complete the following tasks:

- Section 2.1, “Assigning the Join Proxy Role to a Device,” on page 2
- Section 2.2, “Creating Locations,” on page 3
- Section 2.3, “Associating Join Proxy to the Created Locations,” on page 3
- Section 2.4, “Refreshing the Managed Device to View the New Closest Servers List,” on page 3

2.1 Assigning the Join Proxy Role to a Device

In ZENworks Control Center, you first select a device for which you want to assign the Join Proxy role. You can choose either a Primary Server or a Satellite as the Join Proxy.

If you select a Primary Server for the Join Proxy role, there is no need to further configure the server in ZENworks Control Center. However, you can reconfigure the Join Proxy configuration settings by manually editing the `joinproxy.properties` file on the Primary Server device in the following location:

`ZENWORKS_HOME\conf\`

If you plan to use a Satellite, then you need to assign the Join Proxy role to the Satellite server, by using the following steps:

1. In ZENworks Control Center, click *Devices* > *Servers* or *Workstations*.
2. In the Servers or Workstations panel, select the check box for the device that you want to promote to Satellite server.
3. Click *Action* > *Configure Satellite Server*.
4. In the Configure Satellite Server dialog box, select the check box next to *Join Proxy*, then click *Configure*.
5. In the Join Proxy Role Settings dialog box, specify the *Port* on which the Join Proxy listens for a connection. The default port number is 7019.

   NOTE: This is required only if the Join Proxy is running a firewall or is behind a network firewall.

   ---

6. Specify the maximum number of devices that are allowed to connect to the Join Proxy. The default and the maximum value is 1000. Because satellite servers are dedicated to join proxy service, they allow more such connections without being overloaded.

   NOTE: For a Primary server, the default value is 100.To manually increase this limit, update the `joinproxy.properties` file and restart the Join Proxy service. Increasing the join proxy connection limit on a Primary server might overload it when more devices start connecting to the Primary server.

   Though the range for maximum number of connections is from 1- 65535, if you specify a number greater than 1000, the following message is displayed:

   ```
   Maximum number of connections exceeding 1000 may impact the performance of Join Proxy adversely. Do you want to continue anyway?
   ```

7. Specify the frequency interval at which the Join Proxy should check to see whether the devices are still connected to it. The default value is one minute.

   If you specify a lower value in this field, status updates are faster in the database. However, this might result in higher traffic on the network, depending on the number of devices connected to the Join Proxy.

   NOTE: Based on the frequency specified here, Join Proxy will send packets to all the managed devices connected to it, to detect the connection status and update it in the database. This enables remote operators to connect to managed devices through Join Proxy, in order to perform remote sessions on Windows managed devices that are in a private network.

   ---

8. Click *Ok* to return to the Configure Satellite Server dialog box.

For details on Satellite Roles, see“Understanding the Satellite Roles” in the *ZENworks 11 SP3 Primary Server and Satellite Reference*.

2.2 Creating Locations

After assigning the Join Proxy role to the device, you need to create a location by providing a location name and then associating the desired network environments with the location. For details, see "Creating Locations"in the *ZENworks 11 SP3 Location Awareness Reference*.

2.3 Associating Join Proxy to the Created Locations

After creating the location, You also need to configure the Join Proxy Closest Server rules for the location and network environment; tis ensures that the managed device connects to the closest Join Proxy servers defined for it in the location. You need to modify the list of the closest servers for the location or locations in which you want to use a Join Proxy. Typically, at least the unknown location is configured to use a Join Proxy.

For details, see "Adding Closest Servers to Locations" in the *ZENworks 11 SP3 Location Awareness Reference*.

1. In ZENworks Control Center, click the created location, then click the *Servers* tab.
2. Click *Add* in the Join Proxy Servers list.
3. In the Select Join Proxy Servers dialog, click either *Servers* or *Workstations* to select a device or a server. You can choose either a Primary Server or a Satellite as the Join Proxy.
4. Click *OK*.

   The selected servers are listed under Join Proxy servers.
5. Click *Move Up* or *Move Down* as necessary to change its order in the list.
6. Click *Apply*.

2.4 Refreshing the Managed Device to View the New Closest Servers List

You need to refresh the managed device after associating the Join Proxy to the locations; this ensures that the device reads the new closest servers list. You will be able to see the Join Proxy server(s) in the ZENworks Agent status page, if the managed device is already in a location that has a Join Proxy configured.

For details, see "Viewing the Agent's Status" and "Viewing the Closest Server Details"in the *Novell ZENworks Adaptive Agent Help*.

3 Remote Controlling the Managed Device - Join Proxy

When you have enabled Join Proxy and configured the agent to use the Join Proxy in specific locations, you can start remotely managing the devices through the Join Proxy.

1. In ZENworks Control Center, select the device that you want to remote control.
2. Select *Actions* > *Remote Control*.
3. Click the *More Options* link to access the Join Proxy related fields. These are populated by default.

NOTE: If the managed device you are trying to remotely control is already connected to the Join Proxy, then the *Route Through Join Proxy* option is selected by default and the values for the *Join Proxy* and *Join Proxy Port* options are populated.

Alternately, if you are trying to launch a remote operation without selecting a device and have manually entered an IP address /DNS name, then you need to enter the address and port of the Join Proxy.

4 Click *OK* to initiate the remote session.

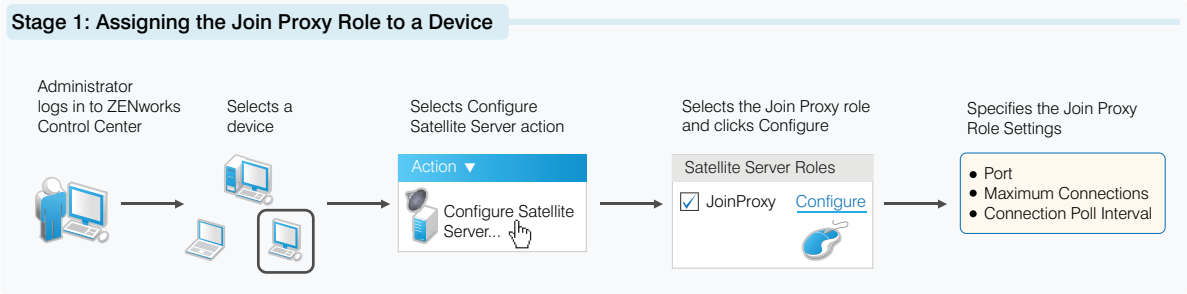
During the connection negotiation, the initial connection is made with the Join Proxy. Thus, by deploying the Join Proxy satellite or Primary Server in the demilitarized zone (DMZ), you can now remotely manage Windows devices regardless of whether they are behind one or more NATs.

4 Workflow Diagrams

- Section 4.1, “Stage 1,” on page 4
- Section 4.2, “Stage 2,” on page 4
- Section 4.3, “Stage 3,” on page 5
- Section 4.4, “Stage 4,” on page 5
- Section 4.5, “Stage 5,” on page 5

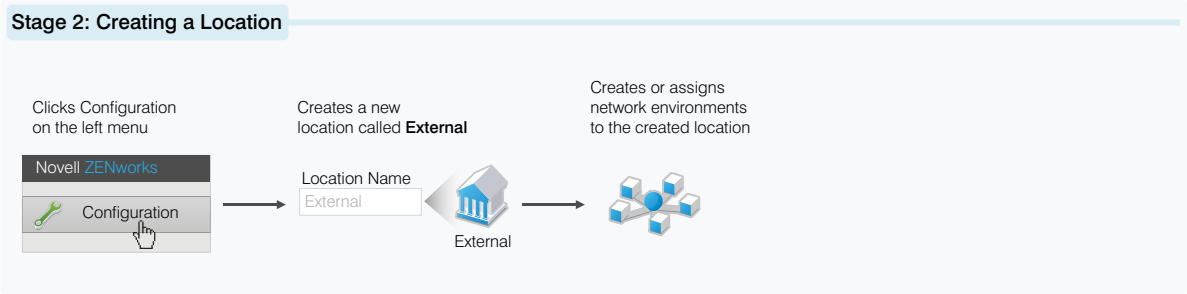
4.1 Stage 1

Assigning the Join Proxy Role to a device



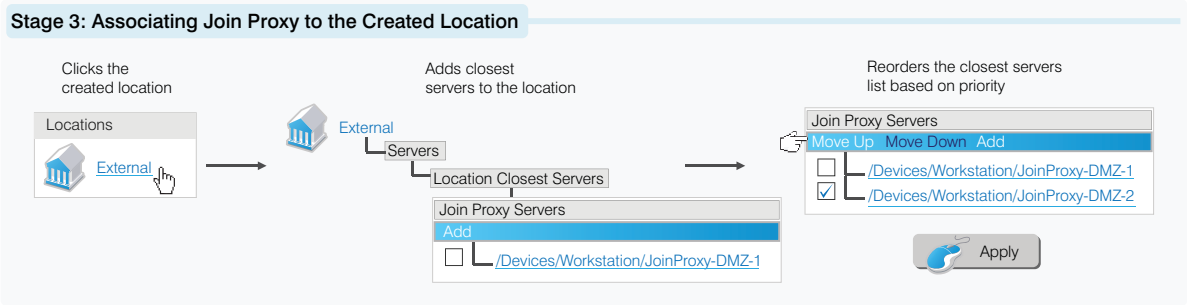
4.2 Stage 2

Creating a Location



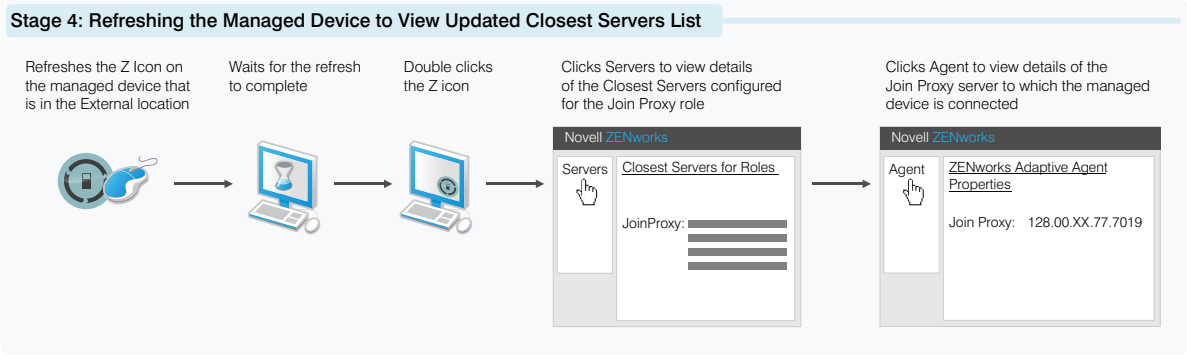
4.3 Stage 3

Assigning Join Proxy to the Created Location



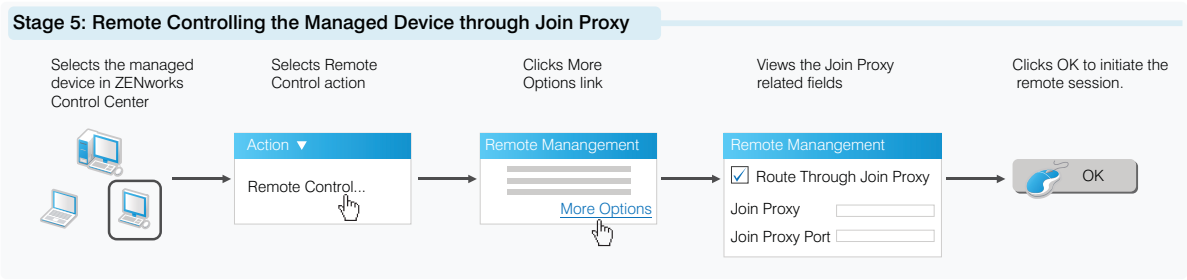
4.4 Stage 4

Refreshing the Managed Device



4.5 Stage 5

Remote Controlling the Managed Device through Join Proxy



5 Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please refer to the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2014 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.