
MSP DEPLOYMENT GUIDE

TRAVERSE 5.5



zyrion
Business Service Assurance

© 2011 Zyrion, Inc. (www.zyrion.com) All rights reserved. Zyrion, Traverse and the Zyrion logo are registered trademarks of Zyrion, Inc. and/or its affiliates in the United States and/or other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners. Zyrion, Inc. reserves the right, at its sole discretion, to make changes at any time in its technical information and specifications, and service and support programs.

ABOUT TRAVERSE

Zyrion's Traverse is a breakthrough Business Service Management application that provides real-time visibility into the performance of IT services. Traverse's innovative Service Container technology enables IT and business personnel to create unique virtual views of discrete business services. Traverse facilitates decentralized remote infrastructure management that is pro-active and preventive rather than reactive, giving all employee levels the control and information they require based on their specific responsibilities and permissions. Traverse provides an easy-to-use Web-based user interface and is a distributed, scalable, real-time, and easy-to-manage platform.

CONTACTING ZYRION

Customer Support

You can reach Zyrion technical support online:

<http://www.zyrion.com/support>

Telephone:

In the US: 877-7-ZYRION (877-799-7644)

Outside the US: +1 408-524-7426

Email:

support@zyrion.com

User Forum

To join our customer-driven user group connecting the worldwide community of Zyrion users, visit the online forum:

<http://community.zyrion.com/>

CONFIDENTIALITY NOTICE

This document contains information that is the property of Zyrion Incorporated. No part of this document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without the expressed written permission of Zyrion.

Contents

1. OVERVIEW AND INSTALLATION	4
1.1. ABOUT THIS GUIDE.....	4
1.2. TRAVERSE ARCHITECTURE	4
1.3. SECURITY MODEL	5
1.4. INSTALLING TRAVERSE AT THE MSP LOCATION (CENTRAL DATA CENTER)	6
2. CREATING NEW USERS	7
2.1. CONFIGURING GROUPS.....	7
2.2. CREATING NEW CUSTOMER USERS	7
3. ADDING A NEW CUSTOMER SITE	8
3.1. CONFIGURING AND INSTALLING THE DGE-X COMPONENT	8
3.2. PROVISIONING CUSTOMER DEVICES.....	9
3.3. PRODUCT BRANDING (THEMES & LOGOS)	9

1. Overview and Installation

1.1. About This Guide

This Deployment Guide contains instructions for installing Zyrion Traverse in a Managed Service Provider (MSP) environment. Users should also review the [‘Traverse 5.5 Evaluation Guide’](#), which provides instructions on exercising key features of Traverse, and includes an evaluation checklist.

The specific instructions in this document allow MSPs to exercise key Traverse functionality to address the following requirements:

- Remote monitoring behind firewalls
- Monitoring customer sites with overlapping IP-addresses
- Supporting multiple organizations (multi-tenancy)
- Custom-branding of UI

1.2. Traverse Architecture

The Traverse system comprises the following three components:

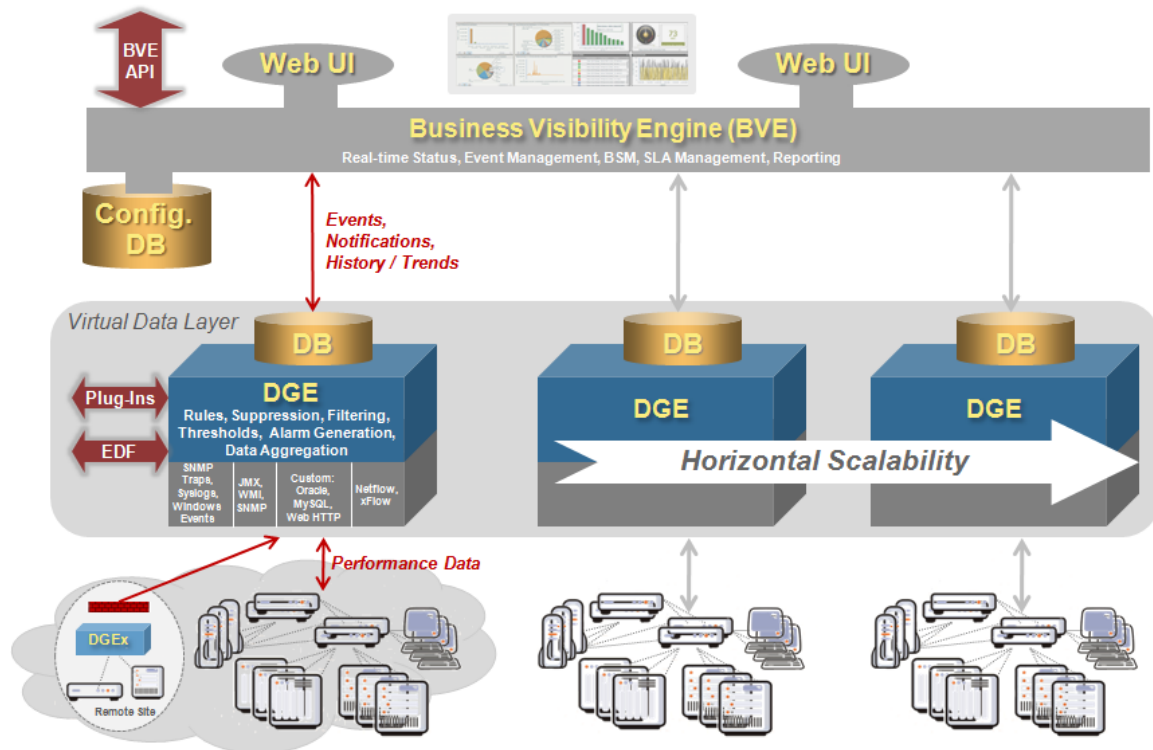
Business Visibility Engine (BVE): An embedded object-oriented database that stores all configuration information, including metadata related to user authentication, devices, tests, thresholds for test results, action profiles and other key information. The BVE FlexAPI, which allows access to the BVE for provisioning and results, also operates on this server.

BVE WebApp: Provides the Web-based user interface into Traverse. It correlates the data from multiple DGEs, and allows end users to look at the real-time status of their devices, add new devices and actions, and execute reports, using a simple Web browser. It manages the distributed databases and distributed processing while generating the real-time reports and graphs. You can have more than one BVE Web application for load sharing.

Data Gathering Engines (DGE): Performs the actual polling of data, receives SNMP traps, generates alarms based on thresholds, and does the aggregation of data in real time. DGEs should be located as close as possible to the devices being monitored to reduce wide area network traffic. The DGEs can be geographically dispersed or you can have multiple DGEs in the same location to distribute the load across different physical servers. When you have multiple DGEs in the same location, the system automatically provisions new devices onto the DGE with a lower number of devices.

DGE Extensions: DGE-extensions are software components that site behind firewalled sites and store-and-forward performance data to an upstream DGE over a secure SSL connection. The advantage of using DGE-extensions in

MSP environments is that all data transmission is outbound from the DGE-extension and it can be placed inside a customer network behind a firewall, and no firewall ports need to be opened up on the customer side. Additionally, these DGE-extensions are also designed to handle overlapping IP addresses and operate behind NAT firewalls. You can add custom monitors to a DGE-extension (however, you cannot add a custom action script to a DGE-extension and all the notifications are triggered at an upstream DGE).



1.3. Security Model

Traverse has a robust and flexible federated user security model which provides read-only or read-write privileges for end users depending on your requirements as an MSP. A full description of the security model is described in the Traverse User Guide, but the most common deployment scenario for MSP's is described below.

The following example assumes that the reader is familiar with the concepts of Admin-Users, Departments, and End-users as described in the Traverse User Guide.

Your staff (assuming you are the Managed Service Provider) should belong to an Admin-Group (called msp-group), and an end user department should be created for each of your customers. This will isolate each of your customers' devices automatically so that even if you give full login access to each of your customers, the

system will automatically prevent them from seeing each other's data unless the data is "exported" to the other user intentionally.

NOTE: Create a Department for each end Customer. If you want to create intermediate level MSPs, you need to create Admin Groups.

1.4. Installing Traverse at the MSP Location (Central Data Center)

Download and install the core Traverse software on your network first. You can install the BE and the DGE on the same physical server, or on two separate servers for scalability. The hardware specifications are listed on the Zyrion support site.

Note, all software and documentation files are directly downloadable from the Zyrion support web site at <http://www.zyrion.com/support>. For hardware and software requirements and installation and update instructions, see the Traverse 5.2 User Guide.

When installing Traverse 5.1 at your central site (data center), choose the "Complete Application" option. This will install both the BVE as well as the DGE components on a single server. If you want to install the DGE on a separate server, run the installer on the DGE and select 'Install DGE only' during the install process.

You will also need to enable the following ports on your firewall to allow incoming connections from the DGE-extensions at the customer site. You can allow all incoming connections or explicitly list the IP address of each of your customer's DGE-extensions depending on your security policies.

Port	From	To
TCP/7651	DGE-x	BVE
TCP/7652	DGE-x	BVE
TCP/7653	DGE-x	BVE
TCP/9443	DGE-x	BVE

2. Creating New Users

2.1. Configuring Groups

1. Log in as "superuser" (default password "zyrion")
2. Navigate to "Superuser" -> User Class and click on "Update" for the Default User Class
3. Change the name to be "Default Customer Class" and click on Update User Class. (Alternatively, you can create a new User Class instead of renaming the existing one)
4. Navigate to Superuser -> Admin Class and create a new Admin Class called "MSP Class"
5. Now click on "User Class Mappings" and then "Assign User Class to Admin Class". Select the default grid that is presented and click on 'Update Privileges" button.
6. Navigate to "Administration" -> Departments and click on 'Create new Admin Group". Create a new admin group called 'MSP Group' belonging to the "MSP Class"
7. Create new users in the 'MSP Group' for each of your staff by going to Administration -> Departments and clicking on 'Create User'

At this point, you have the basic security model setup with all your staff belonging to 'MSP Group'

2.2. Creating New Customer Users

You can either give your end customers a full read-only login account so that they can get read-only access to all the data in their 'department', or else you can create a special URL so that they can log in and only see a single page.

1. In the central MSP Traverse installation, log into the Web Application as "superuser" with default password "zyrion"
2. Navigate to Administration -> Departments and then click on "Create New Department"
3. Give a meaningful name to the Department (such as Customer X). A default user will automatically be created.
4. If you want to create a 'read only' account for your customer, click on 'Create User' and add a new user (preferably use the user's email address as the login).

Creating URL with auto-login: You can create a URL with an encrypted username and password to do autologin for a single Traverse page by using the Auto-Login URL generator at www.zyrion.com/support/tools/urlgen/

3. Adding a New Customer Site

3.1. Configuring and Installing the DGE-X Component

At the central MSP Traverse installation, Navigate to Superuser -> DGE Mgmt. Create a new DGE-extension for the end customer using the following steps:

- Click on "Create New DGE Extension"
- Provide a unique name like "dgex-customerA"
- Give a suitable Description field to identify the customer for example
- Select the upstream DGE name from the drop down list. In most cases if you have only one DGE, it will be "localhost".
- Provide the IP address of the upstream DGE from the DGE-extension's network. As an example, for a DGE-x on the same internal network as the DGE, the IP address might be 192.168.1.2 but for a DGE extension at a remote customer network, this would need to be the externally visible IP address of the DGE (e.g. 128.121.x.y)
- Click on "Create DGE Extension"

The screenshot shows the 'CREATE DGE EXTENSION' form within the Superuser interface. The navigation bar includes STATUS, DASHBOARD, REPORTS, ADMINISTRATION, and SUPERUSER. Below the navigation bar, there are links for DGE MGMT, HEALTH, ADMIN CLASS, USER CLASS, and GLOBAL CONFIG, along with a 'Logged in: superuser' indicator. The form itself has the following fields:

- * Unique Name:
- * Description:
- * Upstream DGE Name:
- * Upstream DGE IP Address:
- * Soft Limit:
- * Hard Limit:

At the bottom of the form are two buttons: 'Create DGE Extension' and 'Reset'.

Then configure the DGE-X at the end customer site, using the following steps:

1. Run the Traverse DGE-X installer at your customer location and choose the "Data Gathering Engine" option. You will need to give the same name for the DGE-extension which you entered in the step above (dgex-customerA). You will also need to enter the IP address of the central BVE.
2. At the end of the installation, the server will reboot if running on Windows and on reboot, the DGE extension service will automatically start and establish a connection to the upstream BE and DGE. On Linux or Solaris

platforms, just start the DGE extension by running the startup script under `traverse/etc/traverse.init start`

3. On the central BVE web application, log in as superuser and navigate to Superuser -> Health to verify that the new DGE-extension is communicating with the central BVE & upstream DGE.

3.2. Provisioning Customer Devices

You are now ready to provision devices for this customer.

1. Represent a user in this customer's department
2. Create a new device by navigating to Administration -> Devices -> Create a Device
3. Provide a suitable device name, IP address or FQDN and other information
4. For "Create in Location", you must select the Unique Name for the customers DGE extension "dgex-customer A"

The newly created device will automatically be monitored from the DGE-extension specified and periodically transfer the data over an SSL connection to the upstream DGE.

The DGE-extension is also capable of handling traps and logs and provides functionality similar to a DGE for filtering.

3.3. Product Branding (Themes & Logos)

If the provided Traverse license permits you to change the logo, you can set the logo and theme and custom URL for each of the customers (and intermediate MSPs) by logging in as Superuser and going to Administration > Departments and selecting Themes from the Modify column.