RN

Precise 9.9.0 release information

Introduction

Introducing Precise 9.9.0

Precise 9.9.0 is a complete Precise version, which includes and provides enhancements and fixes for Precise version 9.8.x. This document describes the new features introduced, the technologies supported, and the issues resolved by this version.

Installing Precise 9.9.0

Precise 9.9.0 can be installed in the following ways, depending on the currently installed Precise version:

- If this is the first time you are installing Precise, install Precise version 9.9.0 as described in “Clean installation of the Precise Framework” in the *Precise Installation Guide*.
- If Precise version 9.8.0 is currently installed, upgrade directly to version 9.9.0 as described in “Upgrading Precise” in the *Precise Upgrade Guide*.

New Features and Enhancements for Precise 9.9.0

Support for the Precise framework and monitored instances (Web, J2EE, SQL Server, Network, and OS) on Microsoft Azure environments

Support is added for the Precise framework and monitored instances (Web, J2EE, SQL Server, Network, and OS) on Microsoft Azure environments.

Support for the Precise framework and monitored instances (Web, J2EE, Oracle, Network, and OS) on Amazon AWS environments

Support is added for the Precise framework and monitored instances (Web, J2EE, Oracle, Network, and OS) on Amazon AWS environments.

Support for monitoring Tuxedo 12.2.2 on Linux

Support is added for monitoring Tuxedo 12.2.2 on Linux.

Support for monitoring Peoplesoft 8.56 on Linux

Support is added for monitoring Peoplesoft 8.56 on Linux.

Support for monitoring SQL Server 2017

Support is added for monitoring SQL Server 2017.

New AdminPoint user interface

Precise 9.9.0 comes with a new Admin Point user interface based on modern UI technologies and is supported on Chrome, Firefox, and Internet Explorer browsers. As of 9.9.0, the new GUI would co-exist with the existing GUI and is available at the following URL:

http://<hostname>:<port>/precise

This new UI is supported on browsers Chrome, Firefox, and IE 10 and higher.

Allows monitoring of SQL Server instances when using TLS 1.2

Enhancements in this version allow monitoring of SQL Server instances when using TLS 1.2. For more information about enabling this feature, see Monitoring SQL Server instances with TLS 1.2 enabled.

Allows users to set up Precise listeners and Oracle agents on some Linux systems

Enhancements in this version allow users to set up Precise listeners and Oracle agents on Linux systems without 32-bit GLIBC libraries.

Resolved Issues

- Wrong buffer gets (avg) info in Oracle 12.2.0.1 on Linux (PRECISE-18988)
- Activity tab is displaying the Object ID when selecting the Objects option in Oracle 12.2.0.1 monitoring in AIX machine (PRECISE-18986)
- Import from Precise Portlets not working in Precise V970 (PRECISE-18831)

Known Issues

- The Precise Focal Point needs to be restarted after an upgrade if using remote instances. This would also need starting of the SQL agents after the Focal Point restart.
- When an Oracle monitoring instance is created immediately after framework installation, errors are sometimes seen in Oracle warehouse processes (Under **Adminpoint > Warehouse Processes**). In such cases, a restart of the Oracle Focal Point and PMDB focal point fixes the problems.
- After a fresh install or upgrade, it is required to restart the Precise GUI service before using the Custom Portal.

- There is an issue with injdn.dll and injdn_x64.dll on Windows Server 2008 R2 with .NET monitoring. When a .NET instance is installed on Windows Server 2008 R2, a “Bad Image” error pops up. The problem can be resolved by installing a Windows security update on the machine. The security update can be downloaded from https://technet.microsoft.com/en-us/library/security/3033929.aspx

- One of the binaries from the Precise 9.9.0 installer (psin_ba_WIN.exe) shows up as a threat under AVG antivirus. This is a false positive with AVG and does not cause any problems. It might have to be whitelisted when using AVG as antivirus.

Monitoring SQL Server instances with TLS 1.2 enabled

Requirements:

1. The default SQL Server ODBC driver should be installed on the monitored machine where TLS 1.2 is enabled.

2. FIPS should be enabled on the monitored machine where TLS1.2 is enabled. This is to be done using the following steps:

    a. Press Widows Key + R to open the Run dialog.

    b. Type `gpedit.msc` into the Run dialog box (without the quotes), and then press **Enter**.

    c. In the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.

    d. Double-click the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting in the right pane.

    e. Set the setting to **Enabled**, and then click **OK**.