eTrust Vulnerability Manager

Release Summary

r8.3.14

CA Product References

This document references the following CA products:

- eTrust® Vulnerability Manager (eVM)
- CA Desktop and Server Management (DSM)
- CA Desktop Management Suite for Windows (DMS)
- CA Unicenter® Software Delivery (USD)

Contents

Chapter 1: Setup Requirements

This section contains the following topics:

System Requirements

The eTrust Vulnerability Manager software is pre-installed on the platforms listed under Operating System Support. You can access the eTrust Vulnerability Manager application using Internet Explorer version 6.0 or higher or Mozilla version 1.4 or higher.

eTrust Vulnerability Manager must have Internet connectivity to obtain content and code updates, which are a critical part of the eTrust Vulnerability Manager solution.

eTrust Vulnerability Manager must run on a TCP/IP network with sufficient bandwidth to support 100 megabit network transfer speeds.

Operating System Support

The eTrust Vulnerability Manager software is pre-installed on an enterprise appliance and on a standard appliance. A description of the respective platforms follows.

- Enterprise Appliance (eVM3803) - Windows Server 2003 operating system, 64-bit edition, with a SQL Server 2005 database. The 64-bit architecture is based on Explicitly Parallel Instruction Computing (EPIC), and supports the Intel Itanium processor family.
- Standard Appliance (eVM1400S or eVM1400I) - Windows 2000 Server SP4 with a SQL Server 2000 SP4 database.

CA Vulnerability Manager supports the following agents on UNIX, Linux, and Windows assets:

- UNIX
  - IBM AIX 5.1, 5.2, 5.3 (POWER with RPM)
  - HP-UX 11.00, 11i (11.11), 11.23 & 11.31 (IA and RISC, 32-bit)
  - Novell Netware 6.5 SP3
  - Sun Solaris 8, 9 & 10 (UltraSPARC, 32-bit, 64-bit)
- Linux
  - Red Hat Linux 8.0 (Intel, 32-bit)
  - Red Hat Linux 9.0 (Intel, 32-bit)
  - Red Hat Enterprise Linux AS 3.0 (Intel X86 Compatible, 32-bit)
  - Red Hat Enterprise Linux ES 3.0 (Intel X86 Compatible, 32-bit)
  - Red Hat Enterprise Linux AS 4.0 (Intel X86 Compatible, 32-bit)
  - Red Hat Enterprise Linux ES 4.0 (Intel X86 Compatible, 32-bit)
  - Red Hat Enterprise Linux Server 5.0,
  - Red Hat Enterprise Linux Desktop 5.0.
  - SuSe 8.2 (Intel, 32-bit)
  - SuSe 9.0 (Intel, 32-bit)
  - SuSE Linux 10.0, 10.1x86
  - SuSE Linux Enterprise Server 9 x86
  - SuSE Linux Enterprise Server 10 (SLES10)
- Windows
  - Microsoft Windows 2000 Professional SP3, SP4 x86 32
  - Microsoft Windows XP Professional SP1 and SP2 x86 32
  - Microsoft Windows XP SP2 Professional 64-Bit Edition x64 64
  - Microsoft Windows 2000 Server SP3, SP4 x86 32
  - Microsoft Windows 2000 Advanced Server SP3, SP4 x86 32
  - Microsoft Windows Server 2003 Standard, Enterprise & Web Edition SP1 & SP2 x86 32
  - Microsoft Windows Server 2003 Standard, Enterprise & Web Edition SP1 & SP2 x64 64

Chapter 2: Changes to Existing Features

The following sections describe changes to existing features made to eTrust Vulnerability Manager for release r8.3.14.

Note: No new features have been added to eTrust Vulnerability Manager for release r8.3.14.

This section contains the following topics:

Integration with DSM r11 Remediation Servers (see page 9)

Integration with DSM r11 Remediation Servers

A Remediation Server is a server that delivers remediations to clients with a Remediation Agent. Remediation Servers enable you to remediate the assets on which vulnerabilities exist.

Previously, eTrust Vulnerability Manager integrated with Unicenter Software Delivery (Unicenter SD) servers. With this release, the integration functionality has been extended to include DSM r11 servers.

The integration with remediation servers differs between the enterprise appliance (eVM3803) and the standard appliance (eVM1403S) in terms of the interface and the need for the VM Service on assets being remediated by a USD Remediation Server or a DSM Remediation Server.

For purposes of these differences, consider the following two setups:

- The Enterprise Appliance runs a 64-bit Windows Server 2003 operating system with a Microsoft SQL Server 2005 database.
- The Standard Appliance runs a 32-bit Windows Server 2003 operating system with a Microsoft SQL Server 2005 database.

You can add the following types of Remediation Servers:

- USD 4.0 SP1 (or higher) Remediation Server, a component of CA Unicenter Software Delivery (USD)
- DSM r11 (or higher) Remediation Server, a component of CA Desktop Management Suite for Windows

The Remediation Server integration enables you to remediate assets on which you install the associated Remediation Agent. The USD 4.0 Remediation Server lets you remediate vulnerabilities on assets that have a USD Agent installed. The DSM r11 Remediation Server lets you remediate vulnerabilities on assets that have a DSM Agent installed. Target assets require the addition of the VM Service only when used with the standard appliance. On the enterprise appliance, the VM Service is optional for remediation.

Integrate an Enterprise Appliance with Remediation Servers

You can use existing USD 4.0 SP1 servers and/or existing DSM r11 servers as remediation servers. That is, you can invoke remediations from the eVM appliance to remediate assets that qualify for remediation deployment. To qualify for remediation deployment with a given USD Server, assets must be registered with that server and be running the USD Agent. To qualify for remediation deployment with a given DSM Server, assets must be registered with that server and be running the DSM Agent.

To integrate an eTrust Vulnerability Manager enterprise appliance with remediation servers

1. Select the Integration tab and click Remediation Servers.
2. From the Server Type dropdown list, select one of the following server types:
   - USD 4.0
   - DSM r11
3. If you selected USD 4.0, complete the integration information as follows:
   a. Enter the IP address or host name of the USD server to add.
   b. Enter the valid User ID of for this server.
   c. Enter the password for this server.
   d. Click Add.

      The server you identified is configured as a remediation server. Your specifications are added to the server list at the bottom of the page. When you select Tasks, Remediation View, Qualifying Assets and click Search, the configured server location appears in the results for each asset that is registered with that server.

4. If you selected DSM r11, complete the integration information as follows, using examples that follow this procedure as guidelines:

   a. Select the security provider, or authentication mechanism, for the server you are configuring.

      Note: For details, see the *DSM Implementation Guide* section on DSM Security Features.

   b. Enter the IP address or host name of the DSM server to add.

   c. Enter the User name for this server.

   d. Enter the security authority in the Security Authority text box. This is typically the domain part of the domain\userName you entered in the User text box.

   e. Enter the password for this server

   f. Click Add.

      The server you identified is configured as a remediation server. Your specifications are added to the server list at the bottom of the page. When you select Tasks, Remediation View, Qualifying Assets and click Search, the configured server location appears in the results for each asset that is registered with that server.

Note: You can add up to 50 servers of the same or different types.

Example - LDAP Configuration

When integrating with a DSM r11 Remediation Server where the security provider is ldap, use the following example as a guideline for entries:

- Hostname: svm-2k3-7
- Username: *username*@*company*.com
- Security Authority: *company*.com
- Password: *domain_password*

Example - LDAPS Configuration

When integrating with a DSM r11 Remediation Server where the security provider is ldaps, use the following example as a guideline for entries:

- Hostname: svm-2k3-7
- Username: uid=*username*,ou=people,dc=dsm,dc=com
- Security Authority: uni999999-20.*company*.com
- Password: "*password*"

Example - NDS Configuration

When integrating with a DSM r11 Remediation Server where the security provider is nds, use the following example as a guideline for entries:

- Hostname: uni999999-119
- Username: cn=vak.ou=users.o=unisvmnovell1
- Security Authority: unisvmnovell1
- Password: ca12#

Example - WINNT or UNIXL Configuration

When integrating with a DSM r11 Remediation Server where the security provider is winnt or unixl, use the following example as a guideline for entries:

- Hostname: *machine_name*
- Username: Administrator
- Security Authority: *machine_name*
- Password: *password*

Integrate a Standard Appliance with Remediation Servers

The eTrust Vulnerability Manager standard appliance includes an embedded Remediation server. This embedded USD remediation server lets you invoke remediations from the eVM appliance to remediate assets that qualify for remediation deployment. You can use the embedded remediation server or configure up to ten existing remote remediation servers.

That is, you can set up your appliance to send remediation requests in the following ways:

- Enable the internal USD remediation server. When enabled, no remote remediation servers may be used. To qualify for remediation deployment with the embedded remediation server, assets must be running both the USD Agent and the VM Service and must be registered to the embedded remediation server.
- Do not enable the internal USD remediation server. Instead, configure one or more USD r4.0 SP1 remediation servers that already exist on your network. To qualify for remediation deployment with a configured remote remediation server, assets must be registered to that remediation server and must be running both the USD Agent and the VM Service.
- Do not enable the internal USD remediation server. Instead, configure one or more DSM r11 remediation servers that already exist on your network. To qualify for remediation deployment with a configured remote remediation server, assets must be registered to that remediation server and must be running both the DSM r11 Agent and the VM Service.

To integrate an eTrust Vulnerability Manager standard appliance with remediation servers

1. Select the Integration tab and click Remediation Servers.
2. To enable remediation, take one of the following actions:
   - Click Enable Internal Server
   - Select one of the following from the Server Type dropdown list:
     - USD 4.0
     - DSM r11

3. If you selected USD 4.0, complete the integration information as follows:
   a. Enter the IP address or host name of the USD server to add.
   b. Enter the valid User ID of for this server.
   c. Enter the password for this server.
   d. Click Add.

      The server you identified is configured as a remediation server. Your specifications are added to the server list. When you select Tasks, Remediation View, Qualifying Assets and click Search, the configured server location appears in the results for each asset that is registered with that server and is running the required agents.
4. If you selected DSM r11, complete the integration information as follows, using examples that follow this procedure as guidelines:
   a. Select the security provider, or authentication mechanism, for the server you are configuring.

      Note: For details, see the *DSM Implementation Guide* section on DSM Security Features.
   b. Enter the IP address or host name of the DSM server to add.
   c. Enter the User name for this server.
   d. Enter the security authority in the Security Authority text box. This is typically the domain part of the domain\userName you entered in the User text box.
   e. Enter the password for this server
   f. Click Add.

      The server you identified is configured as a remediation server. Your specifications are added to the server list. When you select Tasks, Remediation View, Qualifying Assets and click Search, the configured server location appears in the results for each asset that is registered with that server and is running the required agents.

Example - LDAP Configuration

When integrating with a DSM r11 Remediation Server where the security provider is ldap, use the following example as a guideline for entries:

- Hostname: svm-2k3-7
- Username: *username*@*company*.com
- Security Authority: *company*.com
- Password: *domain_password*

Example - LDAPS Configuration

When integrating with a DSM r11 Remediation Server where the security provider is ldaps, use the following example as a guideline for entries:

- Hostname: svm-2k3-7
- Username: uid=*username*,ou=people,dc=dsm,dc=com
- Security Authority: uni999999-20.*company*.com
- Password: "*password*"

Example - NDS Configuration

When integrating with a DSM r11 Remediation Server where the security provider is nds, use the following example as a guideline for entries:

- Hostname: uni999999-119
- Username: cn=vak.ou=users.o=unisvmnovell1
- Security Authority: unisvmnovell1
- Password: ca12#

Example - WINNT or UNIXL Configuration

When integrating with a DSM r11 Remediation Server where the security provider is winnt or unixl, use the following example as a guideline for entries:

- Hostname: *machine_name*
- Username: Administrator
- Security Authority: *machine_name*
- Password: *password*

DMS Integration Port Requirements

DSM integration requires that port 4104 be open for UDP communication from the DSM Server to the VM Server (inbound).

Important! If you integrate the eVM appliance with DSM r11, configure your firewall to allow inbound UDP traffic through port 4104.

Chapter 3: Known Issues

This section contains the following topics:

Documentation and Help Not Updated

The documentation and online help system are not being updated for the eTrust Vulnerability Manager r8.3.14 release.

Embedded Server Not Supported on Dell 1950 Standard Appliance

The Dell 1950 standard appliance with a single CPU does not have an embedded server. This means that you will be unable to perform remediations on agent machines using the embedded Remediation Server if you are using the Dell 1950 standard appliance. You can, however, add up to ten remote remediation servers on this standard appliance and perform remediations through these servers.

Important! This issue does not affect the standard appliance eVM14001 or eVM 1400S on other hardware.

Turning on Wireless Network Alters Return of IP Address

Consider the scenario where an asset that eTrust Vulnerability Manager manages is assigned two IP addresses--one for an active wired network and another for an unused wireless network. When the wireless network is turned on, the IP address for the wireless network may be returned by the eTrust Vulnerability Manager Service rather than the expected IP address from the wired network.

Remediation Fails When Target is Defined with FQDN

Unicenter SD integrates with eTrust Vulnerability Manager to provide deployment of patches to your assets, a process known as remediation management. If an asset host name includes domain name properties (for example, asset.ca.com), Unicenter SD drops everything to the right of the first period (including the first period), truncating the name to "asset." In this case, remediation management will not work because the asset name in eTrust Vulnerability Manager remains "asset.ca.com" and will not match the Unicenter SD truncated name.

Chapter 4: Usage Considerations

This section contains the following topics:

eTrust Vulnerability Manager Documentation

Hardware installation instructions and set up instructions for the installed eTrust Vulnerability Manager software are included in the eTrust Vulnerability Manager Quick Start r8. This manual is included in the product packaging. No updates have been made to the Quick Start documentation distributed with eVM r8.

The file names for the available eTrust Vulnerability Manager documentation are as follows:

Guide Name	File Name
eTrust Vulnerability Manager Quick Start r8	VM_Quick Start_enu.pdf
eTrust Vulnerability Manager Release Summary r8.3.14	VM_Release_ENU.pdf

To view PDF files, you must download and install the Adobe Reader from the Adobe website if it is not already installed on your computer.

For assistance in finding the eTrust Vulnerability Manager documentation, contact Technical Support at http://ca.com/support.

Published Fixes

The complete list of published bug fixes for this product can be found through Published Solutions on http://ca.com/support.

International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

In addition to the English release of this product, Computer Associates supports *only* those languages listed in the following table.

Language	Internationalized	Translated
Brazilian-Portuguese	No	No
Chinese (Simplified)	Yes	No
Chinese (Traditional)	No	No
French	Yes	No
German	Yes	No
Italian	Yes	No
Japanese	Yes	No
Korean	Yes	No
Spanish	Yes	No

Note: If you run the product in a language environment *not* listed in the table, you may experience problems.

eTrust Vulnerability Manager will not run on internationalized operating systems. It is always delivered on the English operating system, but will take input from the internationalized clients.

Internationalized support is limited to assets with 32-bit edition Windows operating systems.

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Glossary

Remediation Agent

The Remediation Agent can be either a USD Agent, a CA Unicenter Software Delivery 4.0 component, or a DSM Agent, a CA Desktop and Server Management r11 component. The USD Agent installed on a client managed by eTrust Vulnerability Manager can accept remediations from USD 4.0 remediation server. The DSM Agent installed on a client managed by eTrust Vulnerability Manager can accept remediations from the DSM r11 remediation server. When the remediations are invoked from a standard appliance, the target assets must have the VM Service installed. When remediations are invoked from an enterprise appliance, the VM Service is optional for target assets.

Remediation Server

A *Remediation Server* is a Software Delivery (SD) server that delivers remediations to clients with a Remediation Agent. An SD sever must be one of the following server types: USD 4.0 SP1 and above or DSM r11 and above. You can integrate CA Vulnerability Manager with up to fifty Remediation Servers on an enterprise appliance or up to ten Remediation Servers on a standard appliance.