

Title: Assuria Auditor Remote Adapter Release 1.0 now available

Number: 99 Date: 30 July 2009

Title Assuria Auditor Remote Adapter – Release 1

Introduction The Bulletin introduces Assuria's Remote scanning technology Assuria Auditor Remote Adapter which is now released and generally available for downloaded from the AssuriaOnline Download area.

Assuria Auditor Remote Adapter

The release of Assuria Auditor Remote Adapter is another significant step in the development and evolution of Assuria Auditor. For information about the Assuria Auditor roadmap please contact Assuria.

Introduction The Assuria Auditor Remote Adapter (RA) technology enables remote agent-less scanning by Assuria Auditor using the same checks and policies as the Assuria Auditor agents.

Integrated with the Assuria Auditor Console, RA uses the same database, checks, policies and reporting as the current Assuria Auditor agents while RA a new dedicated user interface.

At this first general release RA is supported installed alongside the assuria Auditor Console running on Windows Server 2003. Initial scanning support is Windows Server 2003 systems. Later releases will support scanning LINUX and UNIX as well as Windows Server 2008, Windows VISTA and Windows 7

Remote Adaptor Summary

- Remote agent-less credentialed internal host scanning
- Provides Policy compliance, Configuration Assurance and Vulnerability Assessment capabilities
- Dedicated User Interface for Remote Adapter
- Integrated, optional component of Assuria Auditor
- Uses Assuria Auditor knowledge base
- Uses Assuria Auditor Checks and Policies
- Results stored in Assuria Auditor Console database
- Produces integrated Assuria Auditor Reports
- New Assuria communications protocol using WMI

Assuria Auditor – Remote Adaptor

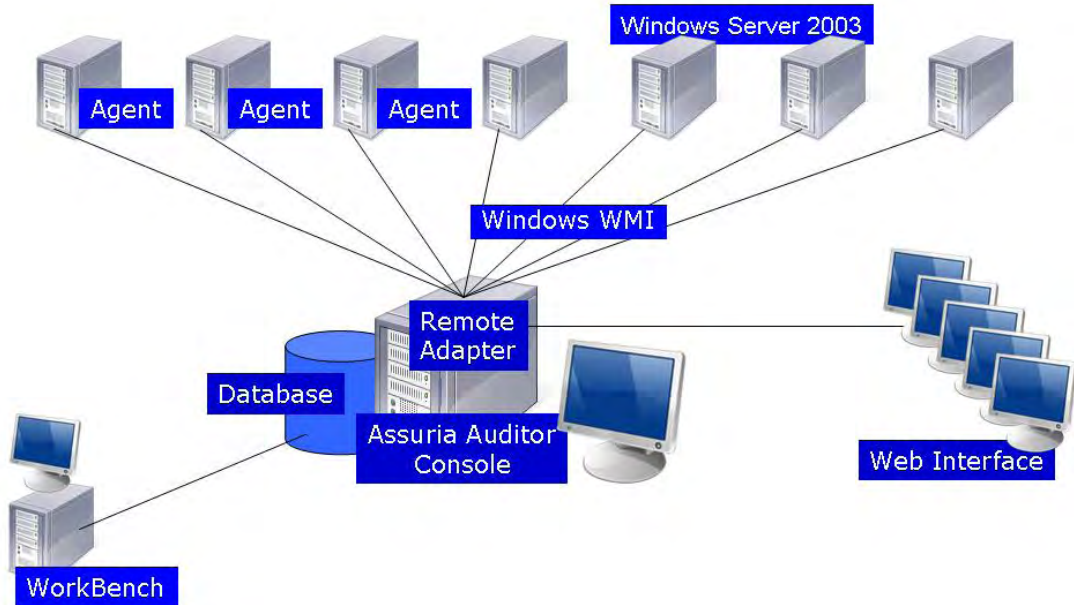


Figure – Assuria Remote Adapter - Architecture

Internal and External scanning

Agent based or credentialed host scanning is often known as “Internal Scanning”. Scanning without the use of credentials, in effect probing from the outside is often known as ‘External Scanning’.

Assuria RA performs internal scanning and uses securely stored credentials to login to the target host or hosts, once logged-in the RA software can obtain ‘host-based’ system data as if it were resident on the system and running as privileged user.

Remote Adapter User Interface

The RA dedicated user interface component is installed and runs alongside the Assuria Auditor Console. RA has a plug-in architecture that allows Assuria to easily add extra functionality without making a new product release. The RA GUI is Java based and data integrated with the current Assuria Auditor Console database.

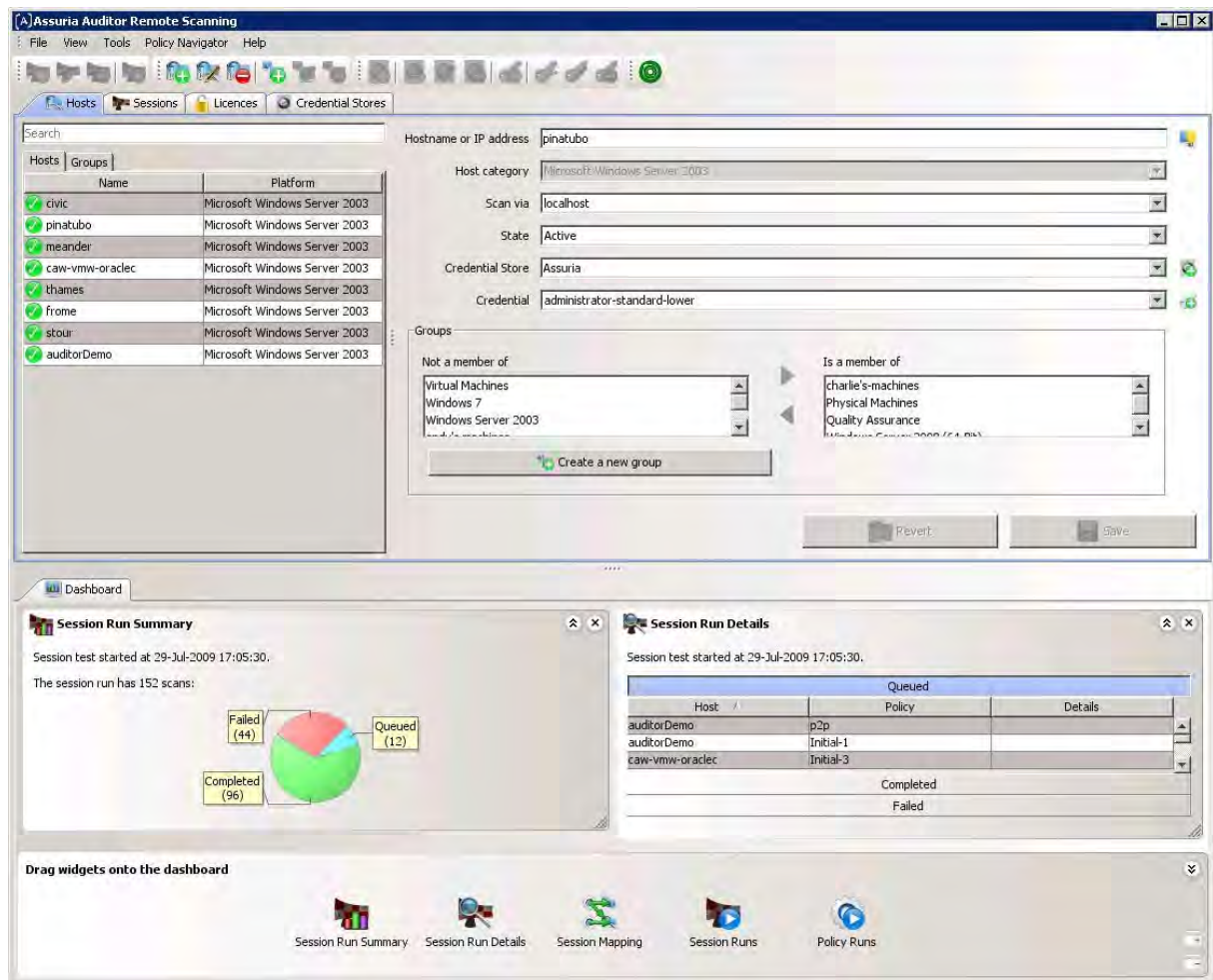


Figure – Assuria Auditor Remote Adapter User Interface

The Remote Adapter user interface provides facilities to:

- Create and manage Credential Stores to securely store credentials required to access the target hosts.
- Add hosts or system to be scanned
- Create sessions. A session is a mapping of Assuria Auditor Policies to target hosts.
- Run sessions. Scan configured hosts or target systems.
- Monitor and view session progress

Hosts (target systems)	<p>The target systems or hosts, i.e. the computer systems to be scanned are known as Hosts and are configured via the User Interface.</p> <p>RA is configured with the name and / or IP address of each host to be scanned. Hosts can be collected into arbitrary groups for simpler management of similar systems. Credentials held in the credential store can be associated with a single Host, any number of Hosts or groups of Hosts.</p>
Password and User Name Management	<p>RA requires credentials for login and authentication by the remote host this is usernames and passwords</p> <p>Ideally the credentials should give 'administrator' access to the host(s) to be scanned. Running with lower privilege may result in some checks not being able to obtain all the information required to fully function.</p>
Credential use	<p>For comprehensive auditing of RA Assuria suggests the creation of separate accounts for exclusive use by RA on target Hosts. Full auditing of the 'scan user' should be activated so that a full audit trail of the account's actions and accesses are available for review and analysis if required¹.</p> <p>The account to be used by the RA requires Administrator rights on the target hosts, the 'scan user' will need read access to the WMI namespace and the ability to execute functions on the registry object. If required the use of more specific privileges can be assigned. User should refer to the following URL from Microsoft (http://support.microsoft.com/kb/325353). Assuria has an FAQ document on the required privileges which is available from Assuria on request.</p>
Credential Security and Management	<p>Remote Adapter manages the credentials according to the security requirements below:</p> <ul style="list-style-type: none"> • Credentials are never transmitted unencrypted. • The ability to use a credential can be restricted to certain individuals. • A credential can be used without the users being able to decrypt the credential. (This lets security personnel run scans using, e.g. a 'superuser' password supplied by a system administrator, without the person running the scan knowing the password.)
Policies and Checks	<p>Most Remote Adapter scan Policies and Checks are identical to those used by the Assuria Auditor resident agents. Assuria Auditor today has consistent cross platform policy and check naming; this is extended to Remote Adapter. Where functionality is implemented that is unique to the Remote Adapter then unique Remote Adapter names are used.</p>
Scan results	<p>The scan results from checks and policies run via RA are imported into the Assuria Auditor database and all Assuria Auditor reports are available.</p>

¹ Assuria Log Manager is the ideal product to collect audit logs from across the Enterprise for such analysis and reporting.

Reports combining both RA and agent based scan results can be produced.

Remote Adapter policies

The Assuria Auditor Policies supported are:

- Initial-All
- Initial-1
- Initial-2
- Initial-3
- Initial-4
- Initial-5
- Maintenance-All
- Maintenance-1
- Maintenance-2
- Maintenance-3
- Maintenance-4
- Maintenance-5
- SANS_Top_20
- accountPolicy
- auditPolicy
- event-logs
- logon-settings
- p2p
- privileges
- user-Checks
- versionChecks

Policy Navigator

See Assuria Auditor Users Guide Chapter 3 for more information about the Policies. A Policy Navigators for the Release 1 is include and accessible form the Scan Adapter user interface.

Licensing

Licensing will be on per Host scanned. An additional Remote Adapter key will be required for the Assuria Auditor system.

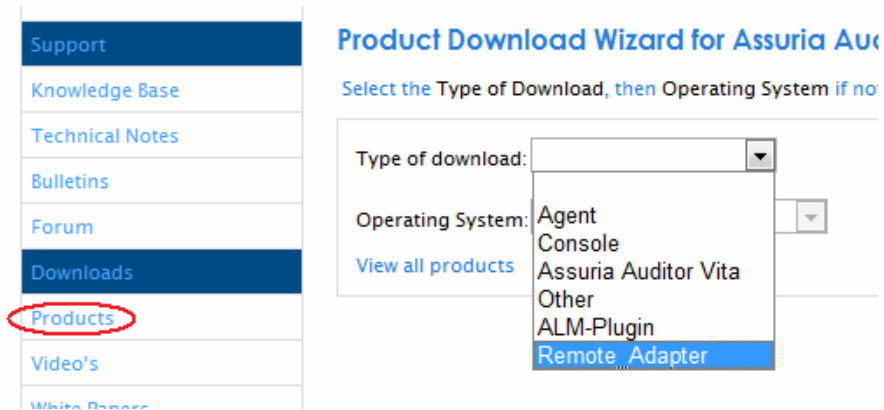
If the count of Hosts is exceeded the GUI will allow currently configured Host to be marked as obsolete and new Host added.

Assuria Auditor Console AutoUpdate level

Support for Remote Adapter is added to the Assuria Auditor Console in AutoUpdate 97 – released 29 July 2009.

Download

Assuria Auditor Remote Adaptor is available for download from the download area on AssuriaOnline.



Select "Remote Adapter" on the 'Type of download' pull down list.

- Documentation** An updated Assuria Auditor Users Guide and Installation Guide with Chapters on RA are available for download
- System Requirements** An updated Assuria Auditor system requirements document is available for download from AssuriaOnline.
- Installation** Installation is described in the updated assuria Auditor Installation Guide.
- Support** For any problems with RA or for any advice regarding the use or deployment of RA please contact Assuria Support or email to 'support@assuria.com'.
- Questions or help** Assuria Support is available to help you make the most of your Assuria products. Please contact support by email to 'support@assuria.com'.

Assuria Limited, Science Technology Centre, The University of Reading, Earley Gate, Reading, RG6 6BZ, UK.

Telephone +44 118 935 7395 Fax +44 118 926 7917 Web www.assuria.com