Radia Client Automation

Software Version: 10.0

Managing Delta Updates

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty of any kind, implied, statutory, or in any communication between them, including without limitation, the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. Accelerite shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Accelerite or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Accelerite.

Copyright Notices

Trademark Notices

Radia, Accelerite and Persistent are trademarks or trade name or service mark or logo of Accelerite/Persistent. All other brands or products are trademarks, trade name, service mark, logo or registered trademarks of their respective holders/owners thereof.

Acknowledgements

This product includes software developed by the Apache Software Foundation (http://www.apache.org/) and user of the products are bound to comply with the provisions of the said software license.

Contents

Background

Radia Patch Management enables you to acquire patches from vendor, determine the vulnerabilities on the managed devices and deploy applicable patches to managed devices. In addition, it allows you to verify applied patches on managed devices to ensure compliance and security. Furthermore, you can generate reports that provide information on which acquired and applicable patches have or have not yet been applied to a managed device. Using Radia, you can manage Windows 10 service updates that are currently cumulative in nature.

Cumulative updates, as the name suggests, contain all the updates specific to that version up to that release. It includes all the previously released fixes, that is, installing the latest cumulative updates always brings the Windows 10 devices fully up to date. However, these updates continue to increase in size with updates coming in every month.

What are Delta Updates?

Delta updates are updates that include the fixes for a particular month. These updates only include the changes developed since the previous Cumulative update. These are relatively small packages that include only the differences between installed and new files and thereby making deployment faster and easier, especially in large networks.
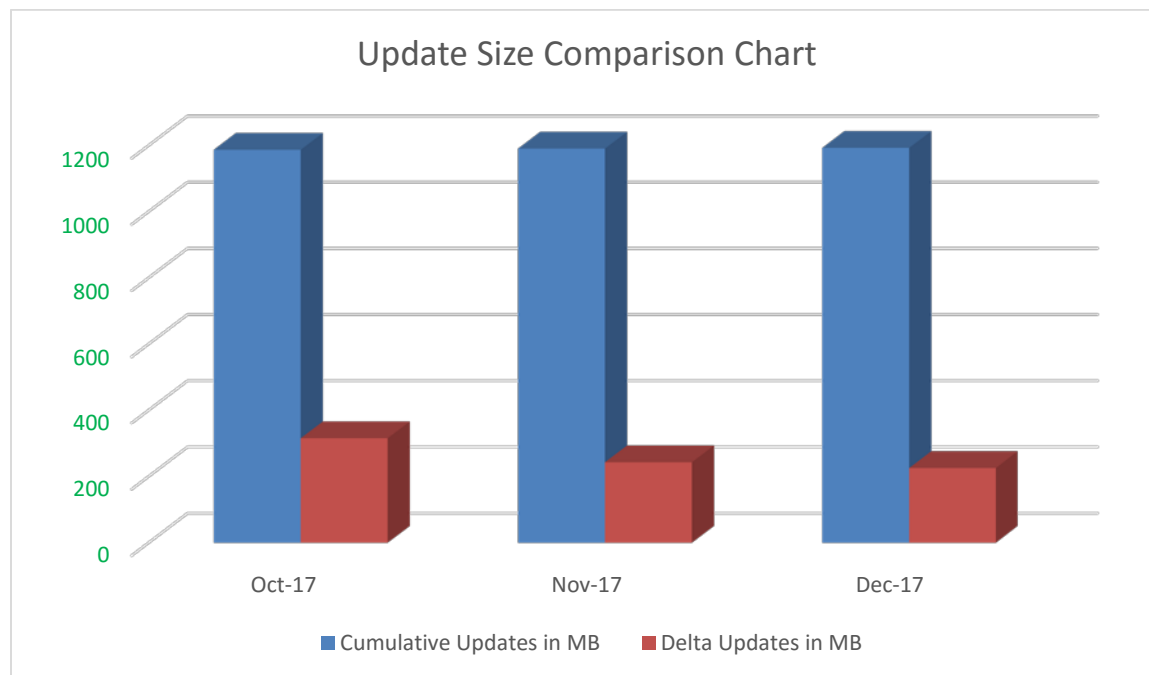

Chart 1: Update Size Comparison

Note: Information in the above chart has been populated against x64 binary size for Windows 10 1607 branch [year 2017].

Delta Updates Vs Cumulative Updates

The following table helps to differentiate between Delta updates and Cumulative updates.

	Delta Updates	Cumulative Updates
Scope	Single update with only new fixes for a particular month	Single bundled update with all new fixes for a particular month and all other fixes for previous months
Update package size	Small	Large
Release date	Every second Tuesday of a month	Every second Tuesday of a month
Changes/Fixes include	Fixes that were implemented for a particular month from the previous Cumulative updates	All fixes for a specific version
Bandwidth usage	Low	High
Applies to	Windows 10 endpoints (for example, 1607, 1703 and 1709) and Windows 2K16 endpoints only if the previous month's Cumulative updates or Delta updates is installed.	All Windows 10 and Windows 2K16 endpoints

Table 1: Comparison between Delta Updates and Cumulative Updates

How Delta Updates Work?

Microsoft releases Delta updates every second Tuesday of a month for all the active Windows 10 branches (for example, 1607, 1703 and 1709) and supported server machines such as, Windows 2K16. For each branch, separate Delta update binaries are released for 32-bit and 64-bit architectures. The KB numbers are same for Delta updates and Cumulative updates, irrespective of the 32 bit or 64 bit architectures.

Delta updates are not part of the wsusscn2.cab file that is published to Windows Update Catalog. As a result, the traditional offline scanning process does not scan and identify risks for a Delta update. To support Delta updates, Radia releases customized metadata files or custom XMLs for each available branch on the same day the patch updates are released. These custom XMLs are named MSDL-KBXXXXXXX, where MSDL stands for Microsoft Delta Updates and KBXXXXXXX is the KB number. For example, Delta updates are named as **MSDL**-KB4038788 whereas Cumulative update are named as **MS**-KB4038788. All the existing acquisition and compliance reports in Radia are applicable to Delta updates. You can view the deployment of Delta updates under Patch Management Reports.

Delta updates can be applied only if the previous month's Cumulative updates or Delta updates have already been installed on the endpoints. For example, to bring Windows 10 endpoints (for example, 1607, 1703 and 1709) up to date with minimum data transfer every month, install the Cumulative updates till the previous month (if not already installed) and then install Delta updates for that particular month and every subsequent month onwards.

Microsoft does not recommend deploying Cumulative and Delta updates of the same month on the endpoints as it may cause inability to reboot the endpoints. Click here for more details. To address this, Radia Patch Manager has the inbuilt intelligence to verify the updates that are already installed on the endpoints and deploy only the updates appropriate to the endpoints, even if both cumulative and delta updates are entitled.

> **Note:**
>
> 1. Delta updates are installed based on the entitlements rather than the state of the endpoints.
>
> 2. If the endpoints are updated with previous month's service updates (n-1 level), Delta updates are pushed to these endpoints. For example, February month's Delta updates are pushed when an endpoint contains January updates.
>
> 3. If the endpoints are not patched for the last two or more months (n-2 or n-3,…), Cumulative updates are pushed to these endpoints rather than two or more consecutive Delta updates. For example, February month's Cumulative updates are pushed when an endpoint contains December (year before) updates.

Acquiring Patches

Delta updates can be acquired as any other patch with the help of custom XMLs. Specify **MSDL*** in the bulletin name to acquire all the Delta updates available on Accelerite Content Network (ACN). Alternatively, you can provide a comma-separated list of specific bulletin names to acquire specific Delta updates.

Note: If you are using regular expression such as MS-KB* while acquiring patches, then to exclude Cumulative updates, provide comma-separated bulletin names in **Configuration tab** > **Patch Management** > **Preferences** > **Retired Bulletins**.

Entitling Patches

The Bulletins/KBs for Delta updates can be entitled as any other bulletin. Entitling the wrapper service for a branch ensures that all Delta updates applicable to that branch are entitled.

Use Cases

The following table explains the basic use cases that can occur while installing Delta or Cumulative Updates.

DU refers to Delta updates, CU refers to Cumulative updates and n refers to current month in the below table.

Note: Patch Compliance Details report is generated only against acquired bulletins. This report displays that both DU and CU are installed. The final list of risks detected appear only in the reports. So, it is recommended to refer to the reports to view the actual risks detected. The initial log files may contain additional risk information which gets resolved at later stages.

Use Case 1: If the endpoints are up to date with the latest updates and all applicable DU and CU are acquired, then no updates are installed (independent of the entitlement).

Current state of endpoints	Entitled	Risk detected/installation status	Update Installed
If endpoints are up to date with the latest DU or CU and both latest DU and CU are acquired	All applicable DU or CU or both	No risk is detected for latest CU and DU. Both will be reported as patched.	None

Use Case 2: If previous month's CU or DU is installed on the endpoints and the latest CU and DU are acquired, then it is recommended to install DU.

Current state of endpoints	Entitled	Risk detected	Update Installed
Last month CU or DU installed (n -1) and latest DU and CU are acquired	Latest DU	Latest DU	Latest DU is installed
	Latest CU	Latest CU	Latest CU is installed
	Latest DU and CU	Latest DU	Latest DU is installed

Use Case 3: If the endpoints are not up to date for last two or more months and all applicable DU and CU are acquired, then it is recommended to entitle CU or both. **Note:** It is not recommended to entitle only Delta updates (multiple) to avoid sequential installation of DU.

Current state of endpoints	Entitled	Risk detected	Update Installed
Not up to date (n -2, n-3, …) and all applicable DU and CU are acquired	All applicable DU **(Not recommended)**	Latest CU and next month's DU from the machine state (n-1, …)	DU is installed and continues to be installed till the latest DU is installed. **Note:** Only DU is installed sequentially.
	All applicable CU		Latest CU is installed
	All applicable DU and CU	Latest CU	Latest CU is installed

Limitations

The limitations observed in this release are listed below:

- Delta updates are not supported for patches acquired using the MSFT model since custom XML support is not currently featured in the MSFT model.
- Uninstallation of Delta patch is not supported.