Active System Manager Release 8.2

Release Notes

Release Type and Definition

Active System Manager

Active System Manager (ASM) is Dell's unified management product that provides a comprehensive infrastructure and workload automation solution for IT administrators and teams.

The release notes contains important information available at the time of release of Active System Manager (ASM) release 8.2, including information about the ASM release lineup and dependencies, ASM documentation lineup, known issues, and the methods to contact Dell technical support.

This document contains updated information for ASM and any other technical documentation included with ASM.

Release

8.2 build 5877

Release Date

April 2016

Previous Release

8.1.1 build 5079

Note: To view the build details, click **?**-> **About** on the ASM user interface.

Platform(s) Affected

Supported ASM Software Components

- ASM Virtual Appliance

Supported Virtualization Platforms

- VMware 5.1 (ASM appliance includes update 03 build 2323236)
- VMware 5.5 (ASM appliance includes update 03 build 3248547)
- VMware 6.0 (ASM appliance includes update 01 build 3073146)
- Microsoft Windows Hyper-V 2012
- Microsoft Windows Hyper-V 2012 R2
- System Center Virtual Machine Manager 2012
- System Center Virtual Machine Manager 2012 R2

What is Supported

Supported Web Browsers

- Microsoft Internet Explorer, version 9 and later
- Mozilla Firefox, version 26 and later
- Google Chrome, version 32 and later
- Safari, version 6 and later

New in this Release

Active System Manager 8.2 is focused on expanding capabilities around workload deployment, adding new capabilities around managing existing environments, and improving the granularity of information shown around the current state of environments under management.

The highlights of Active System Manager release 8.2 include the following:

- Open Platform Support that includes:
  - o Application module SDK and multi-application support
  - o Architectural work to support modularity and to enable a plug-in SDK framework for resource modules, starting with the application level.
  - o Creating Puppet-based application modules and importing the modules in the ASM templates.
- Improved user interface
- Expanded infrastructure and service level monitoring:
  - o Infrastructure health monitoring includes chassis, servers, I/O modules, storage devices, and networking devices.
  - o Service health provides an aggregated view based on services deployed to provide a window into service level health.
- Port view virtualization
  - o A graphical view that provides a mapping of physical to virtual infrastructure and clear notification of connectivity issues.
- Brownfield support to facilitate installing ASM into the existing environment
  - o Includes support for importing existing ESXi hosts and clusters as ASM resources, and the ability use them without requiring ASM to have originally provisioned them. It also enables key features including infrastructure level health and firmware updates.
- Service deployment enhancements that allow:
  - o Validating resources at the template level that is even before the service is deployed.
- Support for deploying bare-metal operating system on certain interface cards using the virtual media available on the server. For such cards, booting from PXE is not required.
- Added static IP support for non-DHCP environment or if you want to use static IP for your deployment.
- Improved post OS configuration and flexibility in provisioning SD with RAID.
- New hardware support for planned Blueprint Reference Architectures (RAs) including virtualization and cloud.

This release also includes compatibility support for the following:
- Storage: Dell Storage SC9000 arrays, Dell EqualLogic PS6610
- Expanded support for Intel 10 Gb interface cards
- Support for VSAN Ready Node configuration for the Dell PowerEdge R730xd server platform. For more information on VSAN Ready Node configuration, see https://www.vmware.com/resources/compatibility/pdf/vi_vsan_rn_guide.
- Added support for RHEL 7.1 and 7.2
- Added support for CentOS 7.1 and 7.2

ASM release 8.2 build 5877 is an update to ASM release 8.1.1. It contains fixes and enhancements that include:

- Support to enable or disable local disks while booting the operating system from SD cards for ESXi deployments.
- Added message prompt in the user interface directing the user to the **Firmware Update** wizard to rerun a firmware update that is failed in a service.
- Added **Test Connection** button to verify if connectivity to a share with the firmware repository is available before attempting to download.
- Added ability to use Customization Specifications when cloning vSphere virtual machines.
- Resolved an issue with the activity log reporting a status as starting the service instead of deleting a service while tearing down a deployment.
- Resolved deployment issues when faulty server interface cards or adapters that returned invalid values were not properly filtered out.
- Resolved an issue where in some cases authentication for CIFS share with firmware repositories failed.
- Resolved an issue where templates created using the **Server (Hardware Only)** configuration prompted for operating system settings.

Important Notes

To support interoperability, ASM 8.2 requires:

- The following resource locales are set to English:
    - Microsoft System Center Virtual Machine Manager (SCVMM)
    - VMware vCenter
    - Dell EqualLogic
    - Dell Compellent
    - Dell Chassis Management Controller (CMC)
    - Integrated Dell Remote Access Controller (iDRAC)
    - NetApp
- All Physical server OS installations must be in English to support unattended installation process.
- The credentials used for all the external systems that ASM interfaces to must be in English. For example, Virtual Machine Manager Credentials for systems such as SCVMM and VMware vCenter must be in English so that ASM can provision to these environments.
- DNS names must be in English.

Fixes

This release includes improvements and bug fixes, including the following previously reported Known Issues that are now resolved:

- **ASM-2381** — Resolves an issue where IQN/IPs are displayed as mandatory for Hyper-V template if ASM is accessed using Mozilla Firefox browser.

- **ASM-3328** — Resolves an issue where import from R430 reference server, sets the server type as undefined in networking section.
- **ASM-3463** — Resolves an issue where a Compellent deployment fails if you type apostrophes (') or other special characters in some fields.
- **ASM-3520** — Resolves an issue where the deployment failed if SD and HDD are enabled and operating system is installed on SD.
- **ASM-3813** — Resolves an issue where adding a firmware repository using a local drive allowed uploading other arbitrary files.
- **ASM-4216** — Resolves an issue where the Boot Order, Target Boot Device and RAID Configuration are not set.

- **ASM-4282** — Resolves an issue in HyperV services, where if only the last server is selected for teardown without including the cluster, the host is removed from the cluster.
- **ASM-4399** — Resolves an issue where the `testing123` message is displayed when upgrading from version 8.1 to version 8.1.1.
- **ASM-4453** — Resolves an issue where the "Management IP Source" option is not available if you add a server using "Add Resource" to a service.
- **ASM-4562** — Resolves an issue when removing resources from ASM HyperV/SCVMM service, does not completely remove resources in SCVMM.
- **ASM-4582** — Resolves an issue with ASM Template not configuring FCOE VLANs correctly with Dell PowerEdge M420 connected to Slot 2B on a PowerEdge M1000e chassis.
- **ASM-4632** — Resolves an issue with creating a deployment with PowerEdge FX2 servers with a Quad Port Card in the Integrated Slot and FC Card in the Chassis Slot 8.

Known Issues

This section provides information on open issues and resolutions with this release of Active System Manager 8.2.

- **Issue: ASM-1469**: The puppet agent fails to install on Cent OS v6.4. The Cent OS v6.4 cannot mount the appliance's CIFS share in order to download the rpm.

  Description: The samba-client needs to be installed on the linux VM for the mount to work, but it is not installed. In RHEL 6.5, samba-client is installed by default but not on Cent OS v6.4.

  Resolution/Workaround: The problem occurs when you use the minimal ISO. It does not contain the samba-client. You should make sure that the full ISOs are used.

- **Issue: ASM-1674:** Invalid password error when trying to create a User, Credential, or Service Template Component.

  Description: Known issue when using FireFox **Remember Password** feature. If FireFox detects that you type in a value that matches the Remembered password it passes a blank value rather than the typed-in value. So the second time you try to type the same password value for the same type of entity in ASM, if the password you enter matches the previously used value for that type of entity then the system will be passed a blank value for the password.

  Resolution/Workaround: Add an exception to FireFox to not save passwords for ASM URL. Perform the following steps:
  1. Start Firefox.
  2. Go to **Tools** -> **Options**.
  3. Click on the **Security** tab.
  4. If you already have saved passwords for your ASM appliance, click the **Save Passwords** button, select your ASM Appliance URL and click **Remove**, then click **Close**.
  5. Exit out of FireFox options.
  6. The next time you log into ASM and enter a password for one of these fields, when prompted to Remember passwords for the site click the drop-down arrow and choose **'Never Remember Passwords** for This Site'.

  NOTE: This is a browser/system specific setting, so if multiple users are using your ASM appliance all users will need to make sure to disable **Remember Password** for ASM Appliance URL.

- **Issue: ASM-1894**: ASM is unable to distinguish volumes with the same names in different Compellent folders.

   Description: ASM cannot distinguish volumes with a same name in different folder in a Compellent inventory

   Resolution/Workaround: Ensure that you provide unique names for volumes used by ASM in your Compellent inventory.

- **Issue: ASM-2144**: Server with bare hard drive fails to get HddSeq set properly

   Description: If you choose SD boot and the server has a bare hard drive (not connected through a RAID controller) the HddSeq may fail to get set properly, Leaving the bare hard drive at the top of the list. The server may boot off the bare hard drive instead of the SD card where the operating system was installed.

   Resolution/Workaround: None

- **Issue: ASM-2287**: The server teardown operation does not remove the Active Directory and DNS entries of the servers.

   Description: If you tear down servers in a service, Active Directory and DNS entries of the server are not removed if the associated cluster is not selected for tear down. In addition, in some cases, if ASM is unable to communicate with the Active Directory or DNS server, these entries may also not be removed.

   Resolution/Workaround: To remove the Active Directory and DNS entries of the server, make sure to select the associated cluster. If the issues persist, confirm that the Active Directory and DNS entries have been removed from the server manually.

- **Issue: ASM-2599**: Issue with Configure Resources when IOM Firmware is out-of-date with minimum firmware requirements.

   Description: The following error message is displayed while configuring resources when a firmware running on the I/O module does not meet the minimum requirements. If the IOM firmware is not within the Compatibility Matrix minimum firmware, The following error is displayed when it attempts to show the discovered resources.
   ```
   An Unexpected error has occurred on the system Please try
   again later.
   ```

   Resolution/Workaround: You must update the I/O module firmware and retry initial discovery and configuration of the chassis.

- **Issue: ASM-2951**: Error message is displayed during firmware update on C series.

   Description: While performing firmware update on C series servers, the health status of the C series switch changes to <gray> and the following error message is displayed.
   ```
   Unknown error querying ipmi on host 172.31.32.142: Could
   not retrieve IPMI status: ipmi_sensor_read: internal IPMI
   error.
   ```

   Resolution/Workaround: This is an expected behavior because connection is not established with the BMC for a few seconds when you initiate firmware update operation, and the firmware update continues after the connectivity is established with BMC.

- **Issue: ASM-3133**: ASM performs the discovery operation on the FX2 chassis after you update the CMC firmware.

   Description: The Chassis firmware update will trigger the Chassis inventory which will trigger the Chassis discovery in order to detect any newly inserted blades or IOMs.

Resolution/Workaround: This is an expected behavior. When you update the CMC firmware on FX2 chassis, the chassis firmware update operation initiates the Chassis inventory operation, which in turn initiates the chassis discovery operation to collect the information about the blades or IOMs that are newly inserted.

- **Issue: ASM-3157**: For SCVMM cluster provisioning, Active Directory must not contain any hosts with the same name.

  Description: When you provision a SCVMM cluster using a Hyper-V cluster creation template, if the template has the AD entries for the Cluster that are persistent and match the name you are trying to provision, the SCVMM cluster deployment will fail.

  Resolution/Workaround: Active Directory and DNS conflicts must be resolved prior to a deployment if you intend to use names that may already exist within your AD/DNS. ASM requires the names to be removed from AD/DNS and these will be re-provisioned during the template execution.

  o **Resolution/Workaround**: None

- **Issue**: **ASM 3490**: Host and sub host groups cannot be used in separate deployments for Hyper-V deployments.

  Description: Hyper-V deployments uses one logical network and all hosts are assigned the same logical network. In case of two deployments, if the first deployment uses the parent host group and the second deployment uses a user defined host group, then the second deployment with the user defined host group fails.

  Resolution/Workaround: None

- **Issue: ASM-3545**: C-series cannot be taken as a reference server though it is displayed in the import list.

  Description: This is an expected behavior. C-series servers cannot be referenced as reference servers as they do not have iDRAC supported.

  Resolution/Workaround: None

- **Issue: ASM-3639**: Time difference between the installed operating system and ASM appliance may cause the operating system post-install configuration on servers and virtual machines to fail while waiting for puppet agent to check in.

  Description: ASM includes a puppet agent while installing the Windows or Linux operating systems. The puppet agent communicates with the ASM appliance to retrieve the post-install configuration and both server (ASM) and client-side SSL certificates are checked for validity during this process. The ASM server-side SSL certificate is created when the ASM appliance is first started and is marked valid only after the first boot time of the appliance. Hence, a failure may occur if the initial time set on the appliance is incorrect.

  To view this issue, manually run the "puppet agent -t" command on the server or VM that is experiencing a failure. This problem usually results in SSL_connect errors in the output and the following message is displayed: `CRL is not yet valid for /CN=dellasm`.

  Resolution/Workaround:

  Ensure that the hypervisor host on which you want to install ASM is set to the correct time and NTP is used for the ASM appliance, ASM installed servers, virtual machines to ensure consistency in the time.

- **Issue: ASM-3862**: UEFI boot is not supported in ASM.

    Description: The BIOS boot mode does not change to UEFI after the local hard drive is set as the target boot device. This issue occurs because ASM does not support UEFI boot support.

    Resolution/Workaround: None

- **Issue: ASM-4123**: Service reports "Error" state though all other components are successful.

    Description: In some cases when deleting a failed resource, for example, a VM Component, from a successful servers puts the service in error state despite all remaining components in successfully "Deployed" state.

    Resolution/Workaround: Retry the service should move the service state back to successful.

- **Issue: ASM-4174:** ASM backend not to tear down the shared resources.

    Description: When deleting a service the user has the option to delete clusters and storage. If these are shared with other services, ASM will not warn the user and will proceed to remove the shared resources.

    Resolution/Workaround: Prior to deleting a service, verify which clusters and storage volumes are shared with other services. Only select delete for resources which will not impact other services.

- **Issue: ASM-4205**: ESXi 6.0 with Compellent will fail if the array has firmware version later than v6.6.

    Description: vCenter 6.0 support is added with Storage Center 6.6. While creating a deployment with ESXi 6.0, select Compellent for which storage center is upgraded to version 6.6

    Resolution/Workaround: In case the storage center is running on version less than 6.6, then for Compellent Storage Component, select Operating System as "ESXi 5.5" or "ESXi 5.1"

- **Issue: ASM-4273**: Volumes deleted from a HyperV service in ASM are not removed completely from the HyperV host.

    Description: If you delete a storage volume from a HyperV service, the volume will be deleted on the storage array and removed from ASM service, but there may be stale references left on HyperV hosts.

    Resolution/Workaround: Manually remove references to non-existent volumes in HyperV using disk manager.

- **Issue: ASM-4328**: After restore, operating system and firmware need to be able to be rebuilt.

    Description: After a restore, operating system and firmware repositories are placeholders. The user must now remove the repositories and add new ones. However, any existing templates or services that rely on the repositories will prevent the existing repositories from being deleted in order to be re-added. Hence, the user has to change the repositories for all templates, and any existing services will have to be deleted in order to point to the correct repository.

    Resolution/Workaround: For any repositories, they cannot be used for new templates or as an option for adding resources to a service, and provide a method to rebuild the existing repository without requiring deletion.

- **Issue: ASM-4561:** Problem with 7.12 Broadcom firmware.

    Description: Broadcom NIC firmware 7.12.xx is not compatible with ASM. It can cause intermittent connectivity issues which will result in hypervisor and bare metal OS deployment failures.

    o **Resolution/Workaround**: Apply the firmware available in the latest ASM catalog. Alternatively, manually downgrade your Broadcom NIC firmware to

7.10.xx. Also, note that v7.12.17 will not work and later versions resolves this issue, but 7.10.xx is the qualified version.

- **Issue: ASM-4590:** Intel NIC cards need to be at version 15.5.0 or later for firmware updates to work.

  Description: Firmware update for 12th generation blades with intel cards and Broadcom card fails in some cases when Intel NICs are installed if it is not of version 15.5.0.

  Resolution/Workaround: Updating Intel X520 cards with versions earlier than 15.5.0 to 16.5.x requires a manual update to 15.5.0, prior to upgrading to 16.5.x with ASM.

- **Issue: ASM-4688**: In NIC firmware, the X520/I350 rNDC firmware version 15.0.28 to version 16.5.20 firmware fails to update in the firmware update logs.

  Description: This is due to a specific firmware update issue with the X520/I350 rNDC firmware version 16.5.20. The X520/I350 rNDC firmware may require a step-up to an intermediate version of the firmware in order to upgrade from 15.0.28 to 16.5.20.

  Resolution/Workaround: Updating Intel X520/l350 cards with versions earlier than 15.5.28 to 16.5.x requires a manual update to 15.5.28, prior to upgrading to 16.5.x with ASM.

- **Issue: ASM-4697:** Logs messages need to be updated for firmware retry logic.

  Description: Firmware updates retries up to three attempts displaying an error message for each failed attempt. The message displayed must be updated to indicate a failed attempt occurred and a retry will follow. In some cases a success message is logged followed by an error message.

  Resolution/Workaround: None

- **Issue: ASM-4775**: Broadcom NIC will fail firmware update if current firmware is older than 7.8.53.

  Description: Broadcom firmware in the ASM catalog, 7.10.18, will require a minimum of 7.8.53 for the firmware update to succeed.

  Resolution/Workaround: None

- **Issue: ASM-4908**: Domain name lookup from the ASM interface continues to fail even after configuring DNS on the appliance.

  Description: If the DNS is not configured during initial setup, the domain name lookup fails and this negative lookup is cached in the system. Subsequent domain name lookup attempts continue to fail even after configuring DNS on the appliance.

  Resolution/Workaround: It is recommended to configure DNS during initial setup. If DNS is configured after the domain lookup fails, restart the appliance to resolve the issue.

- **Issue: ASM-4915**: ESXi install to SD card fails.

  Description: While installing ESXi, a problem with the SD card mirroring may result in a failure occasionally and will display the following error:

  ```
  BANK5: invalid configuration.
  BANK6: invalid configuration.
  No hypervisor found.
  ```

  Resolution/Workaround: Delete the server from the ASM service and redeploy it again.

- **Issue: ASM-5132**: On PowerEdge C6320 systems with ESXi version 5.1 or ESXi version 5.2 (update 2), the keyboard is unresponsive if USB 3.0 is set to enabled in the server BIOS.

> **Description**: This issue occurs because USB 3.0 is not supported by ESXi version 5.1 and ESXi version 5.2 (update 2).
>
> **Resolution/Workaround**: Try any of the following options to resolve the issue:
> - Disable USB 3.0 from the server BIOS.
> - For servers that require USB 3.0, upgrade ESXi to version 5.5 (update 3) or version 6.0.

- **Issue: ASM-5397**: Unable to login to the user interface.

    > **Description**: The user interface is inaccessible when you login after updating to ASM 8.2.
    >
    > **Resolution/Workaround**: Ensure that you clear the browser cache after updating ASM and before logging in the user interface.

- **Issue: ASM-5510**: Removing the battery from a controller on a Dell Compellent storage device displays an inaccurate message.

    > **Description**: After you remove the controller battery on a Dell Compellent storage device, an incorrect error message is displayed on the **Resource** page.
    >
    > **Resolution/Workaround**: None.

- **Issue: ASM-5984**: Static IP addresses are requested or reserved for **Server (Hardware Only)** components.

    > **Description**: When deploying an ASM template with a **Server (Hardware Only)** configuration, IP addresses are reserved for all static networks included on the network configuration of the component. Because this is a "hardware only" component ASM does not configure the server to use these IPs.
    >
    > **Resolution/Workaround**: Ensure that you do not assign static networks to the **Server (Hardware Only)** components or ensure that the static networks that are used have enough IP addresses that can be assigned to the component.

- **Issue: ASM-6170**: You can select unsupported ports for Virtual Link Trunking (VLT) configuration on the I/O Aggregator.

    > **Description**: While configuring VLT on an I/O Aggregator, only ports 33 and 37 are supported. However, ASM allows you to select other non-supported ports.
    >
    > **Resolution/Workaround**: If you wish to configure VLT, ensure that you select ports 33 and 37 in the ASM user interface.

- **Issue: ASM-6247**: After upgrading from 8.1.1 to 8.2, templates including virtual distributed switches and port-group settings in a VMware Cluster component are not imported.

    > **Description**: After an upgrade from ASM version 8.1.1 to 8.2, the virtual distributed switches and port-group settings in an existing 8.1.1 templates with a VMware Cluster component are not correctly populated.
    >
    > **Resolution/Workaround**: While upgrading 8.1.1, if the VMware Virtual Distributed setting is required, ensure that the cluster component is deleted and recreated, and the appropriate data center is selected.

- **Issue: ASM-6299**: When building a template using the Import from Existing Template option, you must renter the password, even though a password is displayed.

    > **Description**: When creating a server template using the Import from Existing Template option, the password field is populated even though there is no password set. If you proceed without updating the password and save it, the server icon turns yellow. Attempting to publish the template displays an error message stating that the admin password and confirmation password are missing.

Resolution/Workaround: As a best practice for all imported templates, clear the password field and set them correctly.

- **Issue: ASM-6311**: Stale Active Directory account entries for HyperV host and cluster can fail HyperV deployments.

  Description: A HyperV deployment may fail if stale Active Directory account entries corresponding to a host or a cluster name are used in a deployment.

  Resolution/Workaround: Ensure that you clear the unused and stale entries from Active Directory and then try a deployment.

- **Issue: ASM-6319**: On the **Network Details** page, released IP Addresses appear under the old service.

  Description: After you scale down a server or virtual machine, the IP address used by the component is released and available for reuse in the future. However, on the **Network Details** page for the network the IP Address belongs to, the IP Address is listed under the old service using it. This issue occurs until the IP Address is used by another service.

  Resolution/Workaround: None.

Limitations

None

Installation Prerequisites

For installation pre-requisites, see the "*Active System Manager 8.2 Installation Guide*" available at **dell.com/asmdocs**.

Installation Procedure

For complete installation instructions, see the "*Active System Manager 8.2 Installation Guide*" available at **dell.com/asmdocs**.

Installation and Configuration Notes

None

Documentation Errata

None

Contacting Dell Technical Support

- Make sure that the Active System Manager Service Tag is available.
- Go to the tech direct portal https://techdirect.dell.com
- Login using your existing account or create an account if you do not have an account.
- Create a new case for your incident.
- Add your Active system Manager service tag.
- Select **Active System Manager** as the Incident type
- Type relevant information in the Problem Details, and add attachments or screenshots if necessary.
- Fill in contact information and submit the request

2016 – 04