Planning

The Cisco Secure Malware Analytics Appliance is a Linux server with Secure Malware Analytics software installed by Cisco Manufacturing prior to shipment. Once a new Secure Malware Analytics Appliance is received, it must be set up and configured for your on-premises network environment.

This chapter describes the environmental, hardware, and network requirements that should be reviewed prior to setup and configuration:

Supported Browsers

Secure Malware Analytics supports the following browsers:

- Google Chrome™
- Mozilla Firefox®
- Apple Safari®

Note Microsoft® Internet Explorer® is **not** supported.

Environmental Requirements

Secure Malware Analytics Appliance (v2.7.2 and later) is deployed on the Secure Malware Analytics M5 Appliance server. Before you set up and configure the Secure Malware Analytics Appliance, make sure the necessary environmental requirements for power, rack space, cooling, and other issues are met, according to the specifications in the *Cisco Threat Grid M5 Hardware Installation Guide*.

Hardware Requirements

The SFP+ form factor is used for the Admin interface. If you are clustering Secure Malware Analytics Appliances, each one will require an additional SFP+ module on the Clust interface.

Note The SFP+ modules must be connected *before* the Secure Malware Analytics Appliance is powered on for the session in which the configuration wizard is going to be run.

If there are no SFP+ ports available on the switch, or SFP+ is not desirable, then a transceiver for 1000Base-T can be used (for example, Cisco Compatible Gigabit RJ 45 Copper SFP Transceiver Module Mini -GBIC - 10/100/1000 Base-T Copper SFP Module).

Figure 1: Cisco 1000BASE-T Copper SFP (GLC-T)

You can attach a monitor to the server, or, if Cisco Integrated Management Controller (CIMC) is configured, you can use a remote KVM (on UCS C220-M3 and C220-M4 servers).

Note CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

The Cisco UCS Power Calculator is available to get a power estimate.

Network Requirements

The Secure Malware Analytics Appliance requires three networks:

- **ADMIN** - The Administrative network must be configured to perform the Secure Malware Analytics Appliance setup.
  - Admin UI Management Traffic (HTTPS)
  - SSH
  - NFSv4 (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.)
- **CLEAN** - The Clean network is used for inbound, trusted traffic to the Secure Malware Analytics Appliance (requests), and integrated appliances such as the Cisco Email Security Appliance and Web Security Appliance; integrated appliances connect to the IP address of the Clean interface.

Note The URL for the Clean network interface will not work until the Admin UI configuration is complete.

The following specific, restricted types of network traffic can be outbound from the Clean network:

- Remote syslog connections
- Email messages sent by the Secure Malware Analytics Appliance
- Disposition Update Service connections to Secure Endpoint Private Cloud devices
- DNS requests (related to any of the above)
- LDAP
- RADIUS traffic

- **DIRTY** - The Dirty network is used for outbound traffic from the Secure Malware Analytics Appliance (including malware traffic).

Note To protect your internal network assets, we recommend using a dedicated external IP address (for example, the Dirty interface) that is different from your corporate IP.

For network interface setup information, see Network Interfaces.

DNS Server Access

The DNS server needs to be accessible via the Dirty network when used for purposes other than Disposition Update Service lookups, resolving remote syslog connections, and resolving the mail server used for notifications from the Secure Malware Analytics software.

By default, DNS uses the Dirty interface. The Clean interface is used for Secure Endpoint Private Cloud integrations and other services. If the Secure Endpoint Private Cloud hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI.

NTP Server Access

By default, the NTP server needs to be accessible via the Dirty network.

Starting with the 2.12 release, an appliance can be optionally configured to connect to an NTP server from the clean interface rather than the dirty interface (default). This makes it possible to use an internal NTP server.

Integrations

Additional planning is required if the Secure Malware Analytics Appliance is going to be used with other Cisco products, such as the Email Security Appliance, Web Security Appliance, or Secure Endpoint Private Cloud. See Connecting ESA/WSA to Threat Grid Appliance for more information.

DHCP Requirements

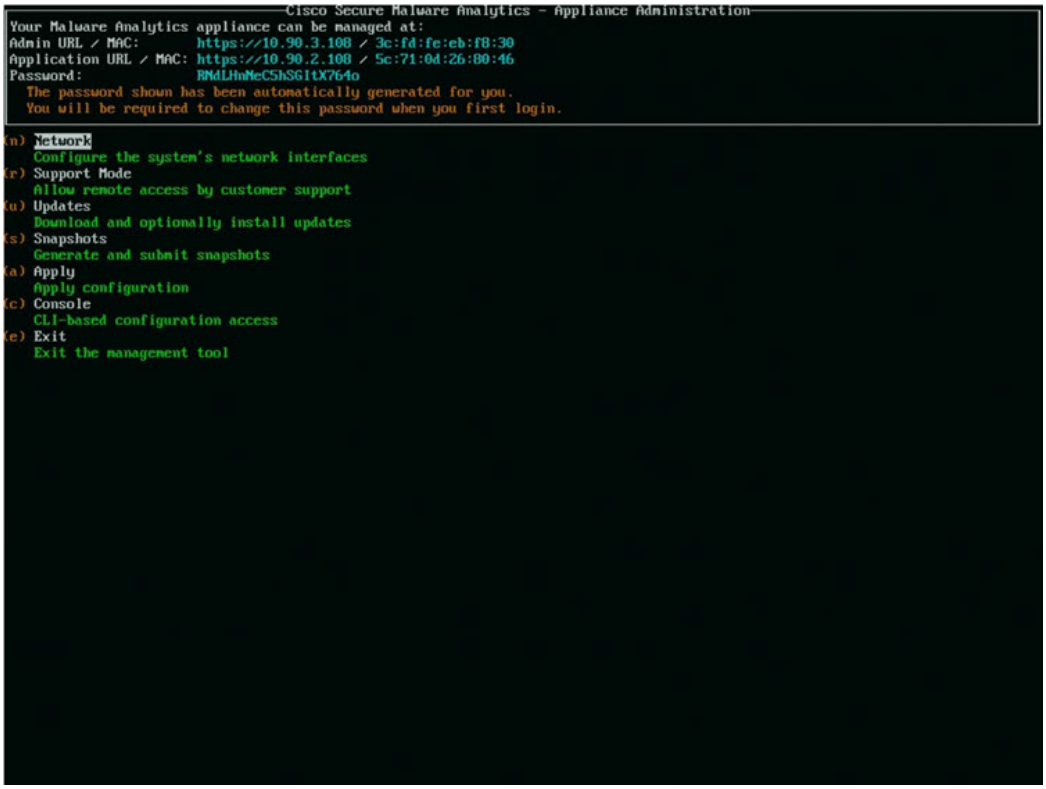
If you are connected to a network configured to use DHCP, it is important that you understand the requirements. Secure Malware Analytics Appliances that use DHCP need to explicitly specify DNS.

Warning An upgrade of a system without a DNS server explicitly specified will fail.

Note The Admin TUI displays the information you will need to access and configure the Admin UI. It may take some time for the IP addresses for DHCP to display after your appliance boots.

Open the Admin TUI (Text-mode UI) and note the following information:

Figure 2: Admin TUI (Connected to a Network Configured to Use DHCP)



- **Admin URL** - The Admin network. You will need this address in order to continue the remaining configuration tasks in the Admin UI.
- **Application URL** - The Clean network. This is the address to use after completing the configuration in the Admin UI.

  The Dirty network is not shown.
- **Password** - The initial Admin password that is randomly generated during the Secure Malware Analytics Appliance installation. You will need to change this password later as the first step the Admin UI configuration process.

If you need to change your initial IP assignments from DHCP to static IP addresses, see Configuring Network and DHCP.

License

When a new appliance is purchased, a license is generated and the **Retrieve License From Server** button on the **Configuration > License** page is enabled. However, if that does not work or if there is a special case (such as a license being a custom one-off), then you will be given the license directly, as an encrypted file with a password.

For additional questions about licenses, contact Support.

Rate Limits

The API sample submission rate limit is global for the Secure Malware Analytics Appliance under the terms of the license agreement. This affects API submissions ONLY, not manual sample submissions.

Rate limits are based on a window of rolling time, not to a calendar day. When the submission limit is exhausted, the next API submission will return a 429 error, plus a message about how long to wait before retrying. See the portal online Help for more information.

Organizations and Users

Once you have completed the Secure Malware Analytics Appliance setup and network configuration, you must create the initial Secure Malware Analytics organizations and add user account(s), so that people can login and begin submitting malware samples for analysis. This task may require planning and coordination among multiple organizations and users, depending on your requirements.

See Create New Organizations and the Secure Malware Analytics portal Help (click **Administration** > **Administrator's Guide** to open the Administration Guide topic) for additional information.

Updates

The initial Secure Malware Analytics Appliance setup and configuration steps **must be completed** before installing any Secure Malware Analytics Appliance updates. We recommend that you check for updates immediately after completing the initial configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Secure Malware Analytics Appliance updates cannot be downloaded until the license is installed, and except where otherwise directed by the customer support, the update process requires that the initial appliance configuration is completed. Updates must be done in sequence.

User Interfaces

After the server has been correctly attached to the network and powered up, there are several user interfaces available for configuring the Secure Malware Analytics Appliance.

Note LDAP authentication is available for Admin TUI and the Admin UI. RADIUS authentication is available for the Secure Malware Analytics Application UI (v2.10 and later).

Admin TUI

The **Admin TUI** interface is used to configure the network interfaces. The Admin TUI is displayed when the Secure Malware Analytics Appliance successfully boots up.

Reconnecting to the Admin TUI

The Admin TUI remains open on the console and is accessed either by attaching a monitor to the appliance or, if CIMC is configured, via remote KVM.

Note CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

To reconnect to the Admin TUI, ssh into the Admin IP address as the user **threatgrid**.

The required password is either the initial, randomly generated password, which is visible initially in the Admin TUI, or the new Admin password you create during the first step of the Admin UI Configuration (see the *Cisco Threat Grid Appliance Getting Started Guide*).

Threat Grid Shell (tgsh)

The Threat Grid Shell (tgsh) is an administrator's interface that is used to execute commands (including destroy-data and forced backup), and for expert, low-level debugging. To access tgsh, choose **CONSOLE** in the Admin TUI.

Note The Admin UI uses the same credentials as the Secure Malware Analytics user, so any password changes/updates made via tgsh will also impact the Admin UI.

Caution Network configuration changes made with tgsh are not supported unless specifically directed by Secure Malware Analytics support; the Admin UI or Admin TUI should be used instead. Options to modify admin email, glovebox URL, SMTP configuration, and so on have been removed with the 2.12 release. The Wipe Appliance operation is now activated within recovery mode tgsh rather than the bootloader menu.

Admin UI

This is the primary Secure Malware Analytics user interface used for configuration. Much of the Secure Malware Analytics Appliance configuration can ONLY be done via the Admin UI, including licenses, email host, and SSL certificates.

Secure Malware Analytics Portal

The Secure Malware Analytics user interface application is available as a cloud service, and is also installed on Secure Malware Analytics Appliances. There is no communication between Secure Malware Analytics Cloud service and the Secure Malware Analytics Portal that is included with a Secure Malware Analytics Appliance.

Network Interfaces

The available network interfaces are described in the following table:

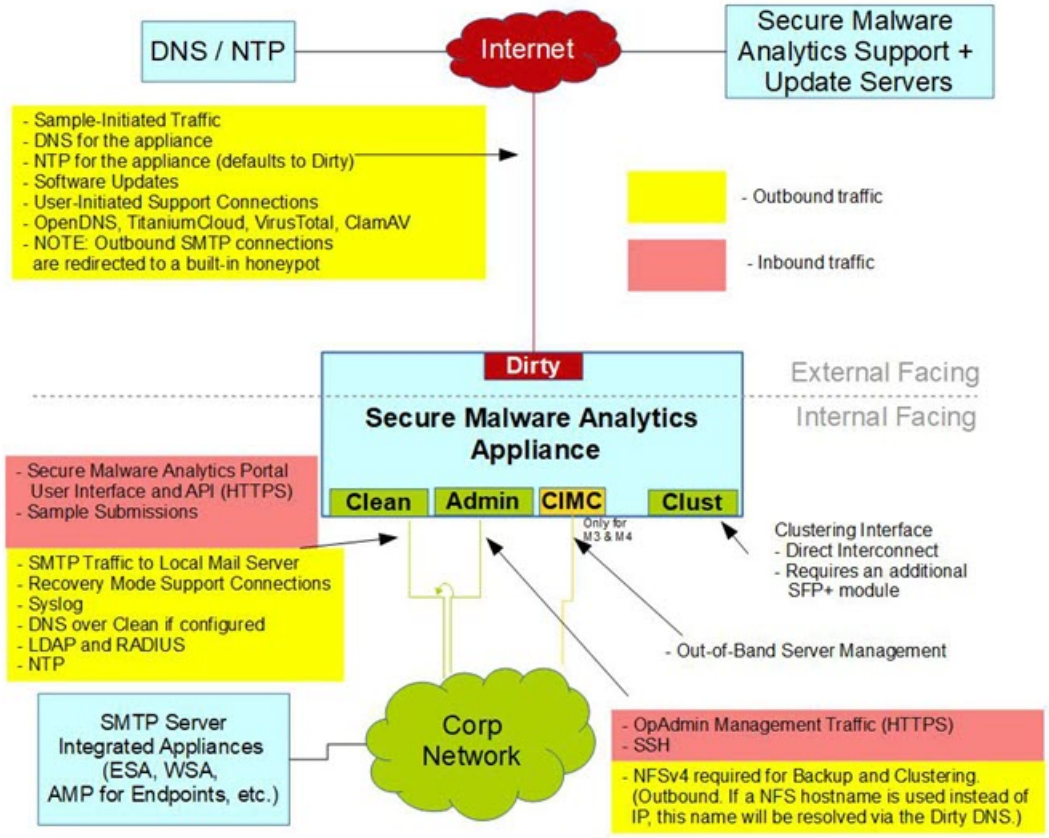
Interface	Description
Admin	• Connect to the Admin network. **Only inbound** from Admin network. • Admin UI traffic • SSH (inbound) for Admin TUI • NFSv4 for backups and clustering (Outbound. If a NFS hostname is used instead of IP, this name will be resolved via Dirty DNS.) Must be accessible from all cluster notes. • The Admin port can be disabled (from the tgsh shell); from the Admin UI with v2.11. When disabled, non-clustered Secure Malware Analytics Appliances can operate correctly with only the clean and dirty ports connected, and the admin UI will be presented on port 8443 of the clean interface (an also port 18443 with the v2.11 release). If the port is not disabled, unplugging the admin port results in a non-functional (or at best, a partially functional) Secure Malware Analytics Appliance. **Note** The form factor for the Admin interface is SFP+. See Hardware Requirements.
Clust	The non-Admin SFP+ port is used for clustering. • Clust interface required for clustering (optional) • Requires an additional SFP+ module for direct interconnect. This interface does not require any configuration. Addresses are automatically assigned.
Clean	• Connect to the Clean network. Clean must be accessible from the corporate network but requires no outbound access to the Internet. • UI and API traffic (inbound) • Sample submissions • SMTP (outbound connection to the configured mail server) • SSH (inbound for Admin TUI) • Syslog (outbound to configured syslog server) • ESA/WSA and CSA Integrations • Secure Endpoint Private Cloud Integration • DNS optional • LDAP (outbound) • RADIUS (outbound) • NTP (for using an internal NTP server)

Interface	Description
Dirty	Connect to the Dirty network; requires Internet access. Outbound Only. You should not use your own DNS (private IP) for the Dirty Interface because traffic sent to a private IP is dropped at the Network Exit Localization firewall. • DNS **Note** If you are setting up an integration with a Secure Endpoint Private Cloud, and the Secure Endpoint appliance hostname cannot be resolved over the Dirty interface, then a separate DNS server that uses the Clean interface can be configured in the Admin UI. • NTP (defaults to Dirty) • Updates • Support sessions • Support snapshots • Malware sample-initiated traffic • OpenDNS, TitaniumCloud, VirusTotal, ClamAV_signature updates • SMTP outbound connections are redirected to a built-in honeypot **Note** Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.
CIMC Interface	If the Cisco Integrated Management Controller (CIMC) interface is configured, it can be used for server management and maintenance. See CIMC Configuration. **Note** CIMC is not supported on the Secure Malware Analytics M5 Appliance server.

Network Interface Setup Diagram

This section describes the most logical and recommended setup for a Secure Malware Analytics Appliance. However, each customer's interface setup is different. Depending on your network requirements, you may decide to connect the Dirty interface to the inside, or the Clean interface to the outside with appropriate network security measures in place.

Figure 3: Network Interfaces Setup Diagram



Note In Secure Malware Analytics Appliance (v2.7.2 and later), the **enable_clean_interface** option is available but is disabled by default. This option (after applying configuration and rebooting) enables access to the administrative interface on port 8443 and 18443 of the assigned clean IP. Disabling the admin ethernet interface will also enable this access on port 8843 of clean.

Firewall Rules

This section provides suggested firewall rules.

Note Implementing a restrictive outgoing policy on the Dirty interface for ports 22 and 19791 requires tracking updates over time and spending more time maintaining the firewall.

Note Using IPv4LL address space (168.254.0.16) for the Dirty interface is not supported.

Dirty Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	ANY	ANY	Allow	Allow outbound traffic from samples, optionally proxied through Cisco datacenters. (To get accurate results it is required that malware be allowed to contact its command and control server using whatever port and protocol it is designed to use.)

Dirty Interface Inbound

Source	Destination	Protocol	Port	Action	Note
ANY	Dirty Internet	ANY	ANY	Deny	Deny all incoming connections.

Clean Interface Outbound

Source	Destination	Protocol	Port	Action	Note
Clean Interface	SMTP Servers	TCP	25	Allow	The appliance uses the clean interface to initiate SMTP connections to the configured mail server.

Clean Interface Outbound (Optional)

Source	Destination	Protocol	Port	Action	Note
Clean Interface	Corporate DNS Server	TCP/UDP	53	Allow	Optional, only required if Clean DNS is configured.
Clean Interface	AMP Private Cloud	TCP	443	Allow	Optional, only required if Secure Endpoint Private Cloud integration is used.
Clean Interface	Syslog Servers	UDP	514	Allow	Allow connectivity to server designated to receive Syslog messages and Secure Malware Analytics notifications.
Clean Interface	LDAP Servers	TCP/UDP	389	Allow	Optional, only required if LDAP is configured.

Source	Destination	Protocol	Port	Action	Note
Clean Interface	LDAP Servers	TCP	636	Allow	Optional, only required if LDAP is configured.
Clean Interface	RADIUS Servers	DTLS	2083	Allow	Allow login to Secure Malware Analytics application UI (Face). Optional, only required if RADIUS is configured.
Clean Interface	Internet	UDP	123	Allow	Optional, use this off-by-default functionality to use an internal NTP server.

Clean Interface Inbound

Source	Destination	Protocol	Port	Action	Note
User Subnet	Clean Interface	TCP	22	Allow	Allow SSH connectivity to the Admin TUI.
User Subnet	Clean Interface	TCP	80	Allow	Appliance API and Secure Malware Analytics user interface. This will redirect to HTTPS TCP/443.
User Subnet	Clean Interface	TCP	443	Allow	Appliance API and Secure Malware Analytics user interface.
User Subnet	Clean Interface	TCP	9443	Allow	Allow connectivity to the Secure Malware Analytics UI Glovebox.

Admin Interface Outbound (Optional)

The following depends on what services are configured.

Source	Destination	Protocol	Port	Action	Note
Admin Interface	NFSv4 Server	TCP	2049	Allow	Optional, only required if Secure Malware Analytics Appliance is configured to send backups to an NFSv4 share.

Admin Interface Inbound

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	22	Allow	Allow SSH connectivity to the Admin TUI.

Source	Destination	Protocol	Port	Action	Note
Admin Subnet	Admin Interface	TCP	80	Allow	Allow access to the Admin UI. This will redirect to HTTPS TCP/443.
Admin Subnet	Admin Interface	TCP	443	Allow	Allow access to the Admin UI.

Dirty Interface for Non Cisco-Validated/Recommended Deployment

Non Cisco-Validated/Recommended - Firewalling outbound traffic can reduce efficacy by preventing malware from connecting to command and control infrastructure, limiting efforts to determine what would be downloaded from that command and control infrastructure.

Source	Destination	Protocol	Port	Action	Note
Dirty Interface	Internet	TCP	22	Allow	Update, support snapshot, and licensing services.
Dirty Interface	Internet	TCP/UDP	53	Allow	Allow outbound DNS.
Dirty Interface	Internet	UDP	123	Allow	Allow outbound NTP.
Dirty Interface	Internet	TCP	19791	Allow	Allow connectivity to Secure Malware Analytics support.
Dirty Interface	Cisco Umbrella	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	VirusTotal	TCP	443	Allow	Connect with third-party detection and enrichment services.
Dirty Interface	TitaniumCloud	TCP	443	Allow	Connect with third-party detection and enrichment services.

Privacy and Sample Visibility

When submitting samples to a Secure Malware Analytics Appliance for analysis, an important consideration is the privacy of the content. Privacy is a particularly important consideration if sensitive documents or archive types are submitted for analysis, because locating sensitive material could be relatively easy for those with access to the Secure Malware Analytics Appliance, especially with the search API.

The privacy and sample visibility model for sample submissions to Secure Malware Analytics is as follows:

- Unless samples are designated as Private, they are visible to users who are outside the submitter's organization.

- Private samples can only be seen by Secure Malware Analytics users within the same organization as the user who submitted the sample.

Samples Submitted by Integrations

The privacy and sample visibility model is modified on Secure Malware Analytics Appliances for samples that are submitted by integrations. Integrations are Cisco products such as Email Security Appliance (ESA), Web Security Appliance (WSA), and other devices or third-party services (you may see the term CSA Integrations, which refers to ESA/WSA and other Cisco appliances, devices, and services that are integrated; for example, registered, with Secure Malware Analytics Appliance via the Cisco Sandbox API.)

All sample submissions on Secure Malware Analytics Appliances are Public by default, and can be viewed by any other appliance user, including integrations, regardless of the organization to which they belong. All appliance users can see all details of samples submitted by all other users.

Secure Malware Analytics users may also submit Private samples to the Secure Malware Analytics Appliance, which are only visible to other Secure Malware Analytics Appliance users, including integrations, from the same organization as the sample submitter.

Privacy and sample visibility model on Secure Malware Analytics Appliances are illustrated in the table.

Figure 4: Privacy and Visibility on a Secure Malware Analytics Appliance

Sample and Analysis Results are visible to:	Public Submissions (Default)	Private Submissions	CSA Integration Submissions (Public by Default)
Users from the Same Organization	✔	✔	✔
Users from a Different Organization	✔	✔	✔
CSA Integrations from the Same Organization	✔	✔	✔
CSA Integrations from a Different Organization	✔	✖	✔

- **Full Access** - The green check mark indicates that users have full access to the sample and the analysis results.
- **Scrubbed Reports** - The grey check mark indicates that the Private submission results are scrubbed. Users have partial access to the sample and analysis results, but all potentially sensitive information about the sample is removed. There are no filenames, process names, screenshots, or even specifics about its activity in the glovebox.

  We omit details from the Metadata section, such as the sample submitter's login information. If you encounter a hash from a private sample in the course of doing business, this will let alert you to known threats, and if you need more details, submit your own copy of the sample for full analysis.

Private samples may not be downloaded. Scrubbed reports include Artifacts (with filename removed), Behavioral Indicators, Domains, and IPs.

- **No Access** - The red X indicates that users have no access to the sample or the analysis results.

The same basic privacy rules apply to Secure Malware Analytics Appliance integrations with Secure Endpoint Private Cloud.

Wipe Appliance Operation

The Wipe Appliance operation enables you to wipe the disks on a Secure Malware Analytics Appliance to remove all data prior to decommissioning or returning it to the Cisco Demo Loan Program.

Important After performing the wipe appliance procedure, the Secure Malware Analytics Appliance will no longer operate without being returned to Cisco for reimaging (Except for demo loan program customers, re-imaging service is not guaranteed to be available without prior agreement).

For more information, see Removing All Data with the Wipe Appliance Operation.

Customer Data

Logs, active configuration, and other customer-owned data is now stored almost exclusively on the RAID 5 data array, rather than being distributed between data and OS drives. The remaining appliance-specific content stored on OS drives is limited to information required for correct operation of recovery mode should the data drives not be mountable, and has limited privacy impact if disclosed.

Because less content is stored on the OS array with the 2.12 release, early appliances (with smaller OS drives) are less likely to need to delete VM images other than the mandatory default image during a data reset (and thus need to download updates online before those deleted VM images become available again).