Intel® Hybrid Cloud platform
Version 3.0
User Guide

Order Number: G47804-001

Rev1.0

October 11, 2011

Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, lifesaving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

The Intel® Hybrid Cloud platform may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Table of Contents

List of Figures

List of Tables

1. About This Document

This User Guide describes in detail, the various features available for configuring and managing the Intel® Hybrid Cloud platform Version 3.0.

1.1 Intended Audience

This User Guide is written for Remote Administrators and end users in the SMB segment, who may want to manage the Intel® Hybrid Cloud server, activate new virtual appliances on the server and monitor virtual appliances running on the server.

1.2 Abbreviations

The following table displays the abbreviations used in this document:

Table 1. Abbreviations

Term	Description
ARP	Address resolution protocol
BMC	Baseboard Management Controller
CLI	Command line interface
DDC	Display Data Channel
DHCP	Dynamic Host Configuration Protocol
DVC	Dambrackas Video Compression
DVO	Dynamic Visual Output
FPGA	Field Programable Gate Array
ICMP	Internet Control Message Protocol
Intel® AMT	Intel® Active Management Technology refers to Intel's management architecture with consistent cross platform capabilities, interfaces, and protocols. Intel® AMT offers a HW chipset based solution for remote out-of-band management, using a secondary processor on the motherboard, with embedded firmware that runs on the Manageability Engine (ME).
Intel® Hybrid Cloud platform	Intel® Hybrid Cloud platform is a unique Hardware and Software solution that is remotely managed and is targeted at small and medium businesses that have a business need for simplified IT functionality.
Intel® RMM3	Intel® Remote Management Module 3
IPMI	Intelligent Platform Management Interface
ITE	Information Technology Equipment
IXE	Intel® Hybrid Cloud Command Line Tool
KVM	Keyboard, video and mouse

Term	Description
LAS	Local Application Store is a local storage repository on the server that contains appliances.
MAC	Media Access Controller
OOB	Out of Band channel, can be used to access a system that is powered down and does not have an OS running.
PBDE	Polybrominated Biphenyls Diphenyl Ethers
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control.
Remote Administrator / MSP	A Managed Service provider (MSP) who interfaces between Intel and the End-User (to provide remote management services).
RMII	Reduced Media Independent Interface
RTC	Real-Time Clock
SMB	Small and Medium Businesses
TCP/IP	Transmission Control Protocol/Internet Protocol
TPS	Technical Product Specification
UART	Universal asynchronous receiver transmitter
UDP	User Datagram Protocol
Virtualization (Intel® VT)	The hardware implementation of Intel® Virtualization Technology (that is, Intel® VT), enables multiple guest OSs and applications (together known as Virtual Machines or VMs) to co-exist on the same computer platform.
VMM*	Virtual Machine Manager, refers to third party ISV SW that uses Intel® VT to enable remote management of VMs.

1.3 Additional Information

For additional information not covered in this guide, refer to our Support page:

http://www.intelhybridcloud.com/support.html

NOTE: You must be logged in to view Confidential content.

2. Intel® Hybrid Cloud platform Overview

The Intel® Hybrid Cloud platform offers small business customers cloud-like flexibility, providing an innovative solution, which implements a subscription-based model for providing locally-hosted server software on a pay-as-you-go basis. Small businesses get all of the benefits of services in the cloud, with the responsiveness and consistency of local applications, plus the security of having data on site.

2.1 Key Elements

The Intel Hybrid Cloud platform is composed of four key elements:

- Intel® Hybrid Cloud server resides on the customer premises and hosts the customer appliances, applications and data locally.
- Intel® Hybrid Cloud software stack runs on the Intel® Hybrid Cloud server on top of a Virtual Machine Monitor (VMM).
- Intel® Hybrid Cloud management portal is an internet accessible asset management site for all of your Intel® Hybrid Cloud Servers. This remotely accessible site allows you to register your servers and manage appliance activation and expiration for each of your customers from any location with an internet connection. Additional details about the Intel® Hybrid Cloud Web Portal are provided in Section 5.
- Intel® Hybrid Cloud server manager provides you with the power to manage your Intel® Hybrid Cloud Servers and users remotely.

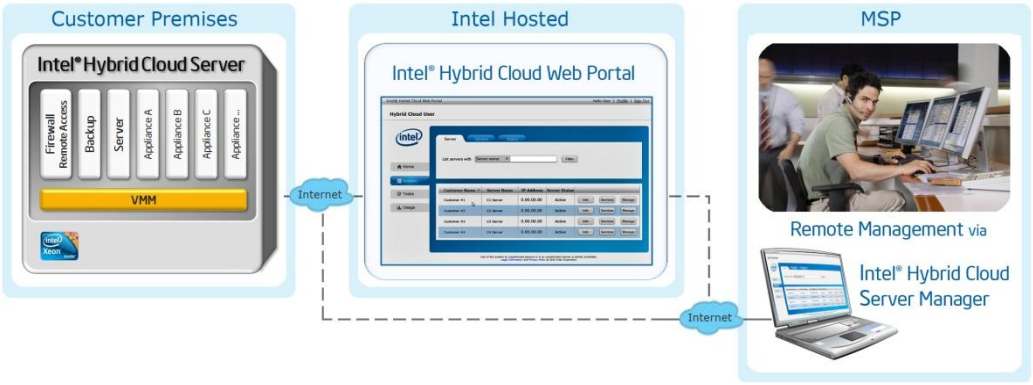

Figure 1: Elements in the Intel® Hybrid Cloud platform

2.1.1 Intel® Hybrid Cloud server

The Intel® Hybrid Cloud server is equipped with the technical ingredients required to support the Intel® Hybrid Cloud software stack, including Intel® Active Management Technology for remote manageability, Intel AMT/BMC and a Trusted Platform Module.

2.1.2 Intel® Hybrid Cloud software stack

The Intel® Hybrid Cloud software stack is a core component that runs on top of a Virtual Machine Monitor (VMM) on the Intel® Hybrid Cloud server. This software provides an abstraction layer over VMM, making it easy to deploy, configure and manage the Intel Hybrid Cloud server. Both Linux* and Microsoft Windows* guest operating systems are supported within the VMM, to run a variety of end-user applications.

2.1.3 Intel® Hybrid Cloud management portal

The Intel® Hybrid Cloud management portal (web interface) requires a valid username and password to access, and is available to authorized remote administrators. Through this portal, you can register your Intel® Hybrid Cloud Servers and activate appliances for your customers. Additional details about the Intel® Hybrid Cloud management portal are provided in Section 5 of this document.

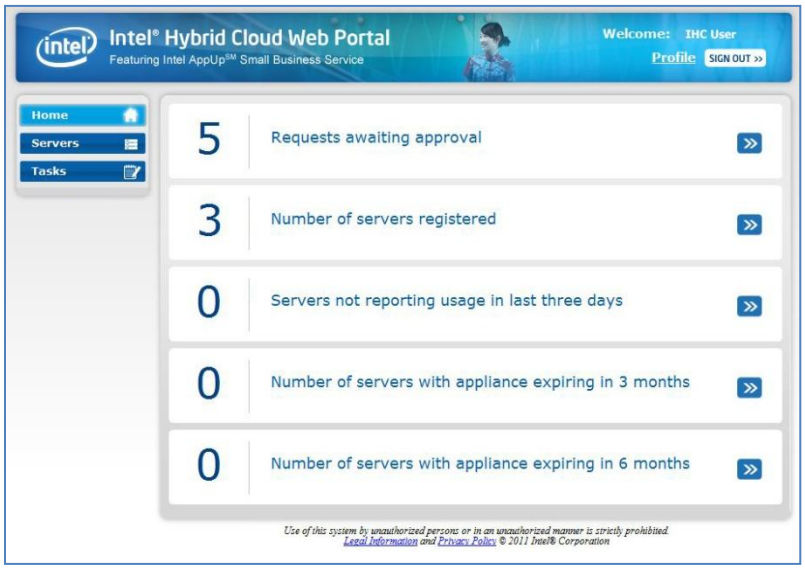

Figure 2. Intel® Hybrid Cloud management portal

2.1.4 Intel® Hybrid Cloud server manager

This user-friendly interface enables remote monitoring, server configuration and management. Since each software appliance runs on a separate virtual machine, you can manage and isolate appliances individually for reconfiguration or troubleshooting. Additional details are provided in Section 5 of this document.

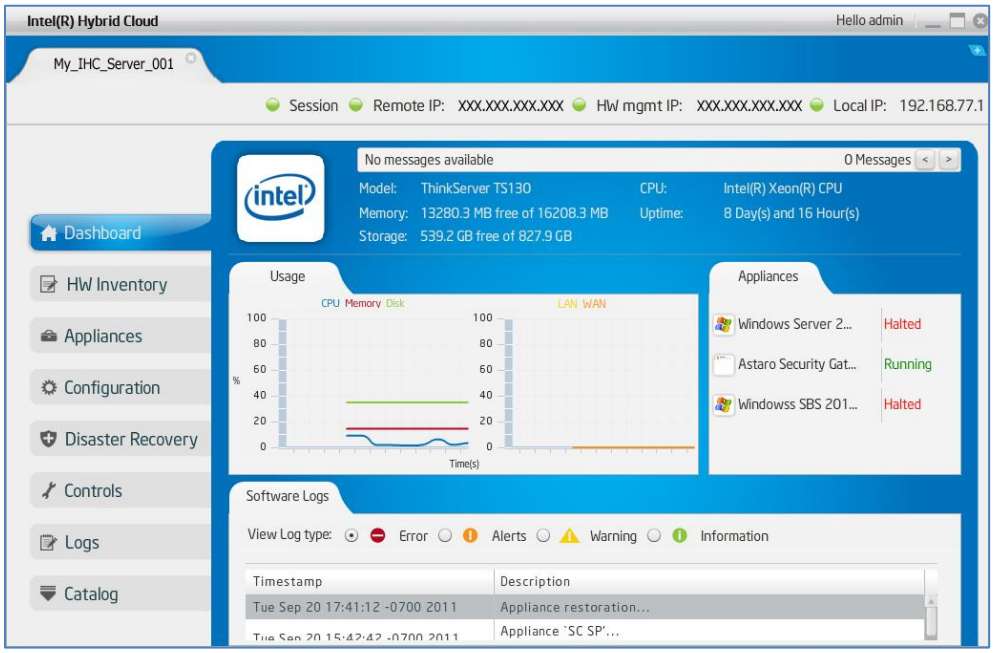

Figure 3. Intel® Hybrid Cloud server manager

Also available in the Intel® Hybrid Cloud Server Manager is a command line utility (called IXE). IXE is available as part of Intel® Hybrid Cloud server manager and can be used for configuring and managing Intel® Hybrid Cloud servers. Additional details for IXE commands are provided in Section 11 of this document.

2.2 Usage Reporting

A core feature of the Intel Hybrid Cloud platform is its ability to track usage of services, and to report those statistics to the Intel® Hybrid Cloud data center. Unique Client IDs are used to anonymously track and report software usage, so your customer's identity is never transmitted beyond the local server. Usage reports are provided to you on a monthly basis and include itemized details for the services used on each of the servers you manage. In turn, you can use this data to add margin to the monthly software subscriptions used by your customers.

The Intel® Hybrid Cloud Server must be connected to the internet (and communicating with the Intel® Hybrid Cloud data center) in order to provide accurate usage reports. Communication with the data center is also required for software downloads from the Intel® Hybrid Cloud catalog, and for patches to components of the Intel® Hybrid Cloud software stack.

NOTE: To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

3. Before You Get Started

3.1 Items you will Need

In addition to the Intel® Hybrid Cloud server, you will also need the following Items:

- Local Computer (see Section 3.2 for details)
- Internet Connection
- 2 CAT5 Ethernet Cables (for Remote & Local IP Connections)
- Your Login information (Intel® Hybrid Cloud user ID & PW)
- Preliminary Setup Guide (in the box with the hardware)
- Password Guide (in the box with the hardware)
- Password List (you must log in to http://www.intelhybridcloud.com/ to download from the this document from the "**Support**" page)

3.2 Local & Management Computer Requirements

A local computer is required to setup and register your Intel® Hybrid Cloud server. You can use the same computer or a different computer to remotely manage your Intel® Hybrid Cloud servers. The system requirements are listed here:

Minimum Hardware Requirements

- Intel® Pentium® 4 Processor 2GHz
- 1GB RAM

Supported Operating Systems

Your management computer will need to run one of the following supported operating systems

- Microsoft Windows XP*
- Microsoft Windows 7*
- Microsoft Windows 2008*

Supported Web Browsers

A supported web browser is required to access the Intel® Hybrid Cloud management portal. The following browsers are currently supported (minimum version listed):

- Mozilla Firefox* 3.6
- Microsoft Internet Explorer* 7.0
- Google Chrome* 10.0

4. Getting Started

This section will help you set up and configure the Intel® Hybrid Cloud platform and management software.

IMPORTANT: Read all cautions and warnings (provided with the hardware) before powering-up the system.

4.1 External Firewall Settings

If an external firewall is used, ensure the following:

- The Intel® Hybrid Cloud server may not contain any Software Firewall appliance.
- All the client machines are to be directly connected to the external firewall.
- All the interfaces of the appliances on the server should use the remote interface (from "Appliances" select the Appliance, then select the Configure tab and scroll to Network section, and ensure the Network is using a remote interface).
- The appropriate Ports must be Forwarded.

4.1.1 Port Forwarding

The following Ports should be forwarded when using an external firewall/router (i.e. a firewall that is not an appliance running on the Intel® Hybrid Cloud Server). Confirm that your external firewall is not blocking these ports. For details regarding your specific firewall/router, refer to the manufacturer's documentation. Use the appropriate table below for your server:

Table 2. Ports (AMT Configuration)

Servers with Intel® Active Management Technology (Intel® AMT)		
Inbound TCP Port	**Server IP Function**	**Forward to IP Address**
22	SSH to the Intel® Hybrid Cloud server	Server IP Address
16993	Used to manage the Intel® Hybrid Cloud server via Intel® AMT －out of band ‖ (OOB)	Server IP Address
16994-16995	Used to manage the Intel® Hybrid Cloud server via SOL	Server IP Address
5910-5920	VNC ports used to access virtual appliances remotely	Server IP Address
64440**	Used for server registration, management and IXE commands	Server IP Address
65222	Used by the script engine for debugging and executing critical tasks	Server IP Address
Outbound TCP Port	**Server IP Function**	**Requirement**
443	Intel® Hybrid Cloud server - Usage Reporting	Must be Open

**If the external firewall device cannot open Port 64440, refer to the Intel® Hybrid Cloud - Release Notes to change the management port.

Table 3. Ports (BMC Configuration)

Servers with Baseboard Management Controller (BMC)		
Inbound TCP Port	**Server IP Function**	**Forward to IP Address**
443	Intel® Remote Management Module 3 (RMM3)	BMC IP Address
8282	Used to manage the Intel® Hybrid Cloud server via BMC －out of band ‖ (OOB)	BMC IP Address
Inbound TCP Port	**Server IP Function**	**Forward to IP Address**
22	SSH to the Intel® Hybrid Cloud server	Server IP Address
5910-5920	VNC ports used to access virtual appliances remotely	Server IP Address
64440**	Used for server registration, management and IXE commands	Server IP Address
65222	Used by the script engine for debugging and executing critical tasks	Server IP Address
Outbound TCP Port	**Server IP Function**	**Requirement**
443	Intel® Hybrid Cloud server - Usage Reporting	Must be Open

**If the external firewall device cannot open Port 64440, refer to the Intel® Hybrid Cloud - Release Notes to change the management port.

4.2 Connect the Cables

NOTE: Intel® Hybrid Cloud servers have more than one network interface port (for Remote and Local connections). These RJ45 jacks are labeled for easy identification:

- Port "**A**" - Remote Network Interface (Default: DHCP)
- Port "**B**" - Local Network Interface (Default IP: 192.168.77.1)

Perform the following steps (as shown in either "**Figure 4**" or "**Figure 5**"):

1. Connect the Remote Network Interface port, labeled **"A"** on the Intel® Hybrid Cloud server, **to the broadband access device** (such as a cable modem, DSL modem etc).
2. Connect the power cable to the server, and to an appropriate power source.
3. Power-up the Intel® Hybrid Cloud server.
4. Before proceding to the next step, **allow 8 to 10 minutes** for the server to boot completely.
5. Connect the Local Network Interface port, labeled **"B"** on the Intel® Hybrid Cloud server, directly **to your Local Computer's network interface**.

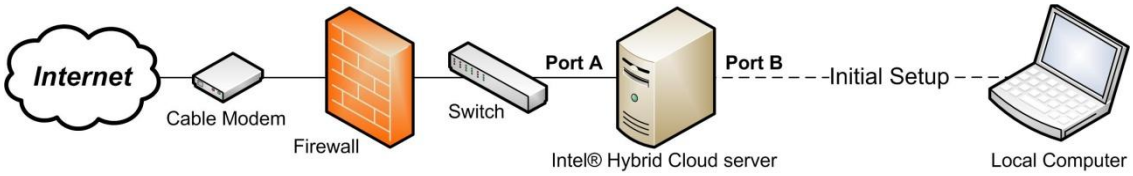

Figure 4. Initial Setup (server behind Firewall)

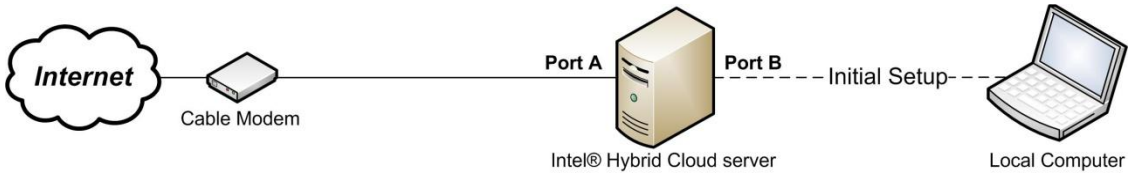

Figure 5. Initial Setup (server as Edge Device)

4.3 Establish Communication & Log In

1. Log into your local computer as the Administrator.
2. Change the network settings on your local computer to:

   IP: **192.168.77.42**

   Subnet Mask: **255.255.255.0**

3. Use a supported Internet browser to navigate to:

   https://192.168.77.1:64440/login

4. Choose “Continue to this website” at the Security Certificate warning.

5. Enter the default User Name and Password in the “**Connect**” login box:

   Username: **admin**

   Password: **Hybr1dC!0ud**

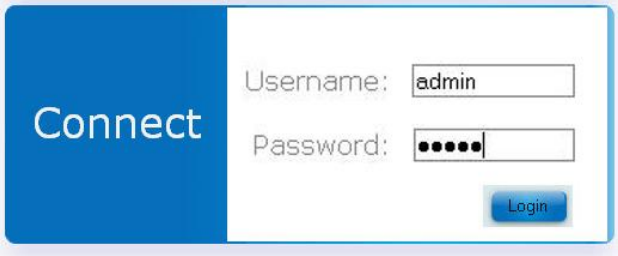

Figure 6. Connect screen

6. Click the “**Login**” button.
7. Read and Accept the “**Intel End User Software License Agreement**.”

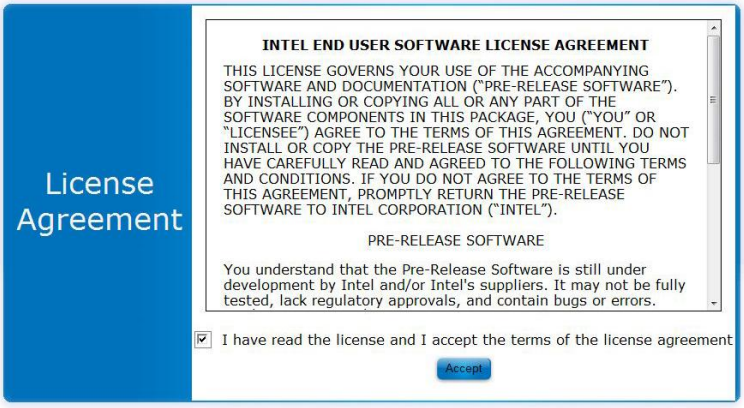

Figure 7. Software License Agreement

4.4 Configure the Network

Choose the appropriate network setting.

- **DHCP** - The values will automatically populate:
    1. Click the "**Keep the Same**" button.
- **Static IP**:
    1. Enter the appropriate network configuration values.
    2. Click the "**Update**" button.

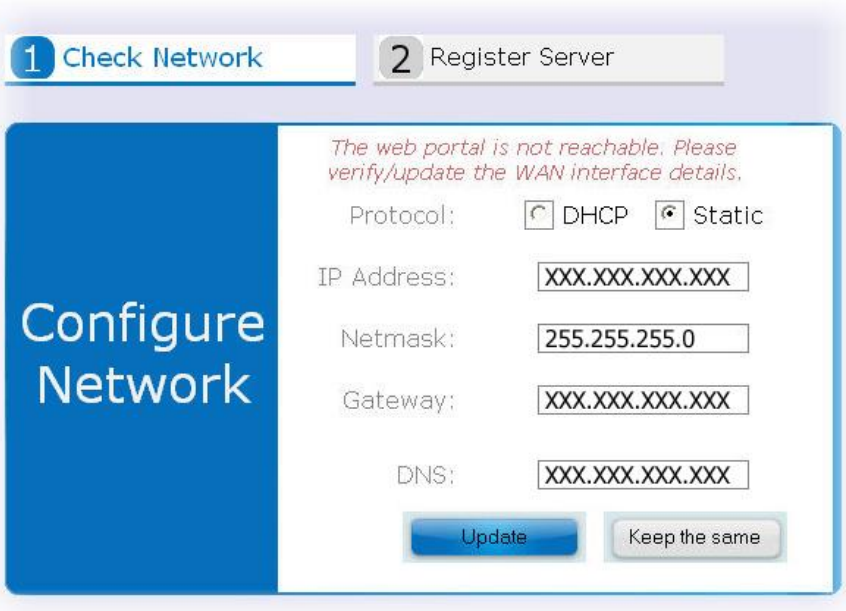

Figure 8. Configure Network screen

4.5 Register the Server

1. Enter a "**System Name**" (no spaces allowed).
   NOTE: The System Name (Server Name) will differentiate this server from your other servers in the Intel® Hybrid Cloud management portal.

2. Enter your "**Remote Administrator ID**" (i.e. same as your Intel® Channel account).
   ATTENTION: Management of this server will be limited to this Administrator ID.

3. Click the "**Register**" button.

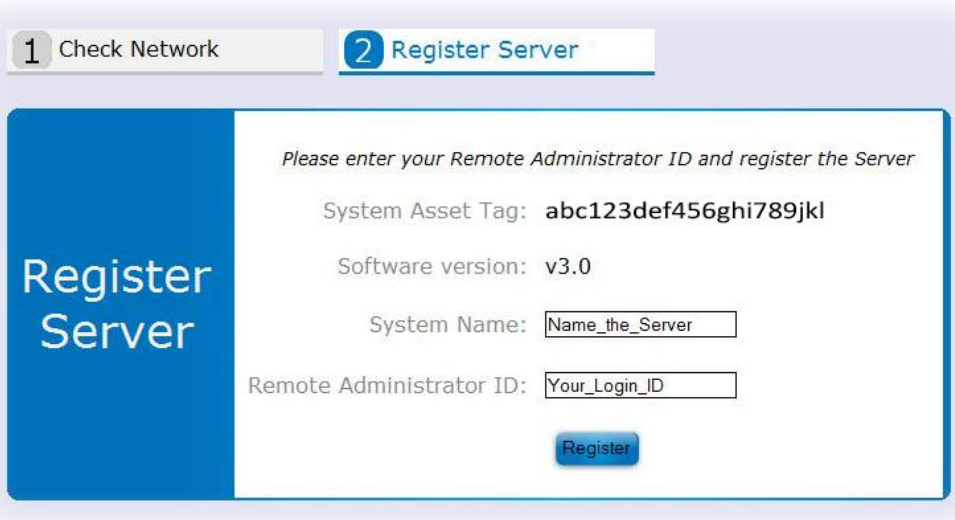

Figure 9. Register Server screen

4.6 Record Data & Download Tools

ATTENTION: Leave the browser open for Steps 4.6 & 4.7 (to install the software and activate the server).

1. Record the data from the Server Configuration box to corresponding spaces on the Intel® Hybrid Cloud - Server Management Info form (required for Step 4.8).

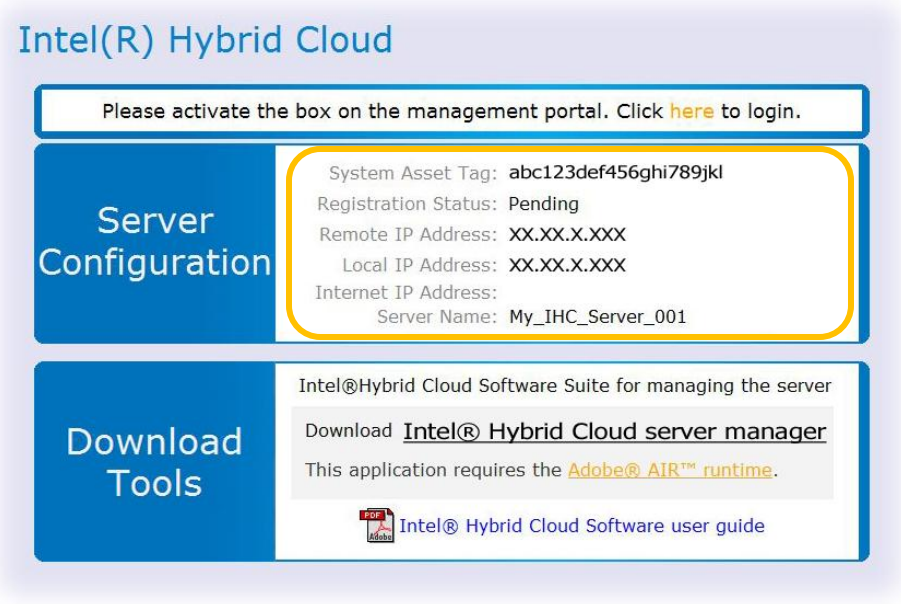

Figure 10. Record the Server Data

2. Disconnect the local computer's network interface from the Intel® Hybrid Cloud server.

3. Connect the local computer to the internet.

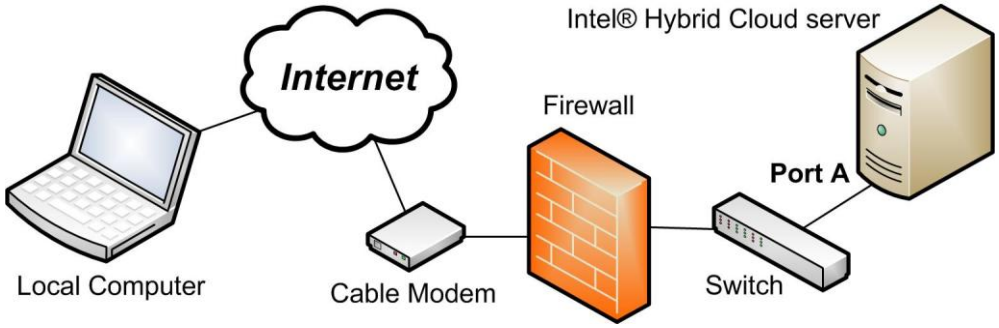

Figure 11. Connect to the Internet (server Behind Firewall)

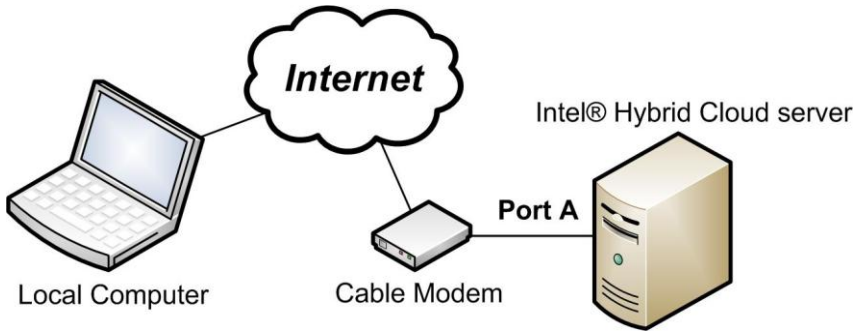

Figure 12. Connect to the Internet (server as Edge Device)

4. Reconfigure the local computer's network settings to access the internet.

5. Under the "**Download Tools**" heading, click the "**Intel® Hybrid Cloud server manager**" link.

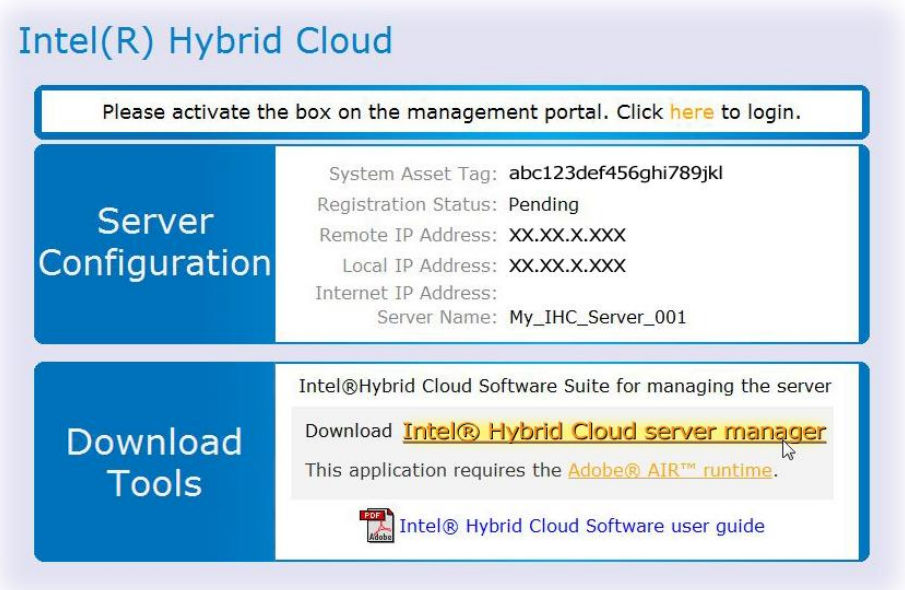

Figure 13. Download Tools

6. Install the Certificates in the store titled "**Trusted Root Certification Authorities**."

   IMPORTANT: Adobe* Air Version 2.7.1 is required and will install with the Intel® Hybrid Cloud server manager software.
   Do NOT Update Adobe* Air (other versions are NOT compatible).

   NOTES:

   - Even if you have previously downloaded the software tools, you may not have the current versions of the tools. If you have already downloaded the current tools, you can skip this step.
   - When you download Intel® Hybrid Cloud server manager, IXE command line tools are automatically downloaded to the client machine. Please refer to chapter 10 for more details on IXE tool usage.
   - If the Adobe Shockwave Flash Player* plugin is installed, an "**Install Now**" button will be provided

7. Return to the browser window and continue to the next step.

4.7 Activate the Server

1. In the upper box, follow the "**Click here to login**" link
   (or go to https://hybridcloud.intel.com in a web browser).

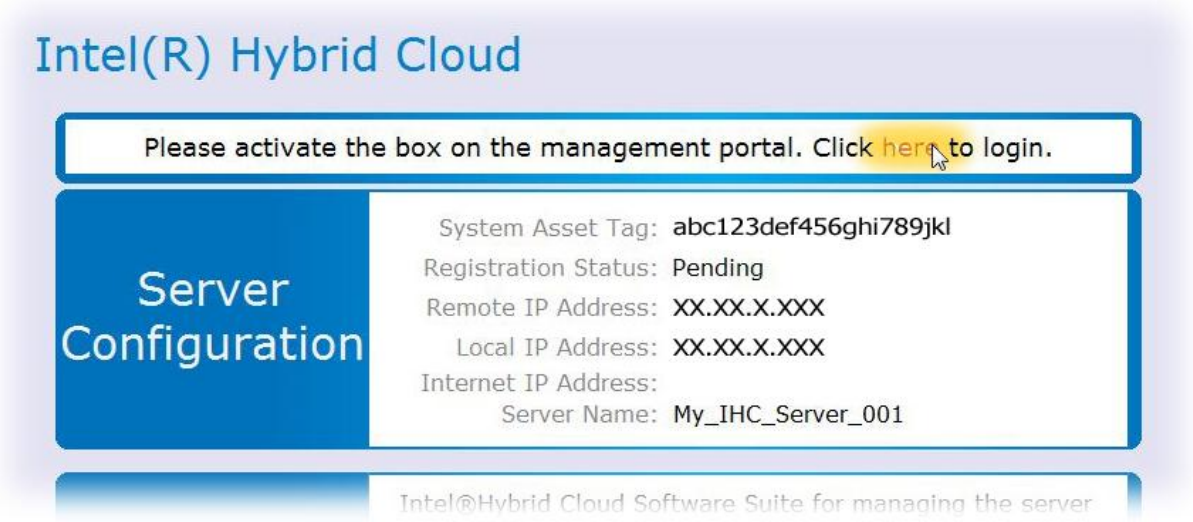

Figure 14. Click Here to Login

2. Enter your Remote Administrator ID ("**Login ID**") and Password.

3. Click the "**Login**" button.

Figure 15. Login screen

4. Select the "**Tasks**" menu bar (on the left).

5. Click the "**Activate**" link (for the new server).

Figure 16. Activate the Server

6. Enter a name for your customer in the "**Customer Name**" space.

7. Click the "**Confirm**" button.

Figure 17. Enter the Customer's Name

NOTE: If you have additional pending registrations, you can activate the servers by repeating the steps above.

4.8 Connect to the Server

1. Select the "**Servers**" menu bar (on the left).
2. Click the "**Manage**" link (for the new server).
3. Click the Intel® Hybrid Cloud server manager icon.

Figure 18. Manage the Server

4. Select the "**Connect**" tab.

5. Enter the remote login information in the "**Connect to Server**" screen:

   - Server Name..... (created in Step 4.5)
   - User Name..... **admin**
   - SW Management Password..... **`Hybr1dC!0ud`**

6. Click the "**Connect**" button.
   TIP: If you are experiencing difficulty with the server connection, refer to Section 4.1 for external firewall and Port Forwarding details.

Figure 19. Connect to Server screen

7. Enter the Remote IP address.

8. Press the "**Add**" button.

Figure 20. Add Server screen

9. Install the Certificate in the store titled "Trusted Root Certification Authorities."

10. At the prompt, change the SW Management Password.

5. Intel® Hybrid Cloud management portal

The internet accessible Intel® Hybrid Cloud management portal features a user friendly interface to register, activate and remotely manage your Intel Hybrid Cloud servers. Through the management portal, you can also download new applications, manage users, and monitor subscription usage.

5.1 Accessing Intel® Hybrid Cloud management portal

1. From your Local Computer, use one of the supported web browsers (identified in Section 3.2) to navigate to the following address:

   https://hybridcloud.intel.com

2. Login to the Intel® Hybrid Cloud management portal using your Remote Administrator ID (Intel® Channel ID).

Figure 21. Management Portal - Login screen

Inactivity of more than five minutes on the Intel® Hybrid Cloud management portal will automatically log the user (or administrator) out. For password recovery information, refer to the "**Password**" section of the "**Intel® Hybrid Cloud - Troubleshooting Guide**."

5.2 Management Portal - Dashboard

The dashboard in the Intel® Hybrid Cloud management portal (Figure 22) shows an overview of the servers you manage and pending requests (for servers to be approved), as well as, some additional management alert links. Also displayed are the menu buttons (on the left) that allow you to navigate to various functional screens throughout the management portal.

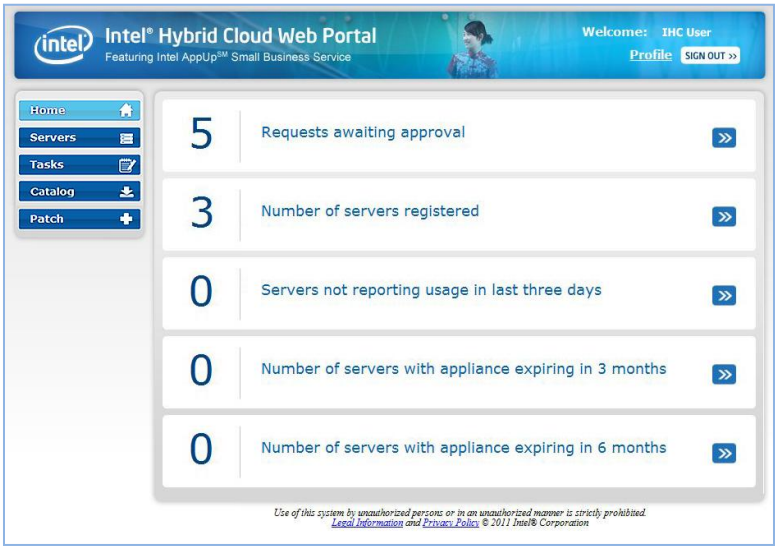

Figure 22. Management Portal - Dashboard

5.3 Managing Servers

Select the "**Servers**" menu button to access the "**Servers**" screen where you can view and modify the expiration dates for appliance licenses, or activate and deactivate the appliances for all of your registered servers. You can also launch the Intel® Hybrid Cloud server manager to monitor or perform maintenance on individual servers.

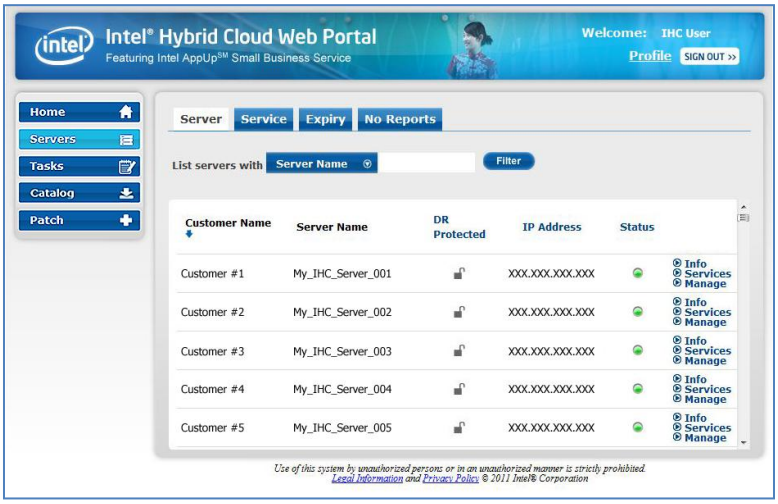

Figure 23. Management Portal – Servers screen

In the "**Servers**" tab on the "**Servers**" screen (Figure 23 above), the following items are available:

- **Info** - Provides details about the server (including VMM expiry, System Asset Tag, System HW serial number, Intel® Hybrid Cloud software stack version).
- **Services** - Displays a list of appliances installed on the server. You can activate/deactivate and change the expiry date of the appliance licenses. Default appliance expiry is set to three years.
- **Manage** – Provides a link to open the Intel® Hybrid Cloud server manager where you can perform additional server manage functions. Refer to Section 6 for details.

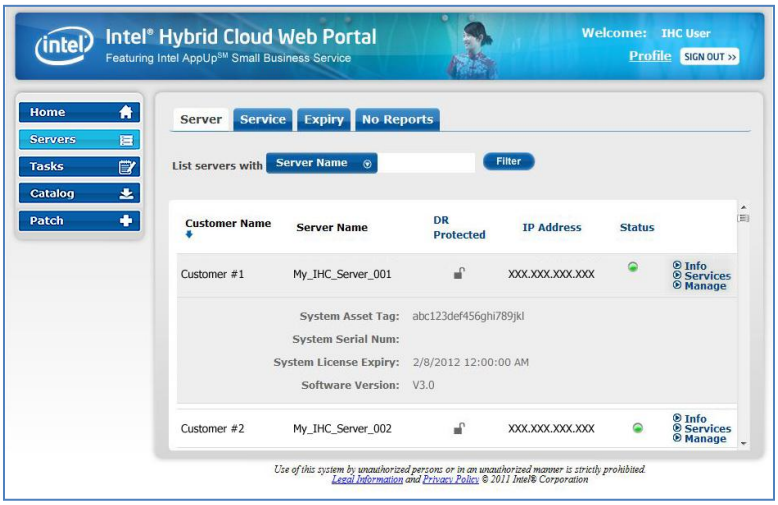

Figure 24. Management Portal – Servers Screen – Info

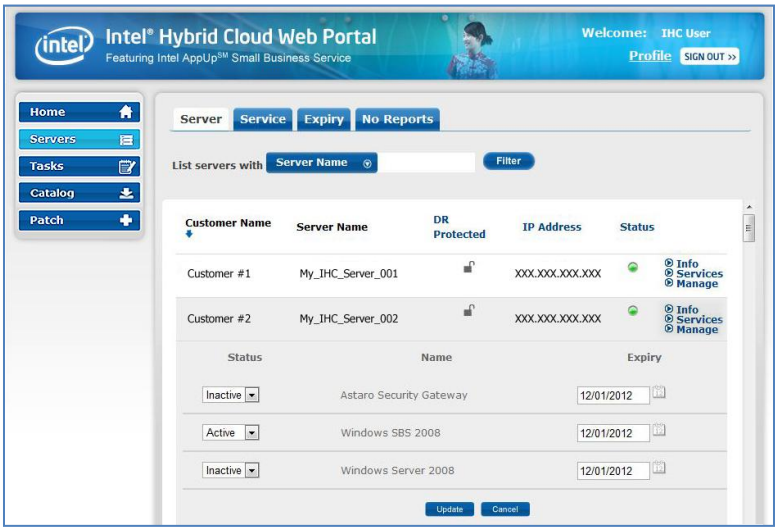

Figure 25. Management Portal – Servers Screen - Services

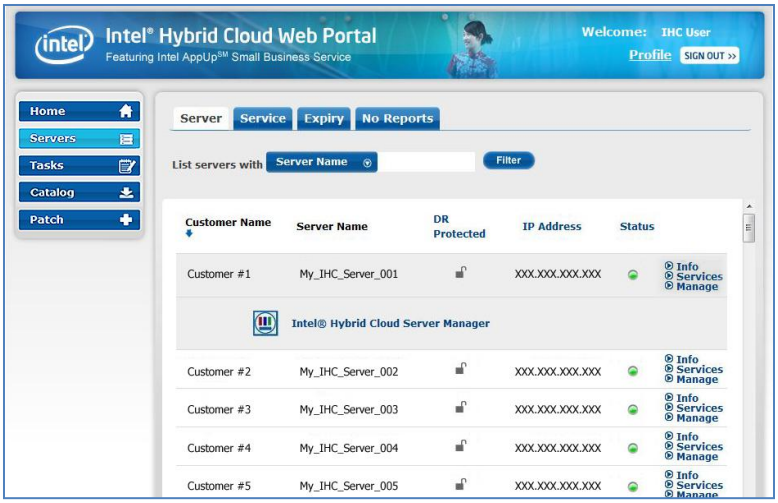

Figure 26. Management Portal –Servers screen - Manage

5.4 Viewing Your Profile

The "**Profile**" link (next to the "**SIGN OUT**" button on the top right) allows you to view your contact information (note: You cannot edit this information here).

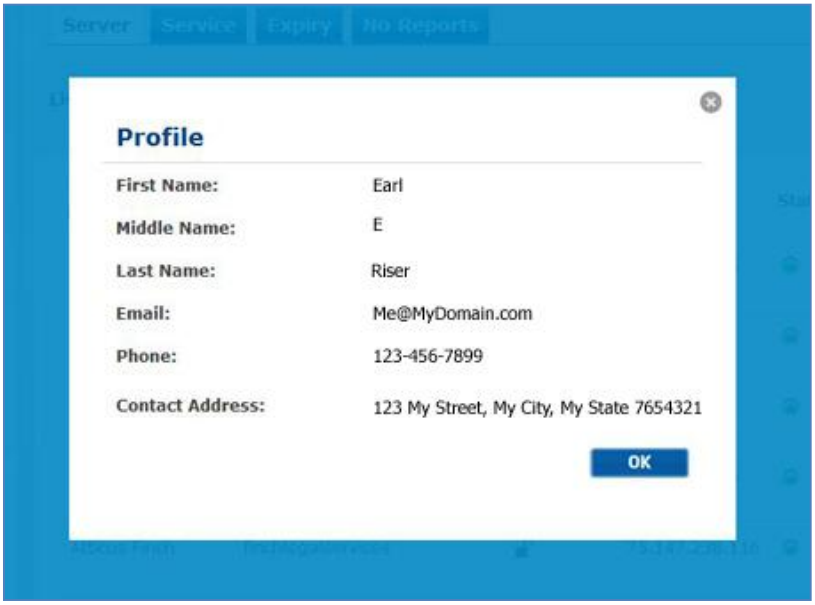

Figure 27. Management Portal – Your Profile

5.5 Appliance & Application Installation

One new feature introduced in Intel® Hybrid Cloud 3.0 allows you to choose and install appliances and applications directly from the Intel AppUp℠ Small Business Service catalog. **NOTE:** Appliance and application installation can also be performed through Intel® Hybrid Cloud server manager. Refer to Section 0 to access the Intel® Hybrid Cloud server manager, and Section 6.12 for appliance and application installation details.

1. Select the "**Catalog**" tab on the left side of the management portal.

2. Click the "**Install**" button for the desired appliance or application.

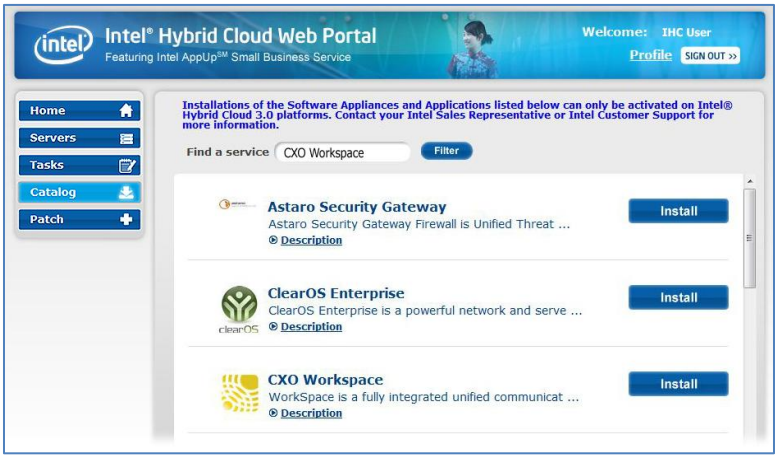

Figure 28 Management Portal - Catalog

NOTE: A search function is provided to quickly find a particular appliance or application. Some software is not compatible with servers running older versions of the Intel® Hybrid Cloud software stack.

1. Select the appropriate server from the list.

2. Click the "**Next**" button.

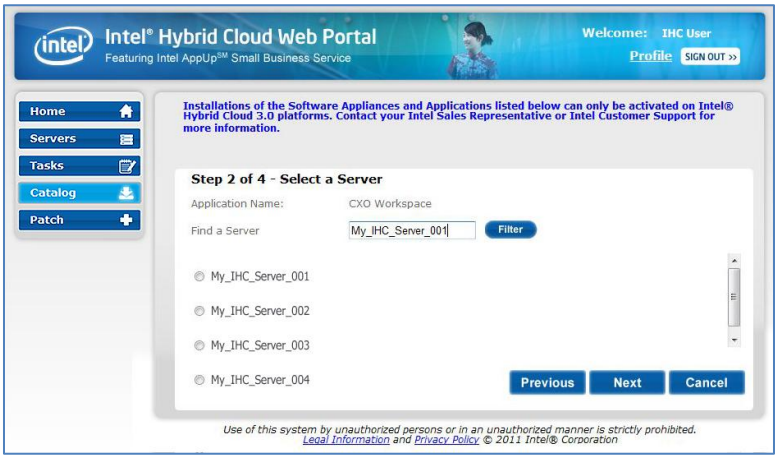

Figure 29 Management Portal – Catalog - Select a Server

3. If you are installing an Application, select the appropriate Appliance (for the installation).
   NOTE: If installing an appliance, this screen will not appear.

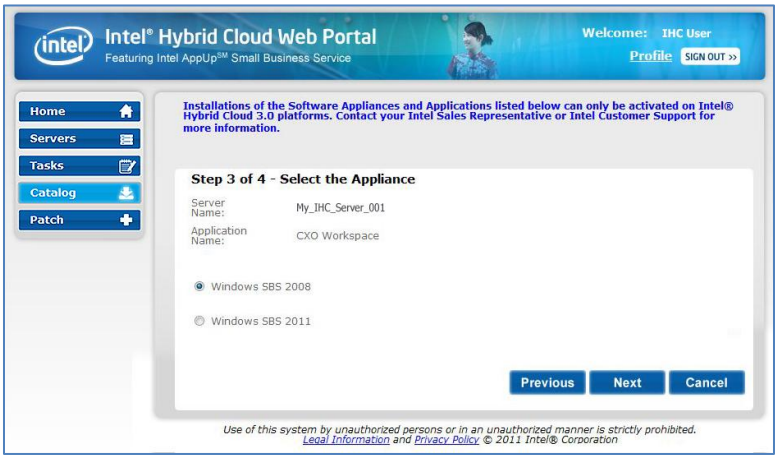

Figure 30 Management Portal – Catalog - Select the Appliance

4. If you are installing an Application, read the End User License Agreement (EULA), and accept the terms and conditions by checking the corresponding box.

5. Click the "**Confirm**" button to proceed.

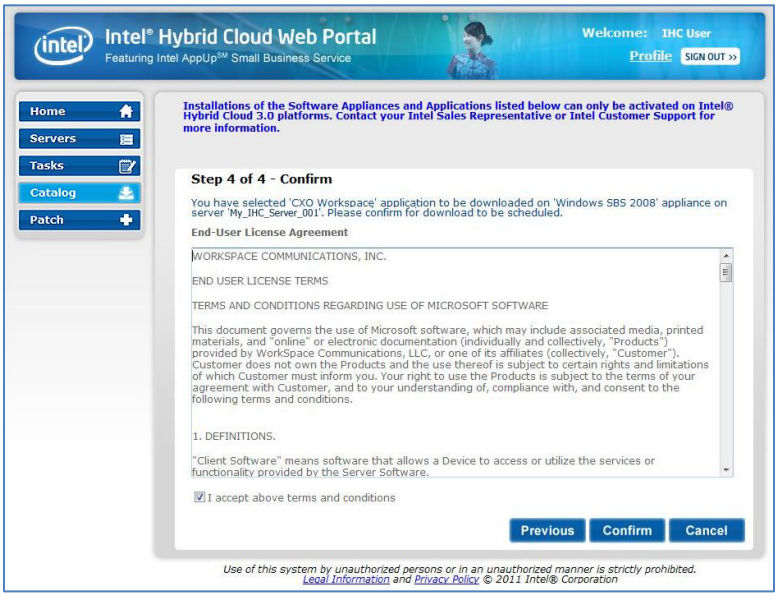

Figure 31 Management Portal – Catalog – Application EULA

6. Click the "**Finish**" button to initiate the download.

NOTE: The software download request will be added to the queue. Downloading and installation will proceed after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

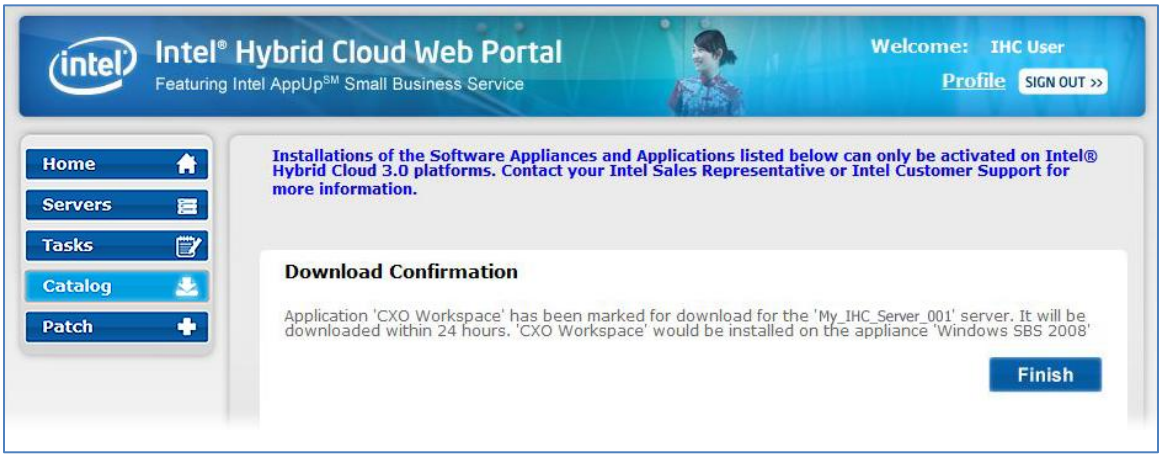

Figure 32 Management Portal – Catalog - Download Confirmation

5.6 Reactivating an Expired Appliance

If the system has not communicated with the Intel® Hybrid Cloud data center for 30 consecutive days, all the running appliances will stop and the appliance licenses will be revoked. The Administrator can use the management portal to re-activate the appliances, re-establishes communication with the management portal.

5.7 Appliance Expiration & Management

Appliance expiration must be managed by the administrator. Starting 15 days prior to the expiration of an appliance license, warning messages will be displayed in the Intel® Hybrid Cloud server manager to indicate the pending appliance license expiration. Email notifications will also be sent to the MSP warning of the pending appliance license expiration. NOTE: The appropriate settings must be entered in the Server Manager in order for email notifications to work properly (Refer to Section 6.8.3 to configure email alerts). After license expiration, there is a 15 day grace period (to use the appliance). Upon expiration of the grace period, the license for the corresponding appliance will be revoked and the appliance will shut down. The Remote Administrator can choose to extend the appliance license from the management portal (to meet end-user requirements).

5.8 View the Applications on an Appliance

The Management Portal allows you to view a list of applications installed on each appliance on any of the servers you manage. To view the applications, select the "**Servers**" screen, the "**Servers**" tab, and the "**Services**" link for a particular server. Appliances with installed applications will display an arrow to the left of the "**Status**" dropdown options. Click the arrow to view the applications on the corresponding appliance (as shown in the following screen).

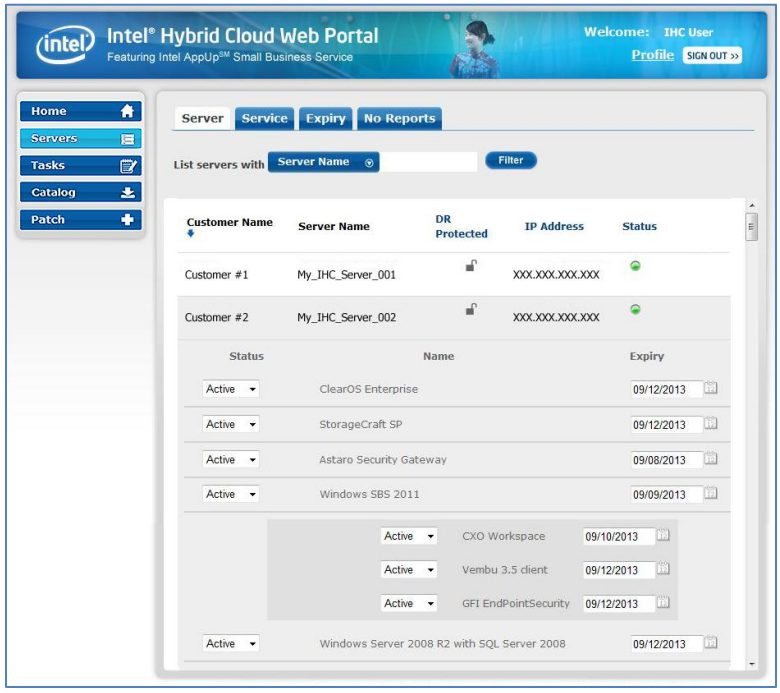

Figure 33. Management Portal – Applications on an Appliance

5.9 Activating or Deactivating an Appliance or Application

The Intel Hybrid Cloud management portal allows you to activate and deactivate appliances and applications. Status change requests will be added to the queue and will take effect after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

Figure 34. Management Portal – Applications Status Updates

5.10 Server Patch Updates

Select the "**Patch**" button from the navigation menu to view available upgrades for the servers you manage. If an upgrade is available, the servers will be listed along with the available upgrade (i.e. Patch). To apply a patch, select the server (check box) and click the "**Confirm**" button.

NOTE: Patch download requests are added to the queue. Downloading will proceed after the next usage report is received from the respective server. As long as the server is communicating properly with the Intel® Hybrid Cloud data center (see Section 2.2), this will occur within 24 hours. To force usage reporting, refer to the IXE Command List in Section 0, (Command: initiate-usage-reporting).

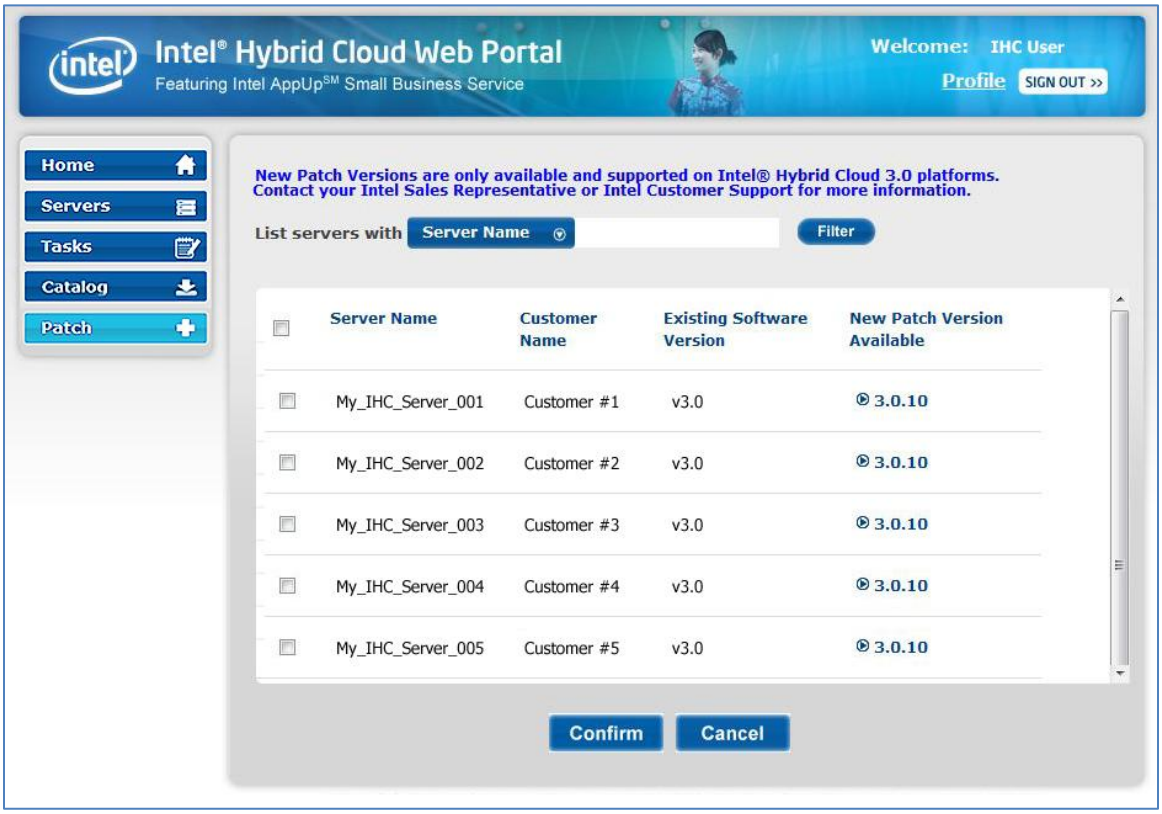

Figure 35. Management Portal – Server Patch Updates

6. Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager provides remote and local access to a variety of management functions. A maximum of 4 simultaneous remote connections are allowed for each Intel® Hybrid Cloud server.

6.1 Installing Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager can be installed in 2 ways.

- Intel® Hybrid Cloud server manager is installed when you setup and register a new server as described in Sections 3 and 4.
- Intel® Hybrid Cloud server manager can also be downloaded and installed from the "**Support**" page on the Intel Hybrid Cloud web site:

  http://www.intelhybridcloud.com/ > **Support**

6.2 Accessing the Intel® Hybrid Cloud server manager

- After you have installed Intel® Hybrid Cloud server manager, you can access it via the icon on your desktop or via your Windows* programs menu.
- You may also access the Intel Hybrid Cloud server manager through the Intel® Hybrid Cloud management portal (refer to Section 5.3 for details).

6.2.1 Role Based Access Control for Intel® Hybrid Cloud server manager

Intel® Hybrid Cloud server manager follows a Role Based Access Control (RBAC) mechanism. Two roles are supported by the Intel® Hybrid Cloud server manager:

Role (User ID)	Password
admin	**Hybr1dC!0ud**
User	**Hybr1dC!0ud**

The content in this section describes functions and features that can be performed or accessed when logged in as the administrator ("admin" role). The administrator can enable priviledges and access for the "User" role.

NOTE: You will be prompted to change the SW Management password upon initial login. This is generally done during server setup.

6.2.2 Login to Multiple Servers

You can login to Intel® Hybrid Cloud server manager using Intel® Hybrid Cloud management portal login credentials and see list of all active servers. They can then launch the Intel® Hybrid Cloud server manager for a specific Intel® Hybrid Cloud server.

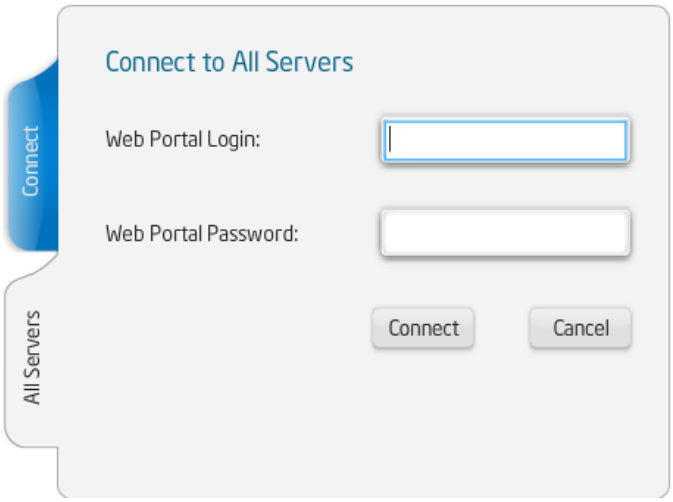

Figure 36. Server Manager – Connecting to All Servers

6.2.3 Login to a Specific Server

If you choose to connect to a particular server directly, you will be asked to also provide the IP address along with the Server name.

NOTE: You can connect to a specific server only if it is already registered.

Figure 37. Server Manager - Login Window

When you access a server for the first time, you need to provide the IP address of the server. The server manager remembers this information and does not require you to provide it thereafter.

Figure 38. Server Manager - Add server to hosts file

If the server is successfully registered and this is the first time Remote Administrator or user is logging in, they are required to change the default password and set a new password. The first time password entered by the remote administrator will also be used to set the password for accessing the Intel AMT features Login for user role will not have an option for accessing Intel® AMT features.

Notes:

- Entering IP address as the hostname is not allowed. User must enter hostname to connect to the server.
- On Windows 7, the server manager must be invoked with “administrator” privileges.
- User with Admin role can connect to server using Intel® AMT even when the server is powered off. In order to connect to Intel® AMT, it is necessary to give only hostname and Intel® AMT password. Using Intel® AMT, user can power on the system remotely. This feature is available only from remote connection (WAN IP) and only for admin role.

6.3 Changing the Default Server Manager Password

In order to change the “admin” and “user” passwords, you will need to login separately for each role (the default passwords for each are shown below).

1. Open Intel Hybrid Cloud server manager (Run as administrator).
2. Select the “Connect” tab.
3. Enter the Server Name and login information:
   - Server Name (created during server setup, Section 4.5)
   - User Name **admin** (or **user**)
   - SW Management Password **`Hybr1dC!0ud`**
     NOTE: The SW management password is automatically synchronized with the HW management password (Intel® ME / Intel® AMT / BMC). Using any other method to change the Intel® AMT password or BMC password will break the synchronization.
4. Press the “Connect” button.
5. Select the “Configuration” menu and the “Server Settings” tab.
6. Change the password.
   NOTE: Perform the steps above for each role (i.e. “user” and “admin” IDs)

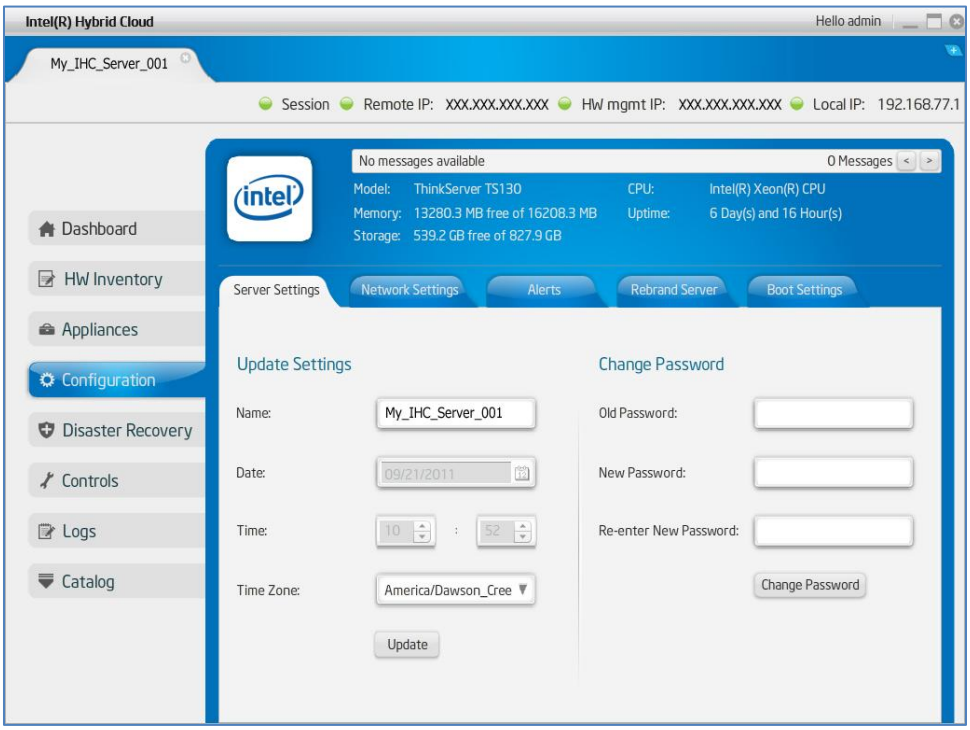

Figure 39. Server Manager – Change the Default Password

6.4 Dashboard

Once connected to an the Intel® Hybrid Cloud server, Intel® Hybrid Cloud server manager "Dashboard" view consists of Intel® Hybrid Cloud server details, main menu, log-in details and a dashboard view. Dashboard consists of three sections as shown in following screen:

- **Usage** — Displays usage graph of Memory, CPU, Disk, LAN, WAN of the server
- **Appliances** — Appliance status listing the installed appliances on Intel® Hybrid Cloud server and their current power state (Starting/Stopping/suspending/halted/Suspended/Importing/Running)
- **Software Logs** — A table of logs that show the last five log entries which could be information, warning, alert or error messages. Each entry has a record ID, timestamp and description. By default, messages that indicate "Errors" are displayed. By choosing the appropriate radio button on top of the messages, different categories of error messages can be viewed.

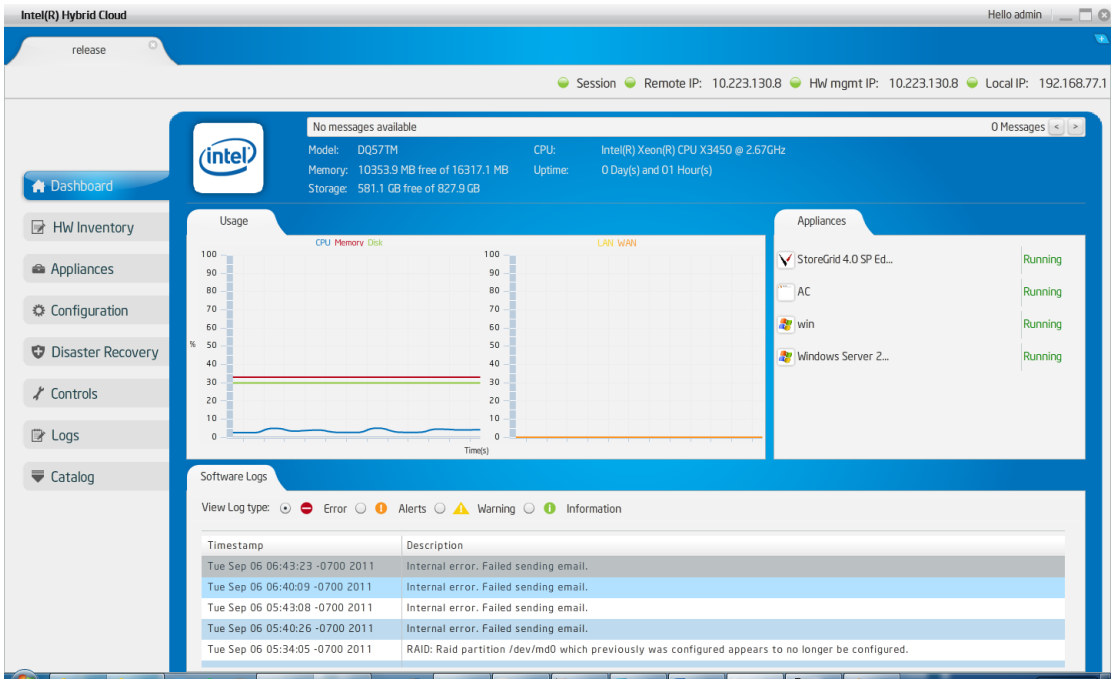

Figure 40. Server Manager - Default view (Dashboard)

A **Message Ticker** also appears at the top of the screen. This ticker will display important messages about any failures that may have occurred or if patches are available for install.

6.5 Hardware Inventory

This tab provides detailed HW information of the Intel® Hybrid Cloud server via Intel® AMT. This option is available only on "admin" role when connected through the remote interface. Following is a sample screenshot for system information. Similar data is available for processors, memory, and disk.

- Intel® AMT features like HW inventory, HW events, force shutdown, and force restart are ONLY available via the WAN interface.

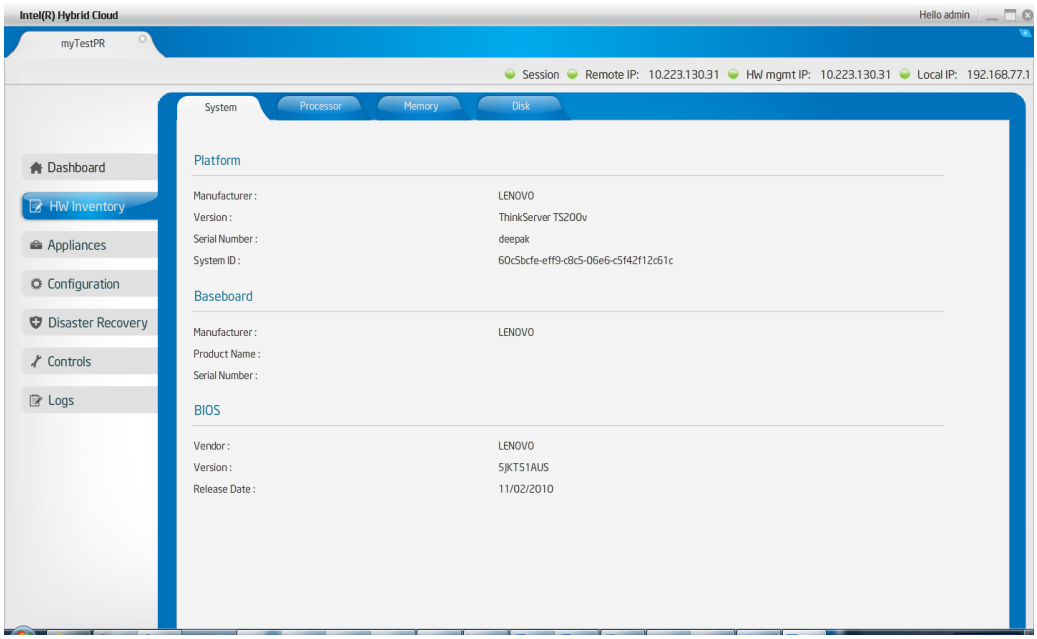

Figure 41. Server Manager - Hardware Inventory - System Information window

6.6 Managing Appliances

Appliances installed on Intel® Hybrid Cloud server can be managed using the "**Appliance"** tab on the default screen. Default view under this option consists of icons for all the appliances available on top along with the power status of each of these appliances. User can select any appliance and manage it. Appliance details like name, vendor, and version are shown along with an option to either start/stop/suspend/resume the appliance depending upon its current state. For example, if an appliance is already started, the option to "stop" and "suspend" it are available and so on. Also, after installing an appliance, it is in the stopped state by default. Appliances can also be uninstalled provided they are in the stopped state.

An appliance can be started or resumed (based on its current state) only when the license state of the appliance is activated via the Intel® Hybrid Cloud management portal. If the license of an appliance is inactive and Remote Administrator/user tries to start the appliance, the appliance license query is sent to the management portal. Only if the license is marked "active" on the management portal is the appliance allowed to start and license is marked "Active" on the Intel® Hybrid Cloud server manager. Else, an error message is displayed.

Likewise, an appliance can be remotely deactivated via the Intel® Hybrid Cloud management portal. However, this information is retrieved by the server only once in 24 hours (when usage information is reported to the management portal) or Remote Administrator can force the usage reporting (via the IXE tool) and thereupon, the appliance state information is immediately updated on the server. For details on IXE commands, please refer Section 11.

If the appliance license has expired, the user is allowed to use the appliance for a grace period of 15 days post license expiry date, after which the appliance is suspended /shutdown (if suspend operation is not possible) Warning messages are displayed 15 days prior to the expiry of the appliance license and error messages are logged in the grace period.

In addition to appliance details, there are other six options available in this view:

6.6.1 Appliance Monitor

Usage details of resources like Memory, CPU, Disk, LAN, and WAN allocated to an appliance can be monitored via the graphs available here. Also, the amount of memory, CPU and disk storage allocated to the appliance is shown here.

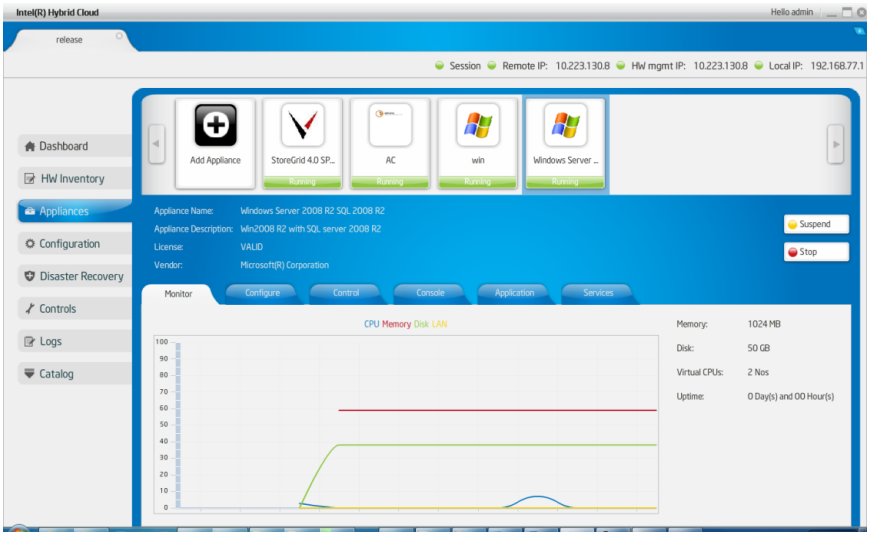

Figure 42. Server Manager - Appliances Monitor window

6.6.2 Appliance Configure

This tab provides user the option to configure appliance specific parameters. These are similar to the ones required to be configured while installing the appliance. The user can update the appliance name, change the number of virtual CPUs, total memory allocated, add or delete hard disk drives and add or delete network interfaces.

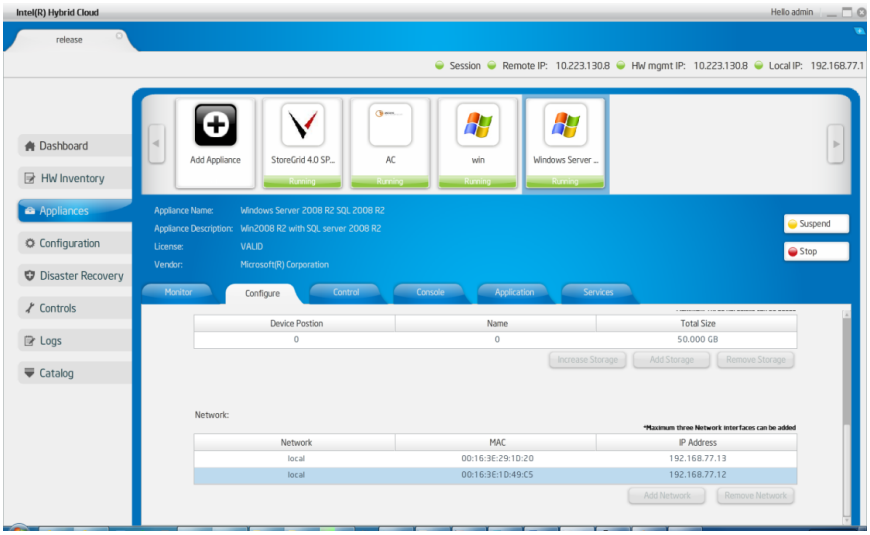

Figure 43. Server Manager - Appliances Configure window

Note: User can perform the actions like Add/remove network/hard disk only when the appliance is in stop state. Also, the changes in the configuration will only take effect once a power restart of the appliance has been effected.

6.6.3 Appliance Control

The user can take a backup of an appliance from this view onto a USB disk that is directly connected to the server. The USB disk should have free space equal or greater than the size of the appliance to be backed up and must be formatted in NTFS format. The backed up appliance can then be restored from the USB disk at a later time.

To know how to restore appliance, refer to Section 6.7. In addition to backing up, appliances can also be deleted from this view. The uninstall button will uninstall the selected appliances.

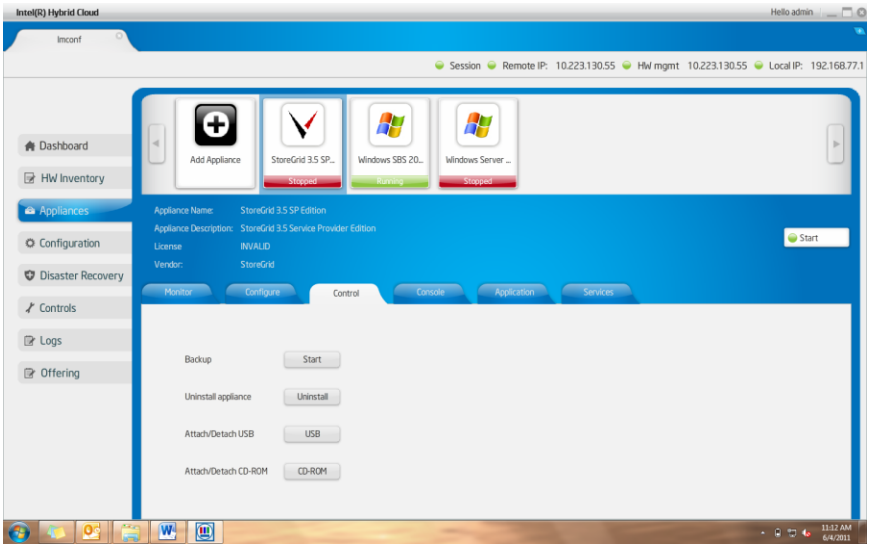

Figure 44. Server Manager - Appliances Control window

Along with the backup and uninstall options, the option to attach or detach a USB or CDROM to a particular appliance is also provided.

MSP/User can connect the USB/CDROM to the server and click the Attach/Detach USB option.

6.6.4 Managing applications and services within Appliances

Once applications are installed, they are ready to be used. Each application can be accessed from within its appliance. Once the user comes to the apps/services tabs of the appliances status of all the services and apps supported by Intel Hybrid Cloud can be seen.

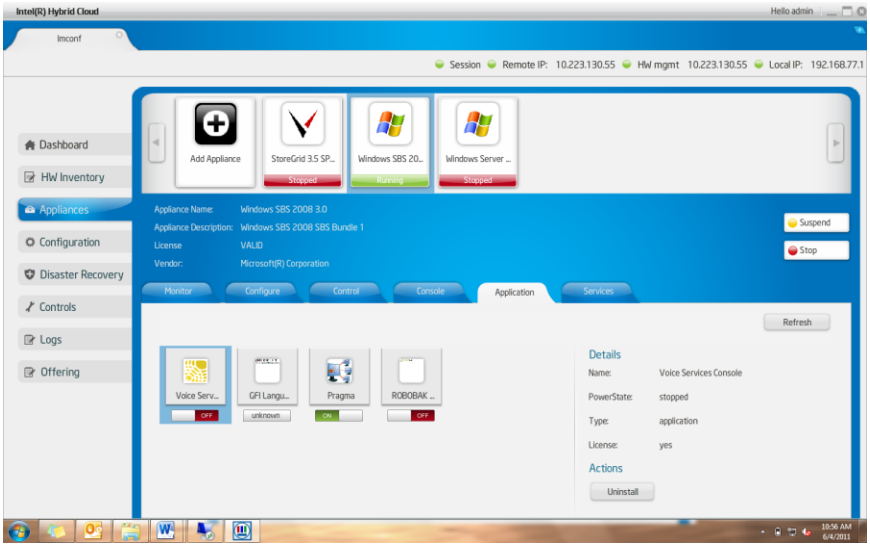

Figure 45. Server Manager – Appliance Services

Following controls are provided for each application.

Application start

Right click on the applications icon and select start option.

If that particular application requires EULA to be accepted the same will be shown to the user. Once the user accepts the license page, license key will be fetched from the portal, which will activate the application and then the application is started.

Application stop

Right click the applications icon and select stop option.

Application uninstall

Under the “Actions” section, an uninstall button is available. Clicking this after choosing a particular application will initiate the uninstall of the application.

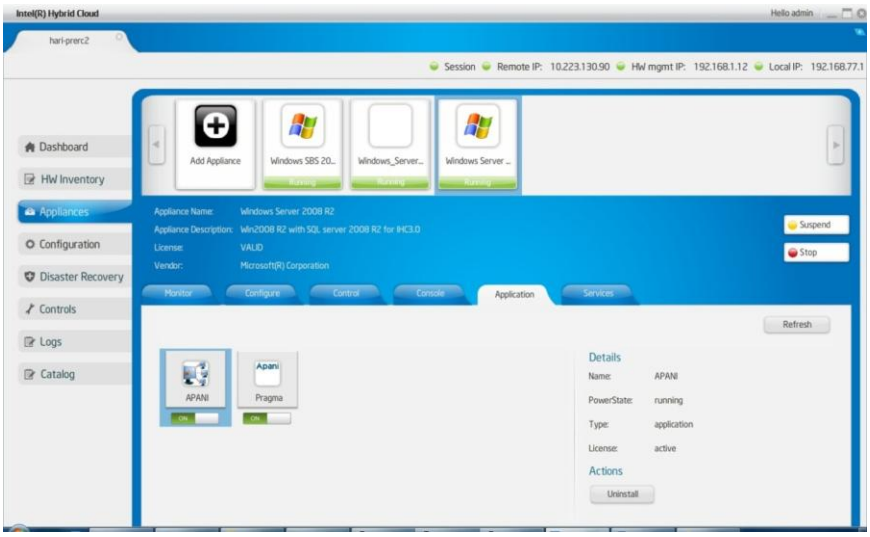

Figure 46 Server Manager - applications tab under Appliances

Services tab

Similar set of operations can be performed under the “Services” tab for all the services that are running under a particular appliance/application.

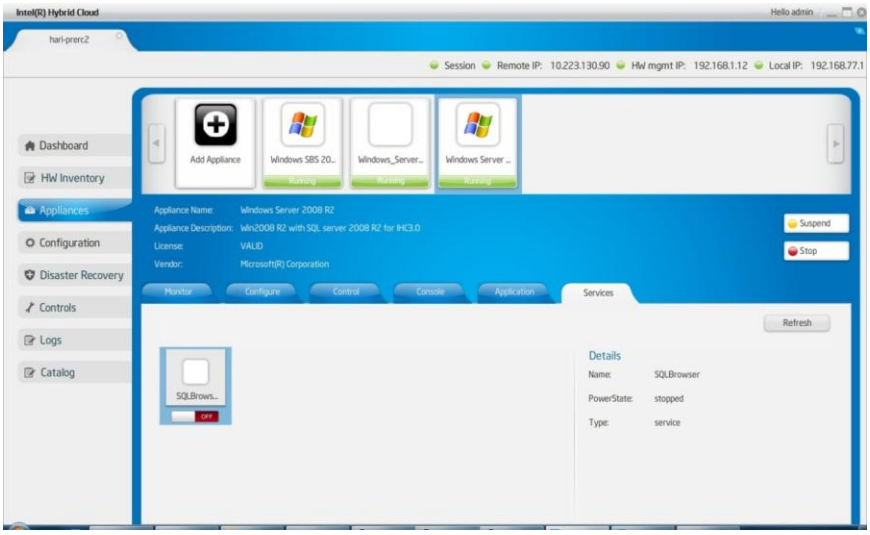

Figure 47 Server Manager - Services tab under Appliances

6.6.5 Appliance Console

Under this tab, user can launch the VNC console of the selected appliance (only for those appliances which are running). User can open only one console per appliance and the same can be closed only from the session that started it.

User can either select the Remote Desktop or VNC to view the console of the particular appliances. For the RDP option, make sure that the protocol is supported and configured properly

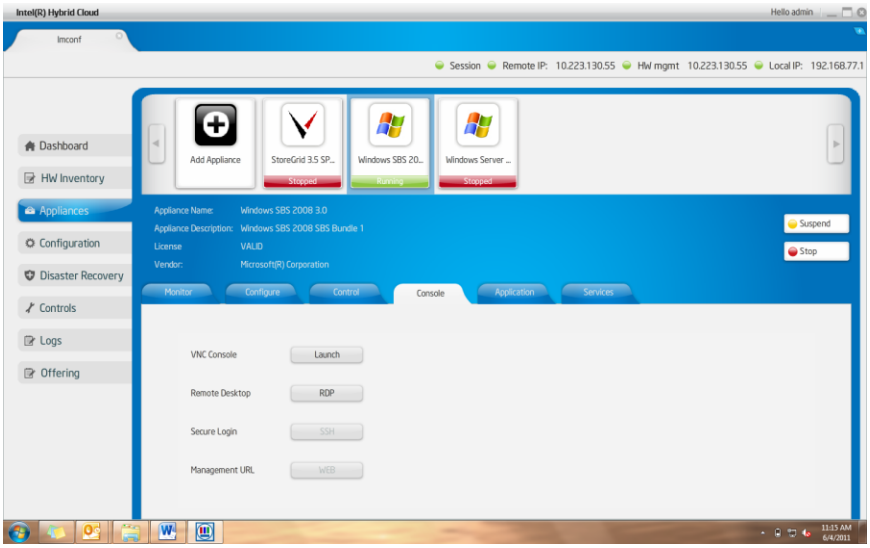

Figure 48. Server Manager - Appliances Console Screen

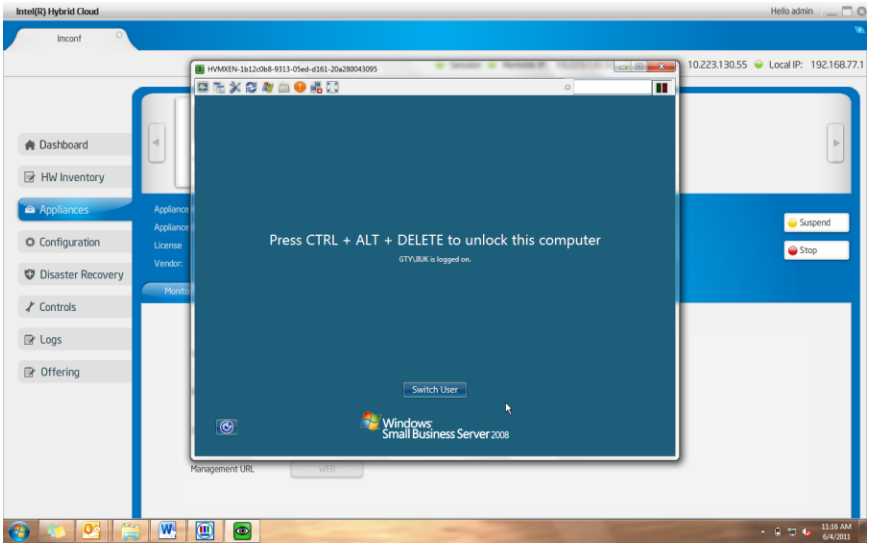

Figure 49. VNC Console

6.7 Appliance Restore

The appliances that were backed up on to a USB disk can be restored via this tab. Once the user connects the USB disk containing backed up appliance images, this tab will show a list of all the backed up appliances. User can select any appliance and click on the restore button provided. The restored appliance needs to be activated again via the management portal before it can be used (see Section 5.9). The restore operation will install the previously backed-up appliance. The older appliance will still be present and has to be deleted manually if required. Please refer Appliance Control section 6.6.3 to see how to delete an appliance. Also note that images backed up on a machine can be restored on any other IHC server, provided the hardware configuration of the machines match.

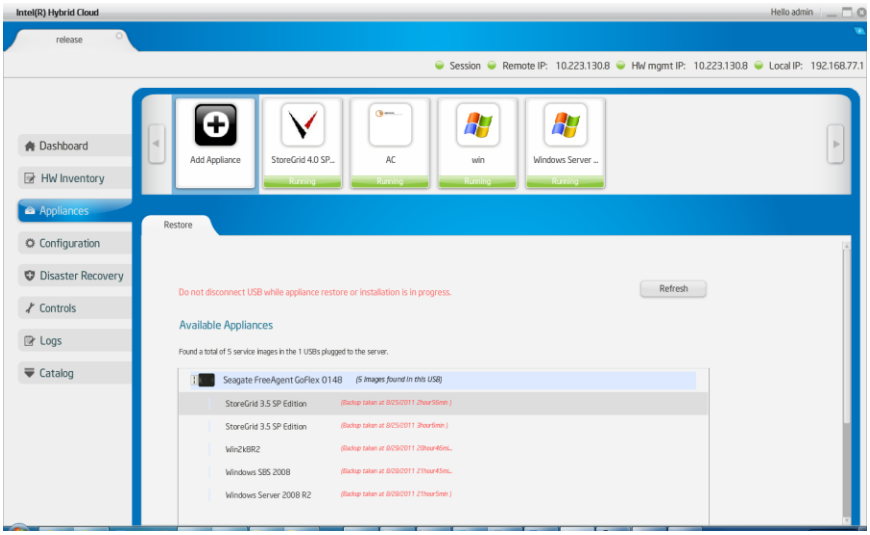

Figure 50. Server Manager - Appliances Restore Screen

6.8 Configuring Intel® Hybrid Cloud server

This feature can be used to configure Intel® Hybrid Cloud server and also to perform few other tasks like changing password, appliance boot settings, etc. Functionality of these features is explained in the following sections.

6.8.1 Server Details

This tab can be used to configure System name, update time zone and change password will sync both system and Intel® AMT or BMC password.

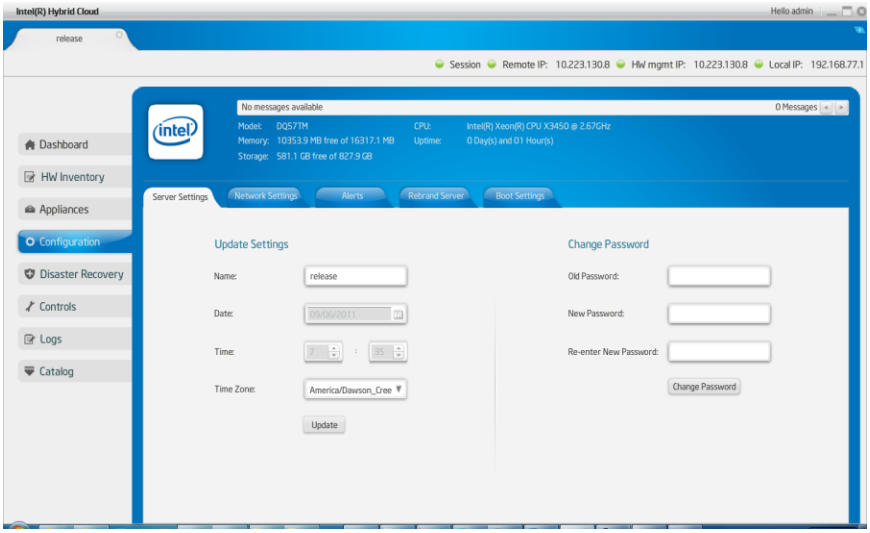

Figure 51. Server Manager - Configure Server Settings window

6.8.2 Network Settings

This tab can be used to configure local and remote interfaces of the Intel® Hybrid Cloud server. If one updates the interface through which the user is connected, it displays a warning message before it proceeds.

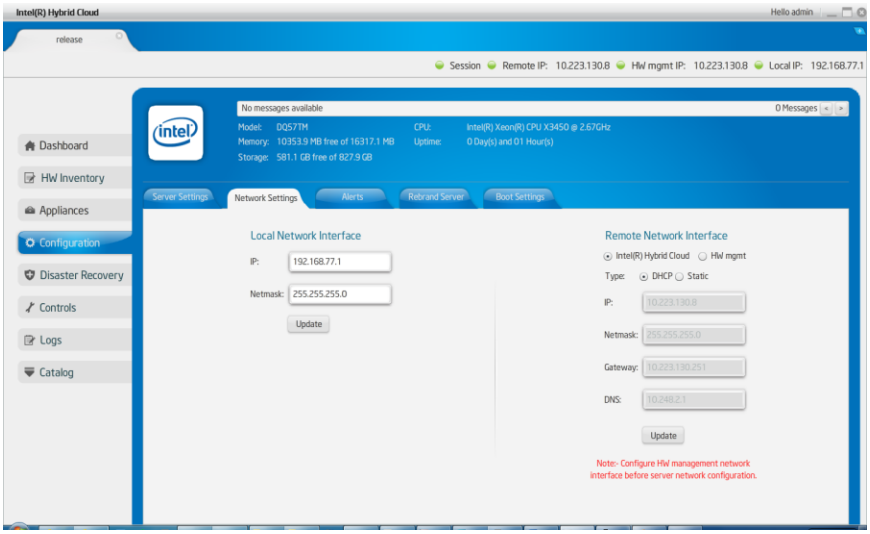

Figure 52. Server Manager - Configure Network Settings Screen

6.8.3 Configuring Email Alerts

This tab lets the admin and user configure the email settings and select the software alerts that can be received from the Intel® Hybrid Cloud server by email. The Server email/SMTP configuration can be updated only by admin. The DNS name of the SMTP server needs to be configured. The user and admin can configure their email addresses to which the alerts are sent and also the specific type of logs for which Intel® Hybrid Cloud server should send the alert emails.

Note: Currently, under the "Server email configuration" option, support is provided only for **TLS/STARTTLS Ports**. Therefore add only such smtp mail servers. The most popular example of such a qualifying email service is Google's gmail (smtp.gmail.com). Refer to the technical documentation of your email provider to check if it provides TLS/STARTTLS ports.

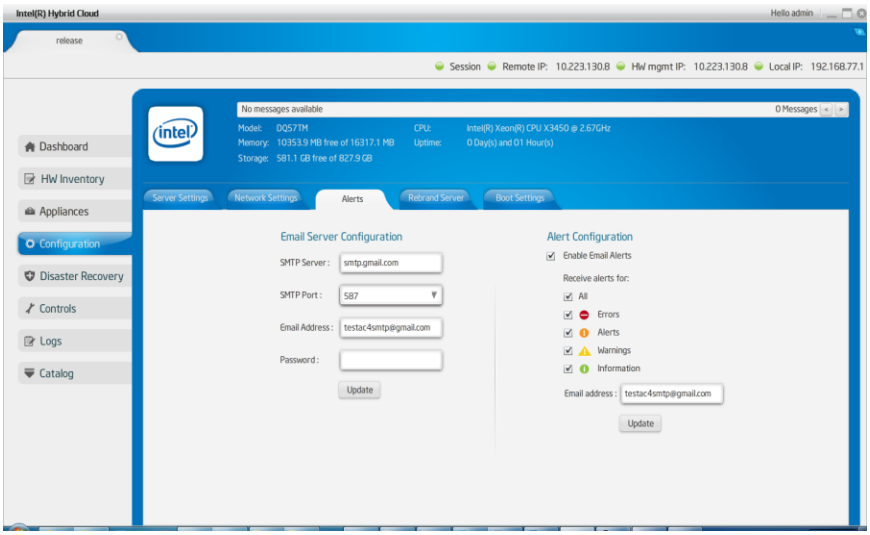

Figure 53. Server Manager - Alerts (Email) Configuration window

6.8.4 Rebrand Intel® Hybrid Cloud server

This option helps OEM/ Remote Administrator/MSPs to rebrand server by changing Vendor name, Client name, logo, and EULA. This option is available only for "Admin" role.

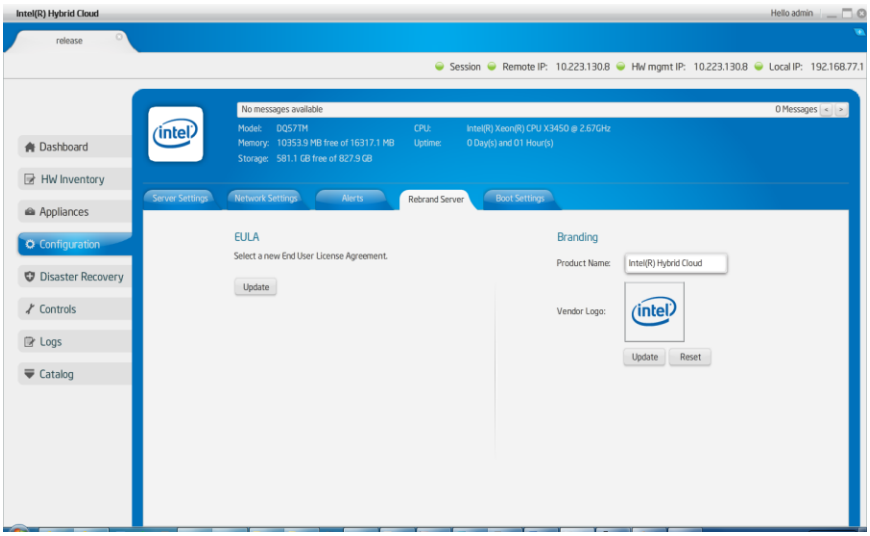

Figure 54. Server Manager - Rebrand Server screen

6.8.5 Configure Boot Settings

This tab can be used to change the order in which appliances should automatically start up post server boot. User can drag and drop to change the order. This order is only applicable on the subsequent boot.

Note: Reorder option for appliances is available only for admin role. Appliances marked to run on boot should have valid licenses installed. Without a valid license, appliance will not be started automatically or otherwise.

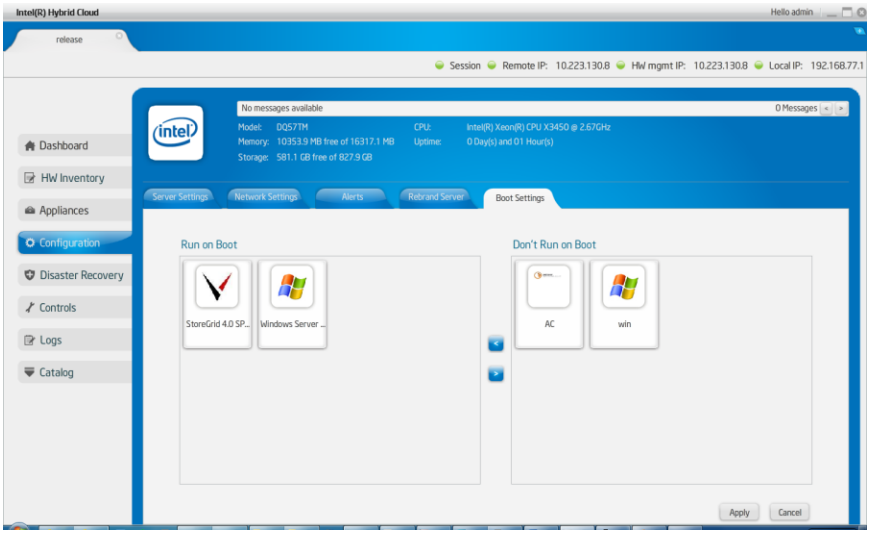

Figure 55. Server Manager - Configure Boot Settings window

6.9 Disaster Recovery

As the Intel® Hybrid Cloud platform works as a one-stop solution for all IT requirements of an SMB, the Intel® Hybrid Cloud server will be the backbone of IT in the SMB premises. The Intel® Hybrid Cloud provides customers an option to subscribe for Disaster Recovery capability wherein the customer will get two Intel® Hybrid Cloud servers. One of the servers acts as a primary server and this server will run the customer applications and IT services. The second server is the secondary server and will mirror the primary server. In the event of the primary server failing, the secondary server can be activated, and the customer can have their business up and running with very minimal downtime.

6.9.1 Setup

Setting up Disaster Recovery is a single step process. Once both the primary and secondary servers are booted, launch the Intel® Hybrid Cloud server manager of the primary server and navigate to the Disaster Recovery tab. This view provides a DR Setup option as given in the screenshot below.

The MSP must enter the Remote/WAN IP address of the secondary server and the Local/LAN IP address that the MSP wants to configure as the secondary server. Both machines must be able to reach each other on the Remote/WAN interface. They need not be on the same network but must be reachable via a router or gateway. Both machines, though, must be on the same LAN.

Additionally, a server should be set to factory defaults prior to being configured as secondary server. The name of this secondary server is set, by default, as the “<primary-server-name>_clone”. This can be modified if the secondary server has been named differently.

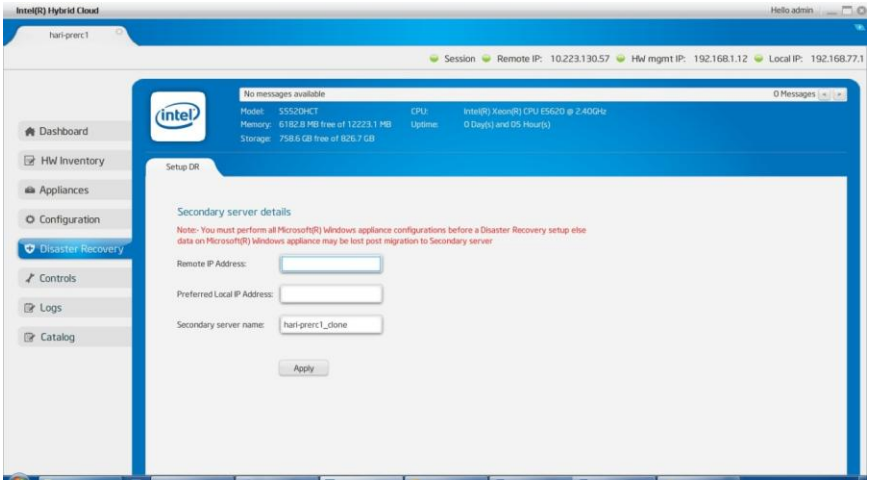

Figure 56. Secondary server details window

Once these details are entered, Intel® Hybrid Cloud software stack configures LAN interfaces of the machines to enable the communication between the servers. Once the LAN is configured, Intel® Hybrid Cloud software stack waits for 5 minutes to connect the LAN interfaces of the two machines and thus enables the communication between machines.

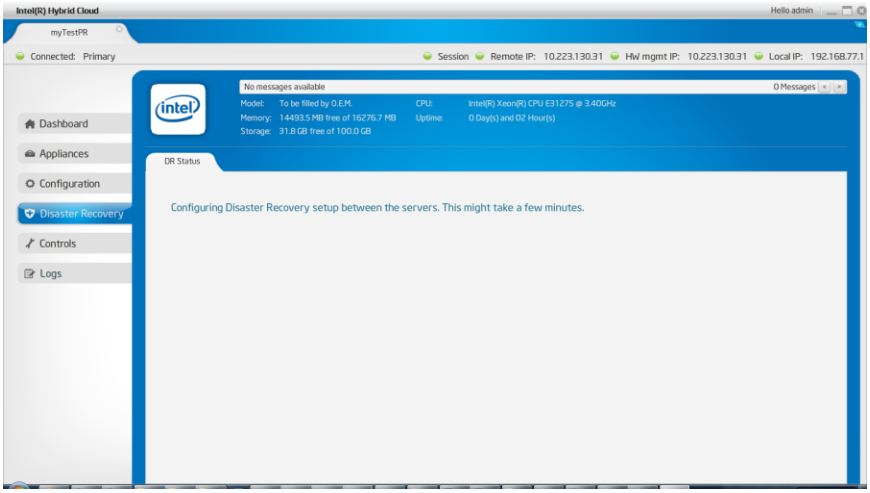

Figure 57. Server Manager - Configuring Disaster Recovery between servers

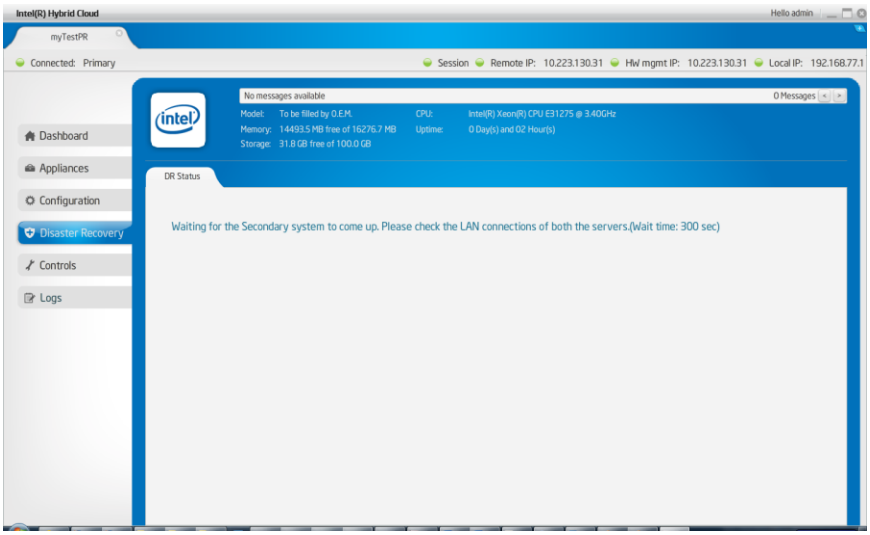

Figure 58. Server Manager - Waiting for Secondary systems to come up

Once the communication between the machines is enabled, the DR sync process starts.

After the DR setup is done, this view shows the present state of the servers for Disaster Recovery setup. It shows the DR Sync percentage for each appliance. Please refer the following screenshot.

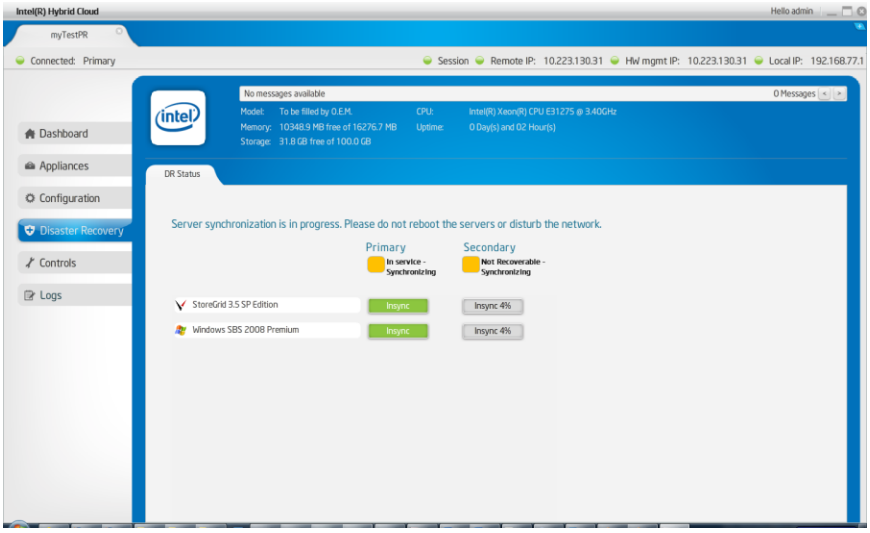

Figure 59. Server Manager - Synchronization in progress

During Sync, the resource on the mirror server would be in a non-recoverable state. Please refer to the screenshot above.

Once the complete sync is done, the view would show the state of each of the servers. Please refer the following screenshot.

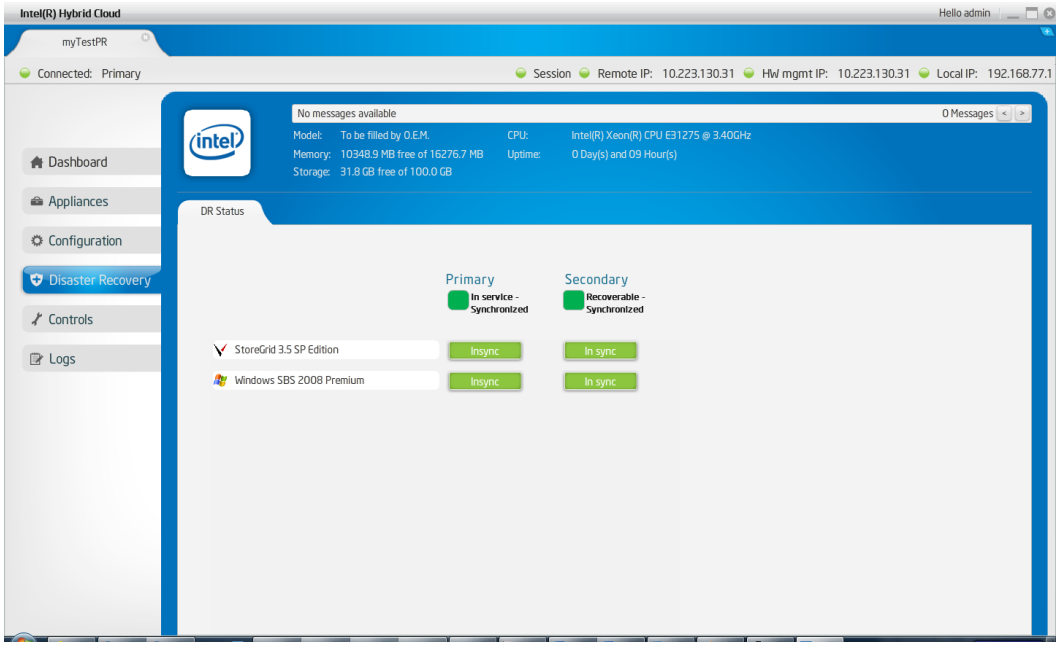

Figure 60. Server Manager - Synchronization complete

Intel® Hybrid Cloud software stack keeps syncing the VM metadata and various other system details (network details, API ACL, SMTP) between the servers so that the switch over during a failure would be as easy as possible for the MSP.

Once the DR setup is done, the dashboard of the Server Management console shows the usage of the mirror server too. Please refer to the following screenshot.

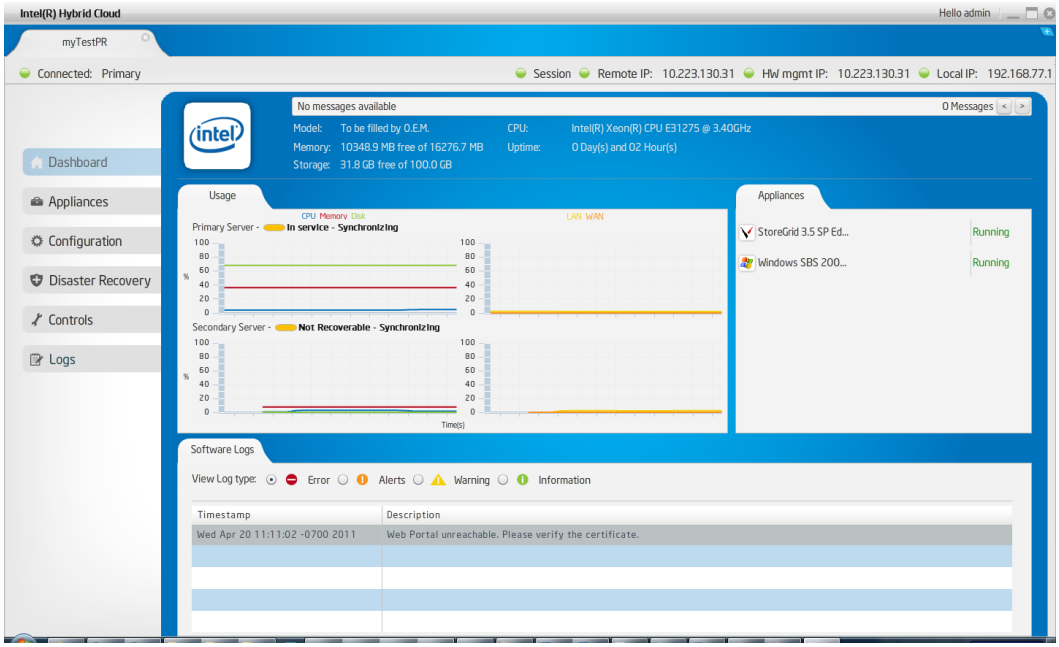

Figure 61. Server Manager - displaying usage of the mirror server

6.9.2 Recover from Primary Server Failure

Once the DR Setup is done, and, if at some point, the Primary server encounters a hardware/software failure, the secondary machine can be brought into service. This would bring back the IT infrastructure of the SMB in a matter of few minutes. When a user/MSP connects to the secondary server while the primary server is down, the following is displayed as the server status.

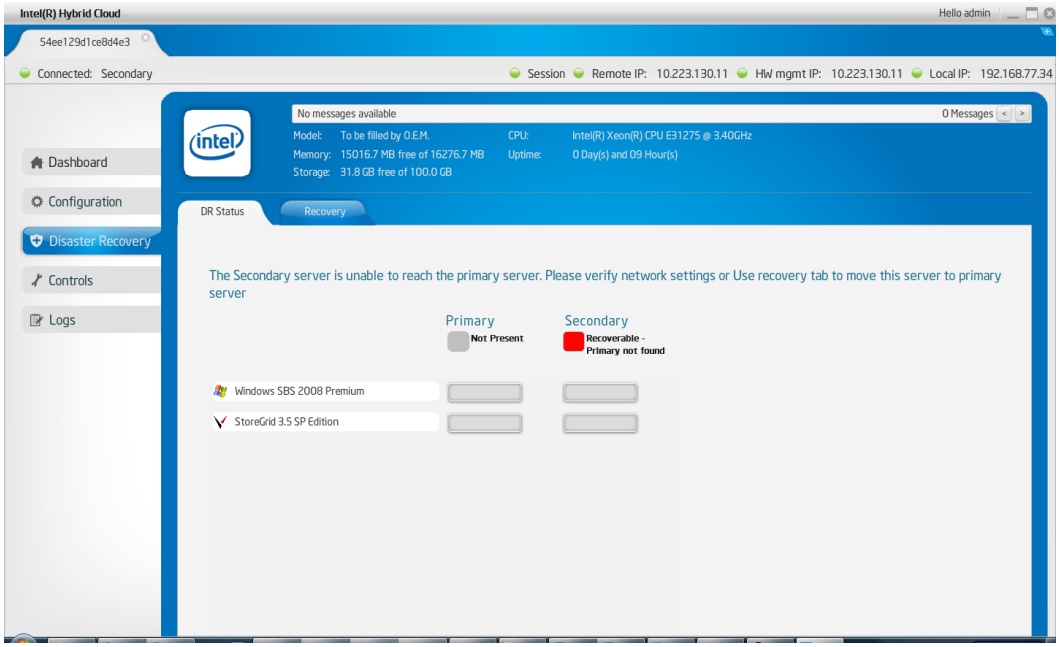

Figure 62. Server Manager - Server status message

Also, the dashboard shows the appropriate status of the machines. Please refer to the screenshot below.

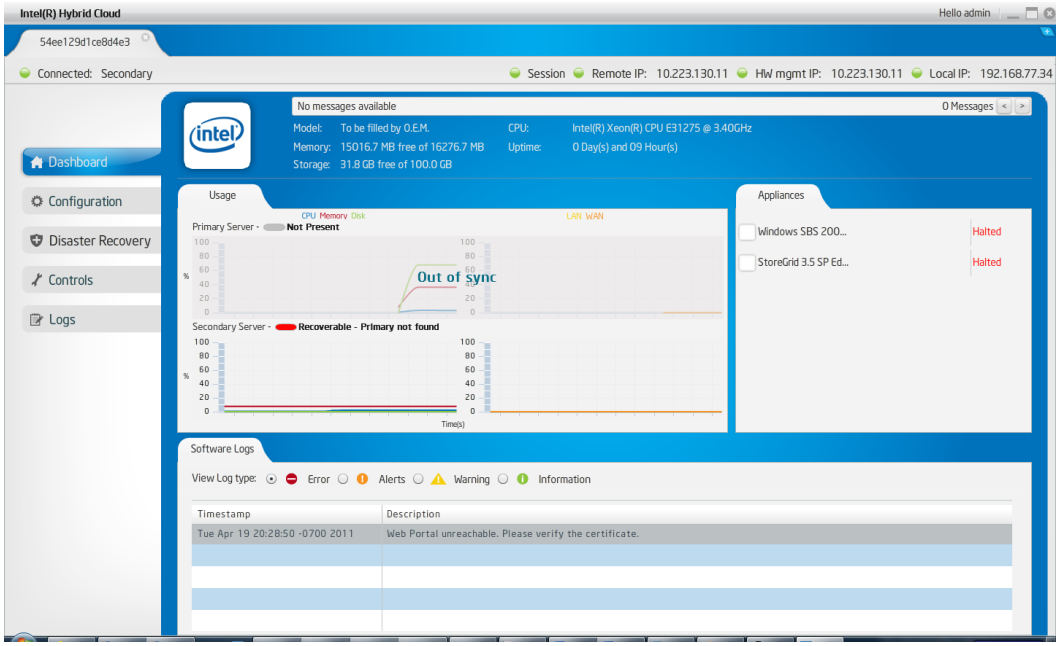

Figure 63. Server Manager - Machine status

MSP can use the Recovery tab to bring the appliance in service on this secondary server which will be the new Primary server post recovery. Please refer the screenshot below for the Recovery tab.

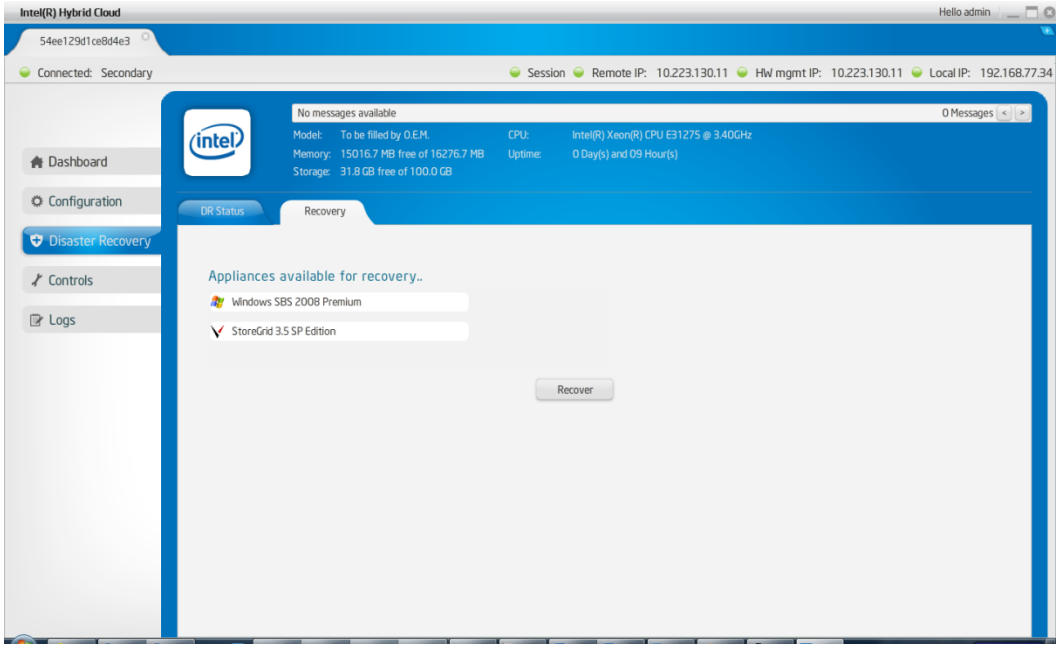

Figure 64. Server Manager - Recovery tab

6.9.3 Repair – Re-Create the Disaster Recovery Setup

Once the appliances are recovered, the original secondary server becomes the primary server. Now MSP can add a new secondary server and repair the setup to have disaster recovery capability once again. Repairing is a single step process where the MSP has to provide the WAN IP address of the new server. Please refer the screenshot below.

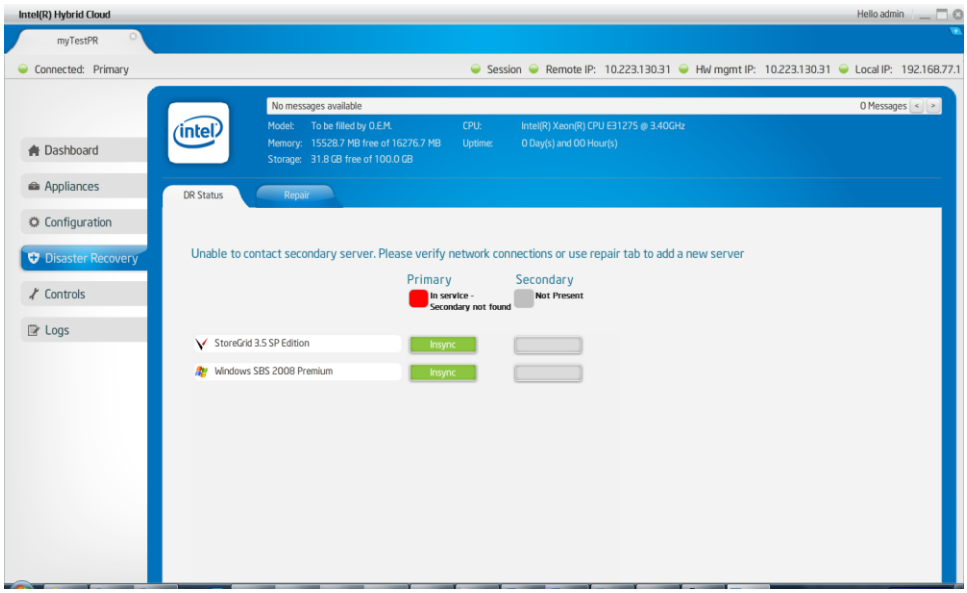

Figure 65. Verify Network Connections for Secondary Server

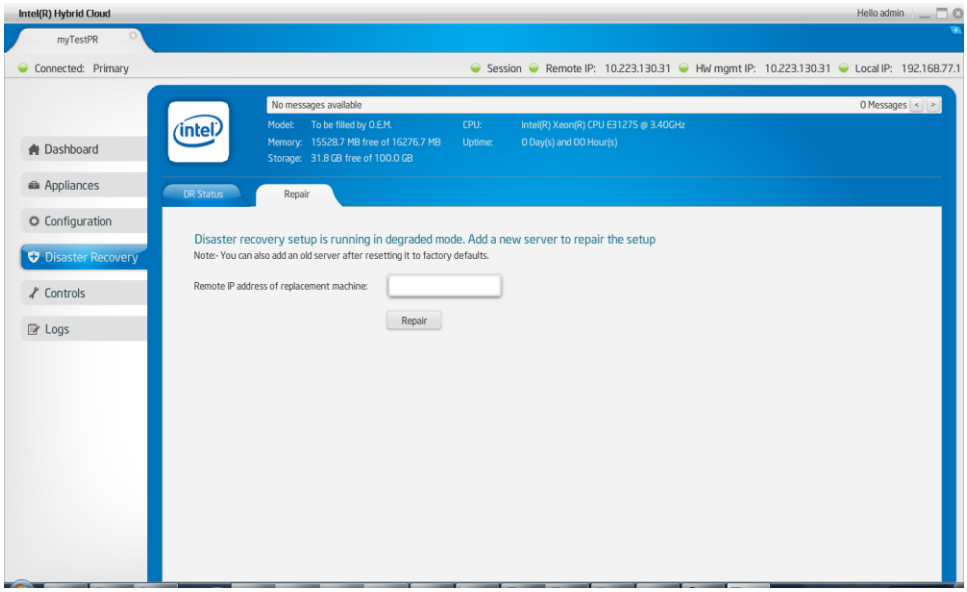

Figure 66. Re-Create the Disaster Recovery Setup

Just like in the case of the first-time DR setup, both the servers must be reachable on the Remote/WAN interface, and on the Local/LAN side both servers have to be connected to the same network. Prior to setting up a server as secondary server, the server must be set to factory defaults, if it is not a new server.

Post-repair, disaster recovery is setup again, and it ensures high availability for the customer's IT infrastructure.

6.10 Intel® Hybrid Cloud management controls

Various actions can be taken on the Intel® Hybrid Cloud server manager using this tab like system restart, shutdown. Force restart and shutdown can be done OOB using Intel® AMT. These Intel® AMT commands are available only for the admin role. For others, admin can grant permission to user role.

There are four options available under software:

Software Reset — Resets the Intel® Hybrid Cloud software stack on the server.

Set System Defaults — Resets the Intel® Hybrid Cloud software stack configuration to initial default settings. This sets the user permissions to default permission levels and disables SSH for the user. It also configures the remote interface to 'dhcp' and sets local interface to 192.168.77.1/255.255.255.0 IP configuration. All Email alert configurations are removed. The boot orders of the appliances are also removed. There is no effect on the server registration and appliance activation state.

Upgrade — The Intel® Hybrid Cloud software stack can be patched using the upgrade option. There is an option to patch both Intel® Hybrid Cloud server manager and Intel® Hybrid Cloud software stack. User needs to copy the patch to the client system and then using the upgrade feature, remotely patch the software stack, or patch the server manager on the client system.

Appliance network — There is also a provision for taking appliances off the network. This could be used in scenarios where a network threat is detected and admin may want to put appliances off the network. Post diagnostics, he/she can put these appliances back on the network. Remote Administrator logged in as "admin" can also allow user role to perform this action.

Note: A power cycle on an appliance after detaching it from network automatically brings the appliance back on the network.

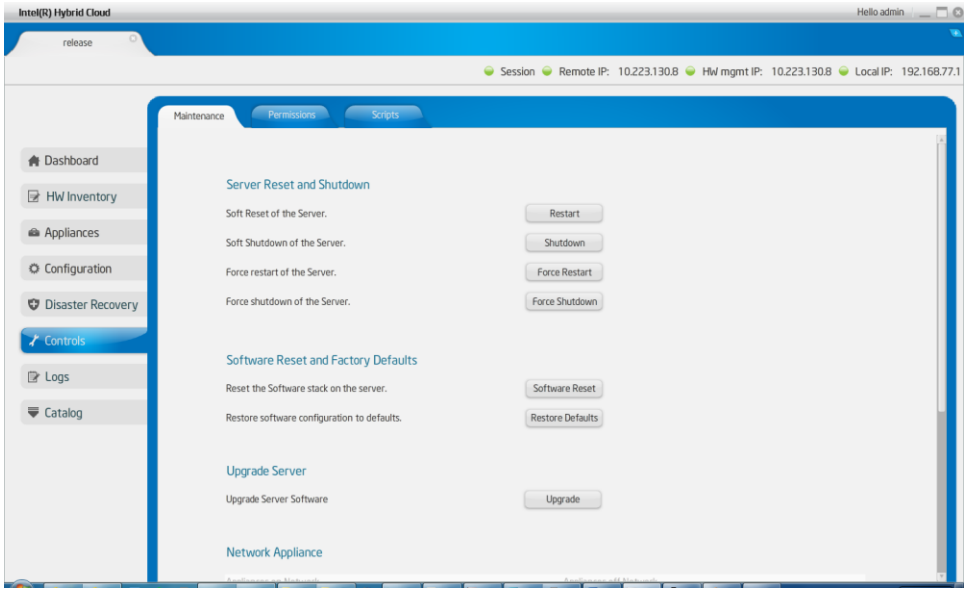

Figure 67. Server Manager - Control - Maintenance Screen 1

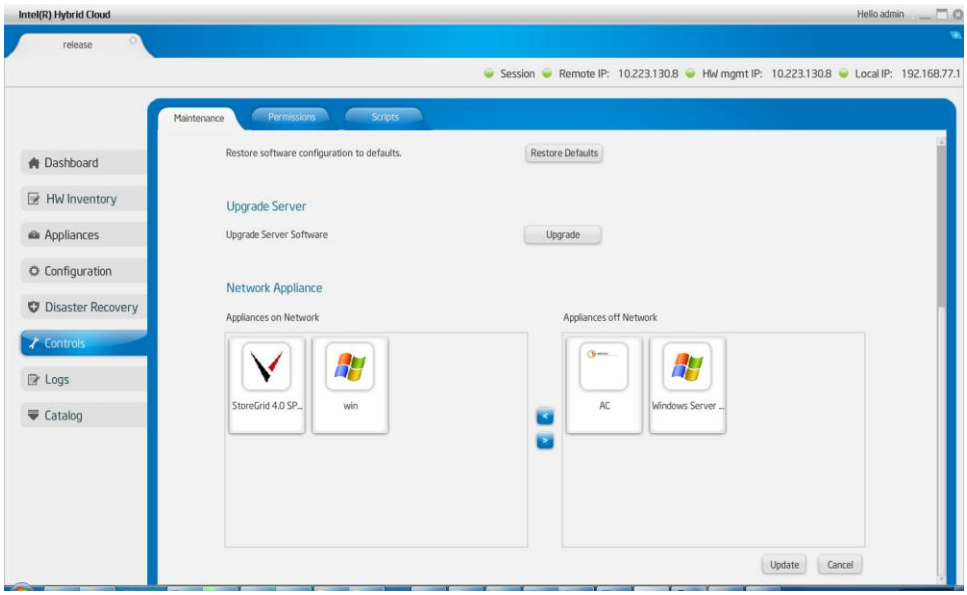

Figure 68. Server Manager - Maintenance Screen 2

6.10.1 Permissions

This screen is divided into 2 groups; system or hardware permissions and User permissions.

System permissions allow “Admin” to enable/disable SSH and SystemConsole.

User permissions allow “Admin” set permissions for user role. Once logged in as “admin”, the Remote Administrator can change the default access permissions for the “user”. The access permissions are limited to “allowed” or “denied” for various operations supported.

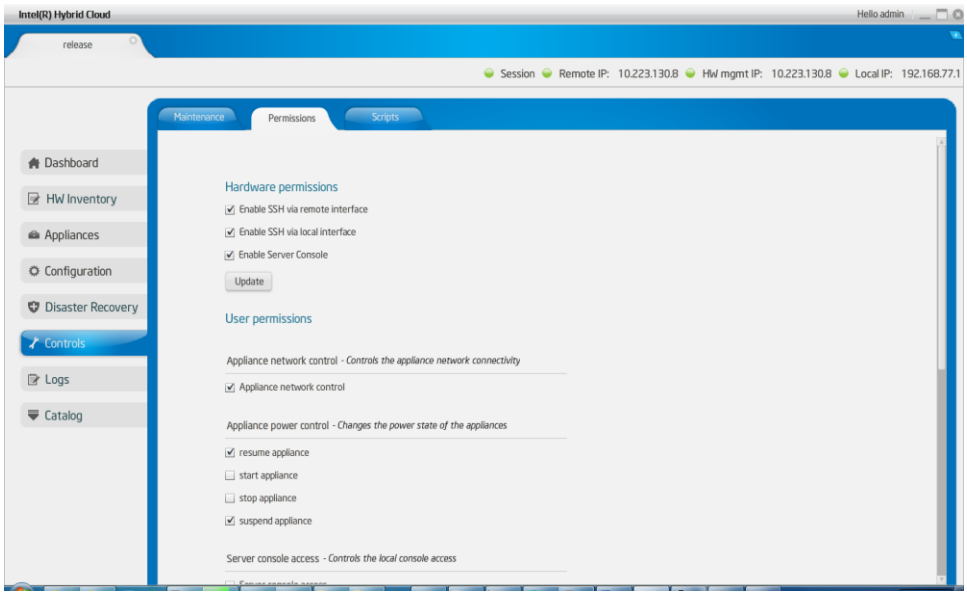

Figure 69. Server Manager - Permissions Screen

6.10.2 Diagnostics (Controls → Scripts)

This tab provides a window to execute scripts to perform operations on the server. The script engine is designed in such a way that the user can add customized scripts. Default scripts available include:

1. Deleting ISO attached to appliance/VM.
2. Manage software RAID on this system.

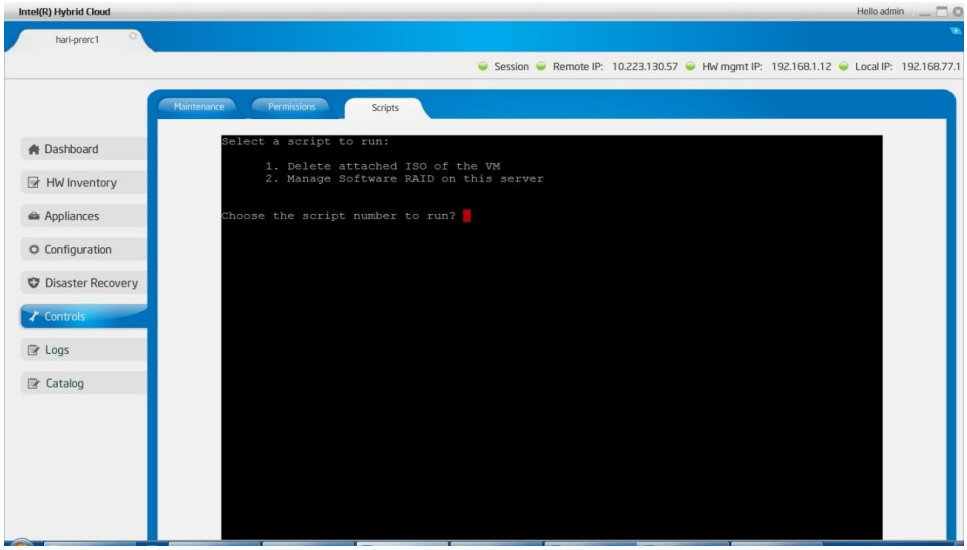

Figure 70. Server Manager - Diagnostics (Control > Scripts) window

6.11 Intel® Hybrid Cloud software logs

This tab shows detailed logs on Intel® Hybrid Cloud server. The log entries fall under various categories viz : information, warning, alerts, and errors. A filtering mechanism is available by which any subset of these categories of messages can be viewed. The log messages are also classified into three "event" types.

- Software events that are captured by Intel® Hybrid Cloud software stack and RAID Controller.
- Hardware events that are captured by Intel® AMT.
- System events that are captured by Citrix* Xenserver*.

Intel® Hybrid Cloud software stack supports both Hardware and Software RAID to be configured on the server to provide maximum availability for the services installed on the server. RAID drives would be used as the default storage for installing all the appliances. Intel® Hybrid Cloud software stack collects the logs generated by RAID and adds them to the Intel® Hybrid Cloud software logs.

The user also has the option of marking a particular log entry, or a set of log entries, as "closed". The default response of the server manager is to not display the closed log entries any more. Using a drop down, the user can select and view closed log entries as well.

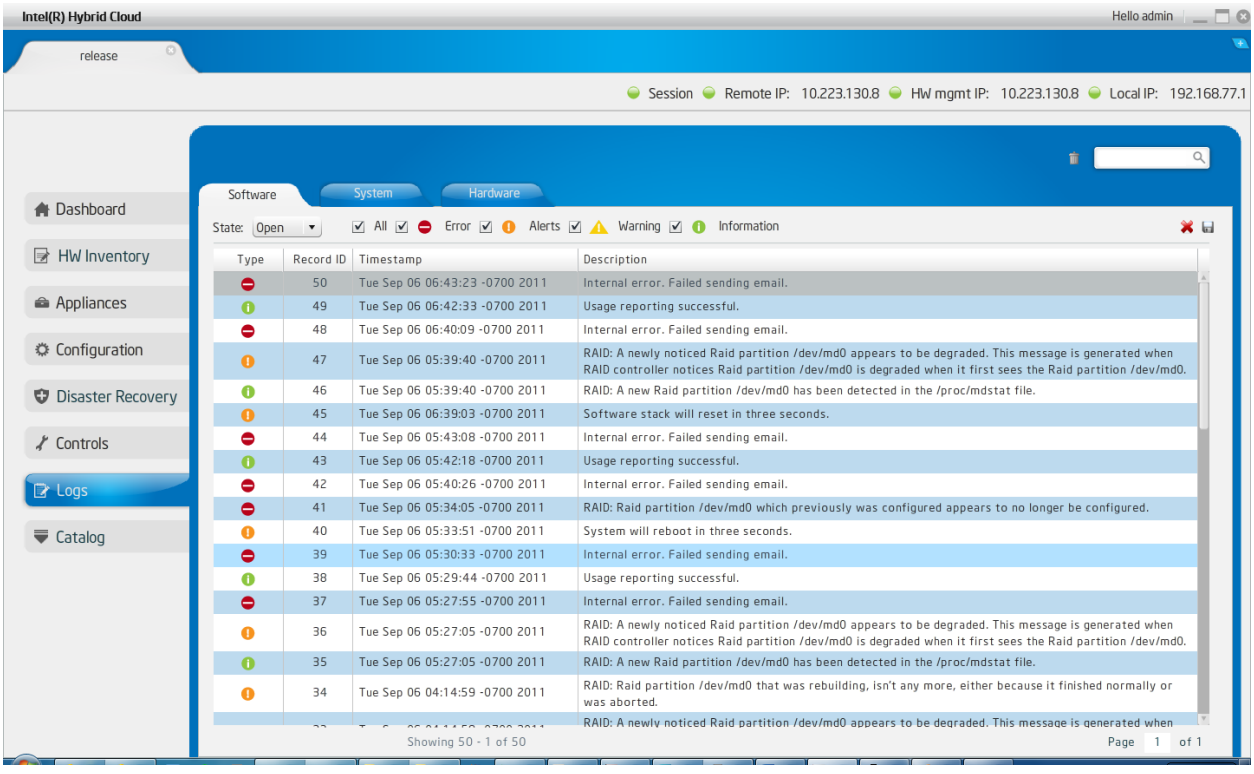

Figure 71. Server Manager - Software Logs screen

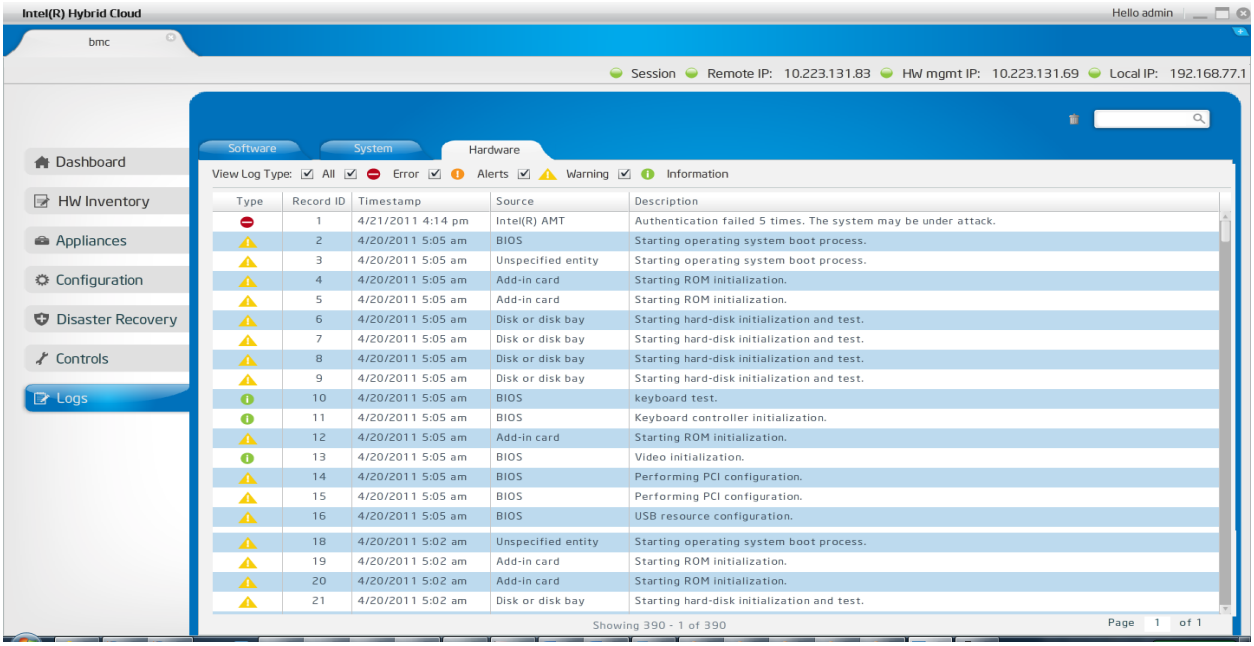

Figure 72. Server Manager - Hardware Logs Screen

6.11.1 Software and Hardware Logs Deletion:

Clicking on the **Trash Bin** icon highlighted below will delete all software or hardware logs. There is no option to delete specific set of logs. Also, system logs cannot be deleted.

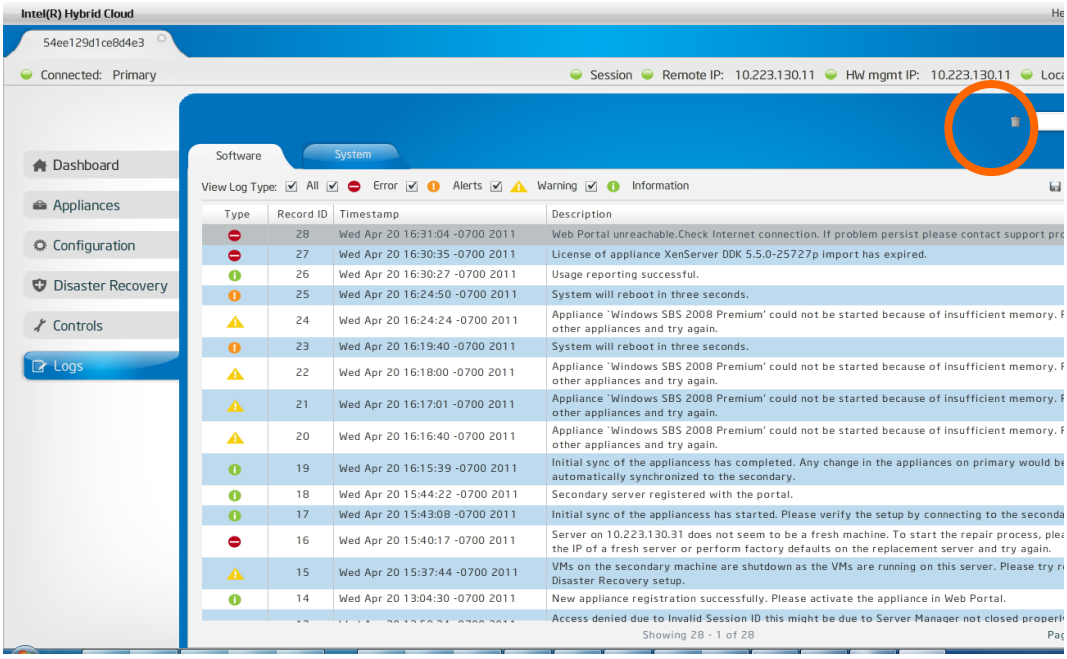

Figure 73. Server Manager - Software and Hardware Logs Deletion

6.11.2 Software Logs Download

The entire software log set can be exported to a CSV (Comma Separated Values) file. This file can also be used to import data to an excel sheet. This feature is available only for software logs. Clicking on the icon highlighted below can download software logs.

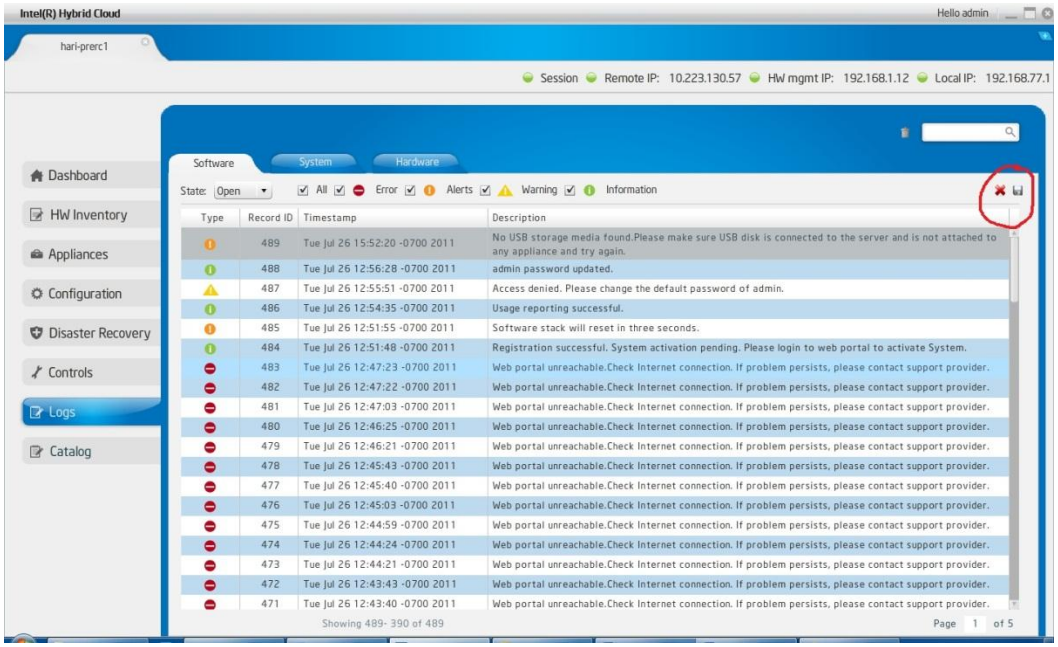

Figure 74. Server Manager - Software Logs Download

6.12 Appliance and Application Download

One new feature introduced in Intel® Hybrid Cloud 3.0 allows you to choose and install appliances and applications directly from the Intel AppUpSM Small Business Service catalog.

You may install appliances using Intel® Hybrid Cloud server manager.

Using the Intel Hybrid Cloud server manager, various appliances and applications can be downloaded and installed on the server.

To choose and download any appliance or application, click the “Catalog” tab. The server manager prompts for the userid and password for access to the portal. Provide your portal credentials at this page and you will be taken into the catalog service page.

A sample screenshot is shown below.

NOTE: Appliance and application installation can also be performed through Intel® Hybrid Cloud management portal. Refer to Section 5.1 to access the Intel® Hybrid Cloud management portal, and Section 5.5 for appliance and application installation details.

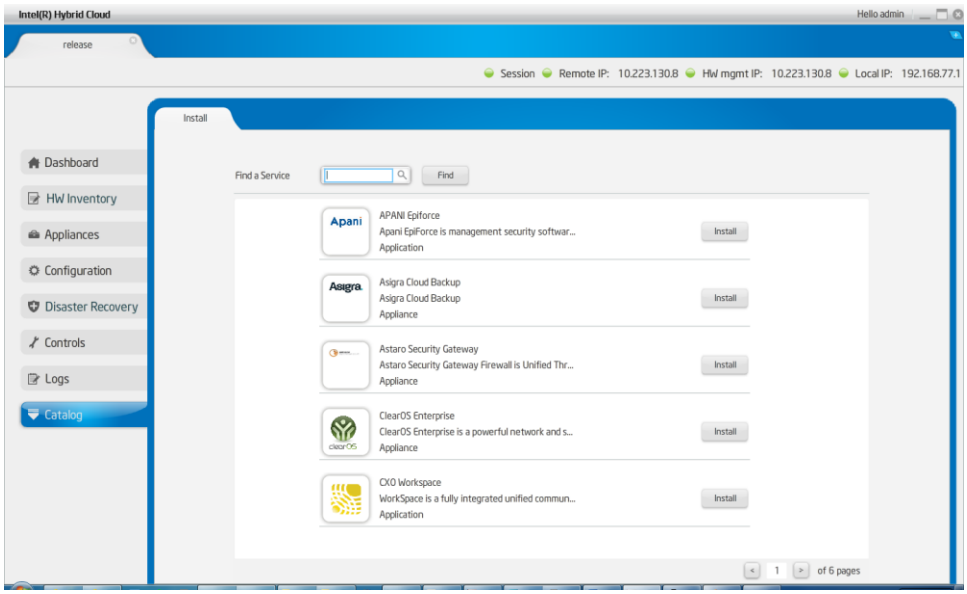

Figure 75. Server Manager - Install an Appliance or Application

A list of all available appliances and applications appears, in alphabetical order. Each listing under this section contains:

- Name of the appliance or application
- A short description
- Nature of download – whether it is an appliance or an application

Using the “filter” box, a few search terms can be entered and relevant results from the available set are displayed. This avoids having to scan the entire set of available entries.

Each of the listed entries also has a corresponding “Install” button. Clicking the button will initiate the installation process. For appliances, there is a 3 step wizard like process involved. For applications, there are 4 steps in the process, the additional step being the selection of the appliance where the application needs to be installed on to.

The following screenshots display the various steps involved in the install sequence.

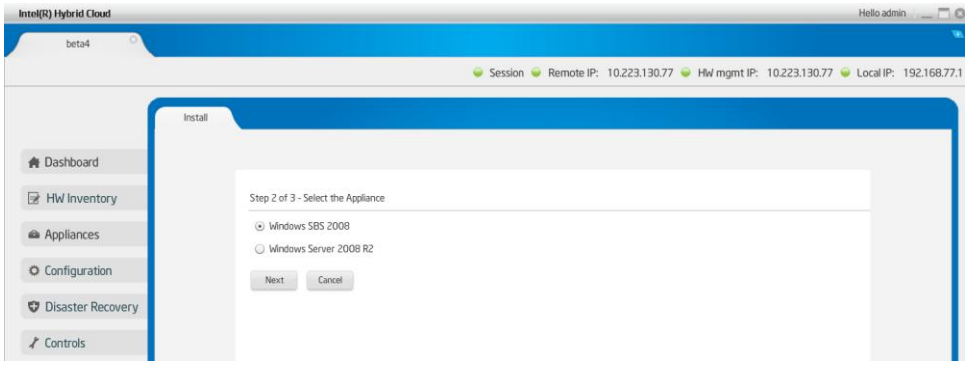

Figure 76. Server Manager - Appliance Installation – Step 2

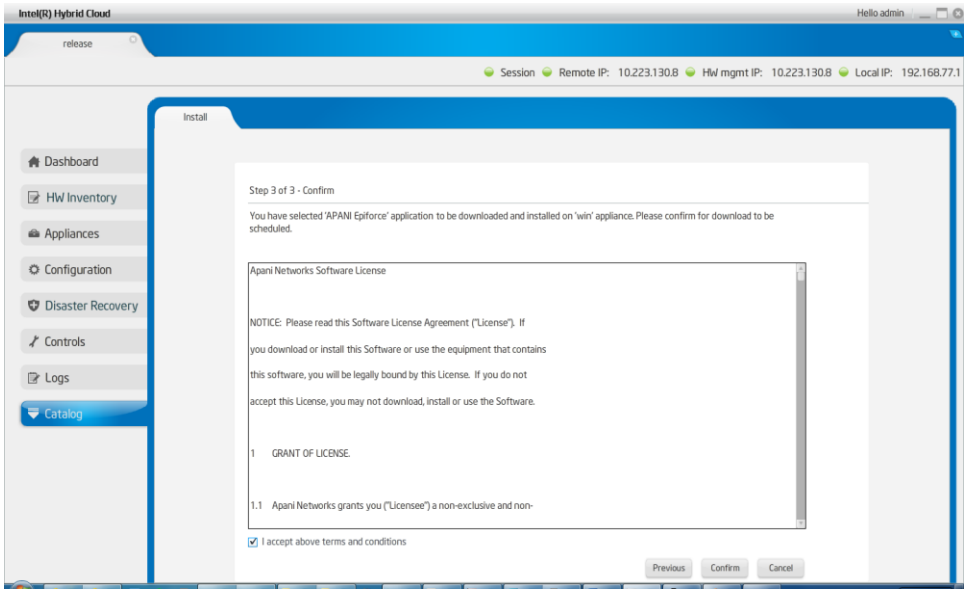

Figure 77. Server Manager - Appliance Installation – Step 3

As shown in the above screenshot, the End User License Agreement (EULA) will be displayed to the user and the user has to read and accept the agreement for the installation to go through.

Note that in the current version of the product, only those appliances that are available in the Local Application Store (LAS) of the server can be installed. The LAS is essentially a local storage repository on the server and contains appliances chosen by the customer during ordering. These appliances come pre-loaded on the server from the factory.

On the other hand, any of the applications in the list can be downloaded, provided the dependent appliance is available and already installed on the server.

Once the 3 (or 4) step installation process has been completed, the chosen appliance or application is set to be downloaded and installed. This process gets initiated during the next usage reporting cycle and is guaranteed to start within 24 hours. Once the download of the chosen appliance/application is completed, the package is automatically installed and will appear under the “Appliances” tab of the server manager. Note that for a particular application to be installed, the appliance on which it needs to be installed should be running. If the appliance is not active, the installation will be triggered only once the appliance has been booted.

If multiple appliances or applications are chosen for download and install, the server manager schedules their download in a sequential manner. Therefore, one should anticipate a considerable amount of time to be taken for the entire download and install of those multiple packages.

6.13 Multiple Server Management

The **All Servers** tab of the Intel® Hybrid Cloud server manager lists all the registered and active servers for the connected Remote Administrator. Remote Administrator needs to provide

management portal login credentials for this server list to be populated on this page. A sample **All Servers** window is displayed below.

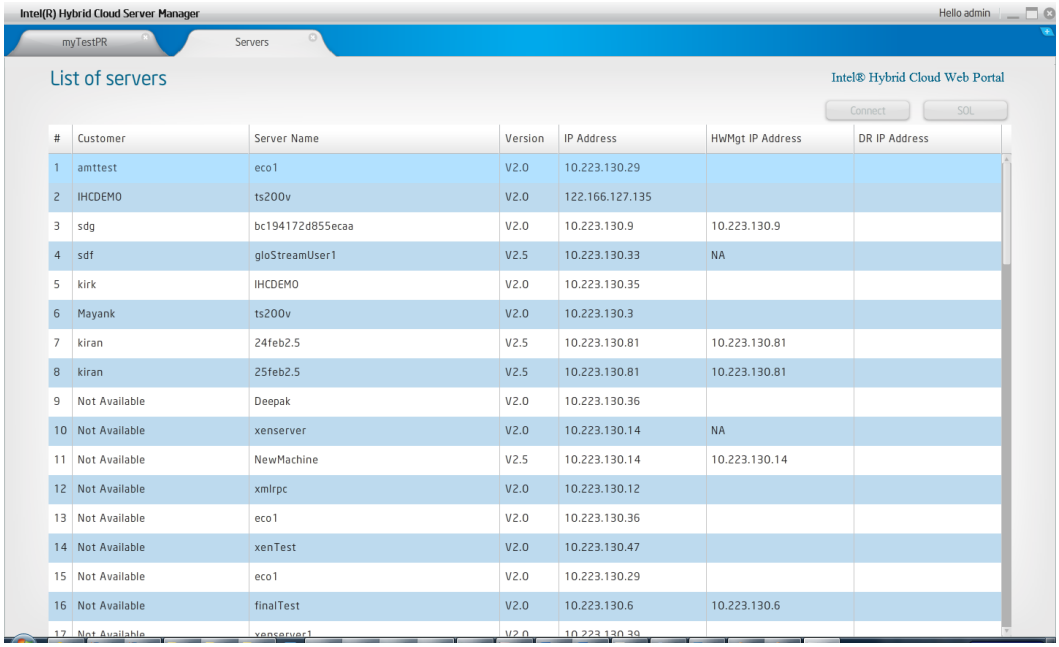

Figure 78. Server Manager - All Servers page

Remote Administrator can then connect to any of the servers listed by clicking **Connect** button and entering user credentials of the specific server in the **Connect to Server** dialog that appears subsequently, as shown in the following screenshot:

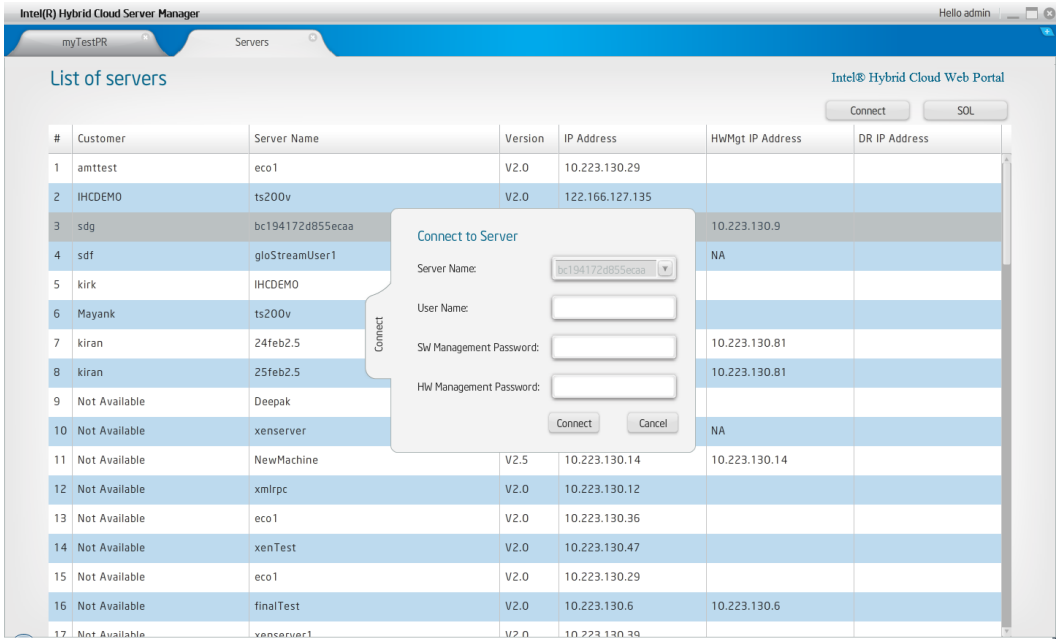

Figure 79. Server Manager - All servers → Connect to Server window

A new tab opens within the existing Intel® Hybrid Cloud server manager UI for the specified server.

Notes:

- Click **Portal** button in the **All Servers** page to open the management portal page in the default browser of the client machine.
- Click **SOL** to open a Serial over LAN access to a specific server. This will need Intel ® AMT login credentials. One can use this for recovering a server remotely via Intel ® AMT.
- If the configured system has BMC support, upon clicking the SOL RMM3 (Remote management module) button, a new page will open. This allows user to perform other actions such as KVM management and other out-of-band operations.

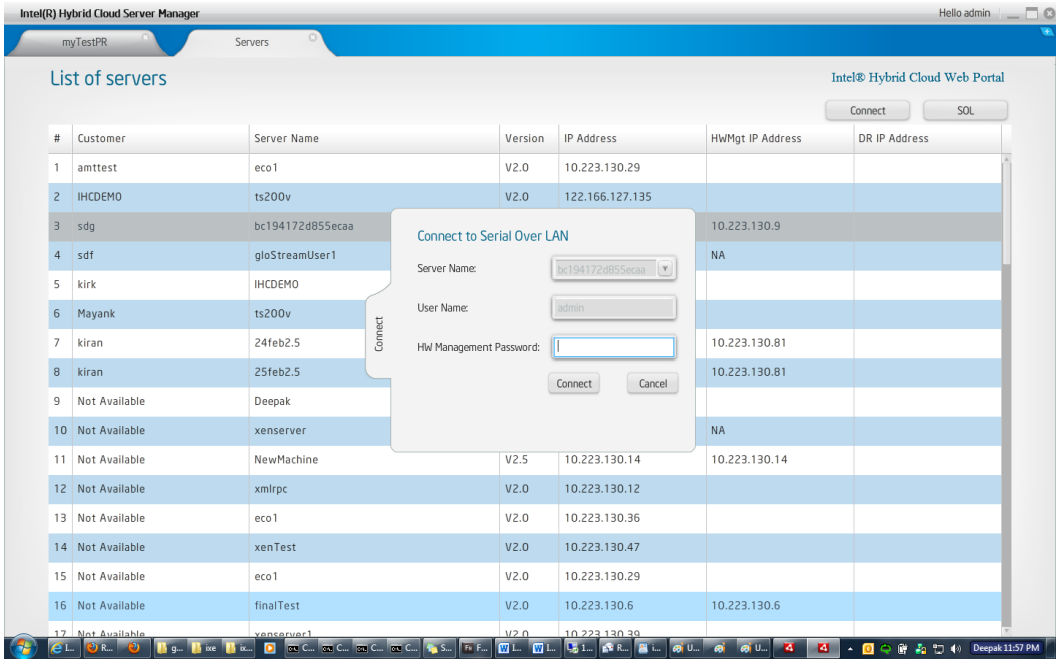

Figure 80. Server Manager - All servers → Connect to Server window (via Intel® AMT)

6.14 Patching mechanism

IHC 3.0 software supports patching the various components. The patching module handles deploying patches for any issues that are fixed once a release is made. During usage reporting, these patches get copied over to the portal and are ready to be applied. These patches are version based patches. A corresponding log entry would be added explaining the reason for the patch.

Here is a brief explanation of the patching mechanism:

- Intel Admin uploads the patch to IHC web portal.
- The portal administrator initiates the download of the patch to the particular server from the management portal. Please refer to section 5.10 for details on this.

- When any IHC server performs usage reporting, the portal checks for any patch availability and if a qualifying patch is found, the usage report response to the stack would contain the patch details.

- The stack downloads the patch and displays a ticker message on the server manager dashboard displaying “Patch is available. Please update”. Refer to screen shot below.

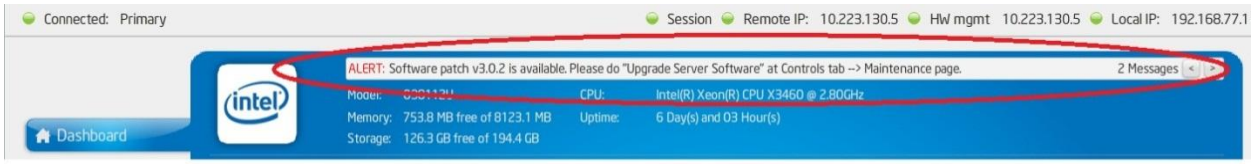

Figure 81. Server Manager - Patch Message

- Whenever user wishes to apply patch to stack, click on “Upgrade button in the server manager under Controls → Maintenance tab, in the “Upgrade Server” section. The following screenshot shows the location of this control.

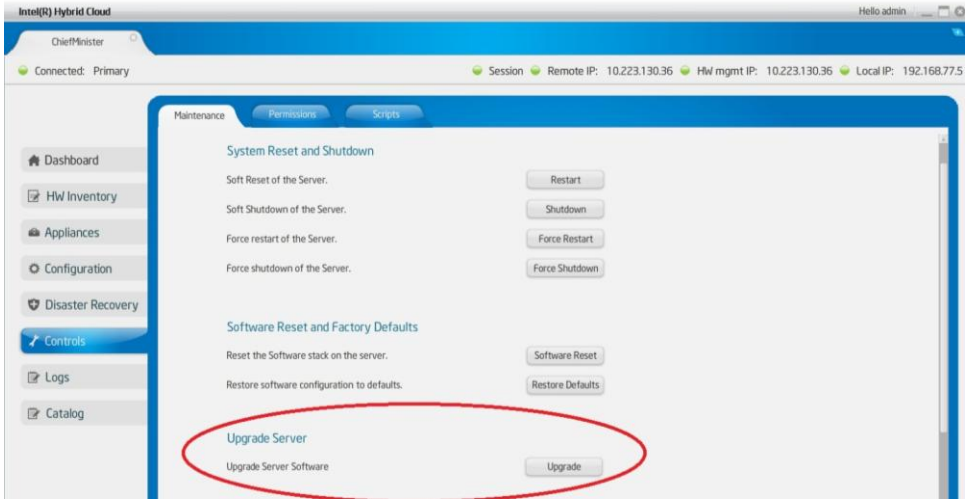

Figure 82. Server Manager - Upgrade the Server Software

- If the current patch has a dependency on other patches, the patching mechanism automatically downloads those previous patches and installs them as well.

Upon successfully applying a patch a log message is recorded.

In a configuration where disaster recovery has been setup, if a patch is applied via the above steps on the primary machine, the patching module automatically takes care of applying the patch on to the secondary machine. Therefore, no additional steps are required to update the secondary machines.

6.15 Logging out of Intel® Hybrid Cloud server manager

User can log out of the management console anytime by using the sign out option as highlighted in following screen OR clicking the UI close (X) button.

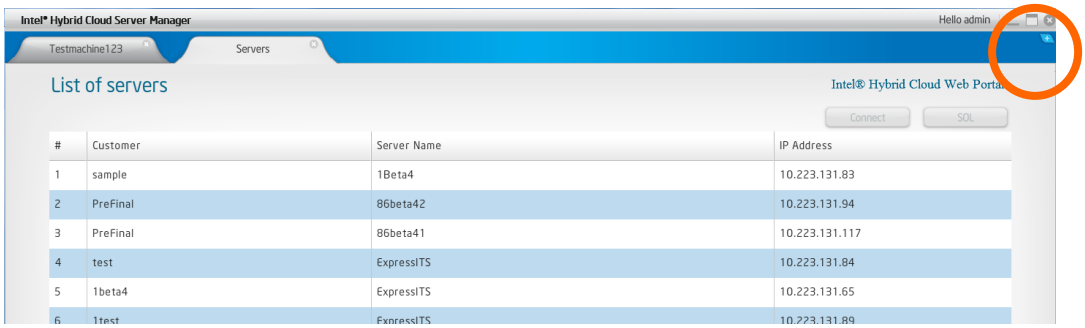

Figure 83. Server Manager - Log Out

7. Saving and Restoring System Configuration

Once the Intel® Hybrid Cloud server is configured, the system configuration can be saved and restored to the same machine (if needed due to a server stack or VMM crash). IXE commands are used to create the restore file, and to subsequently restore the configuration to the server.

The following items may be saved and restored:

- IP table settings: Secure Shell (SSH), Citrix XenServer* management
- Remote & Local IP configuration
- Email alerts configuration
- System Asset Tag
- Appliance store URL
- System brand info
- System name, time-zone
- User permissions
- User & Admin passwords
- System Host Name

NOTE: The restore file can only be applied to the server from which it was created. SMTP configuration can only be restored when using a DNS name. If SMTP is using a server IP address, it will not be restored.

7.1 Saving the Server Configuration

Use the following IXE commands to save the server configuration to a convenient location:

```
IXE –h <server IP> -u <user name> -p <password> -o save-restore-
configuration <directory path>.
```

7.2 Restoring the Server Configuration

Use the following IXE commands to restore the server configuration:

```
IXE –h <server IP> -u <user name> -p <password> -o apply-restore-
configuration user <file name>
```

NOTE: The server will reboot after successfully restoring and applying the configuration. Refer to Section 11 for additional IXE command information.

8. Activating Appliances

8.1 Activating Windows* Appliances

Once the Microsoft Windows* appliance is activated on the management portal and the Remote Administrator tries to start the appliance for the first time via the Intel® Hybrid Cloud server manager, the server manager opens a customer profile page giving an option to fill in appliance specific information (name, login name, business name, machine name, and password) as shown in following figure: This information is used for creating auto answer file for Windows* configuration and will vary from one version of Windows* OS to other.

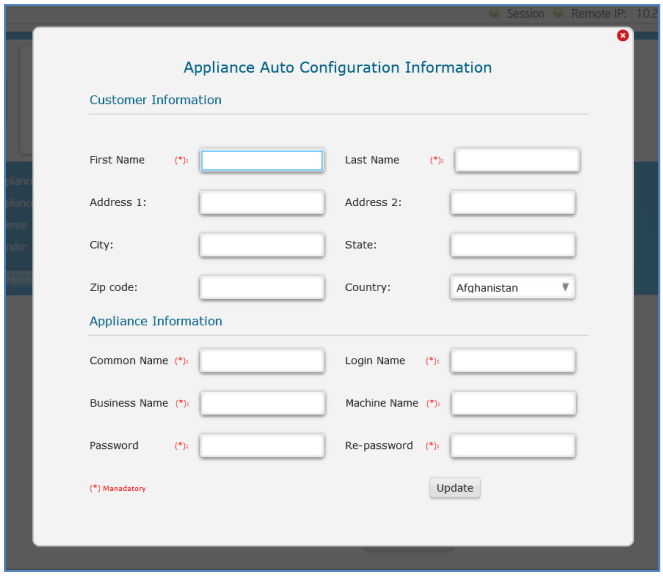

Figure 84. Activating Microsoft Windows* Appliances - Customer Profile page

After the Remote Administrator fills the information and clicks **Update**, server manager gets the available appliance activation key from the management portal, activates the appliance with that key, and configures the appliance with the information entered by the Remote Administrator (like login name, password and so on).

8.2 Activating Other Appliances

All non-Windows* appliances need to be simply activated through the Intel® Hybrid Cloud management portal by the remote administrator. If needed, a license is downloaded by the server manager from the management portal. License mechanism varies depending on the type of appliance. In some cases, an appliance key is emailed to MSP/Remote administrator and remote administrator may have to apply the license key manually for fully activating the appliance functionality. Once the appliance is installed on the server, the information would be sent to the management portal. Remote administrator can login to the management portal and activate the appliance.

9. Intel ® AMT Configuration

This section applies only to Intel® Hybrid Cloud servers with Intel® Active Management Technology (Intel® AMT), and does not apply to servers with Baseboard Management Controller (BMC).

Intel® AMT offers a HW chipset based solution for remote out-of-band management, using a secondary processor on the motherboard, with embedded firmware that runs on the Manageability Engine (ME). You can access Intel® AMT through the server remote IP port connection.

NOTE: If you are using an external firewall, refer to Section 4.1 for port forwarding details.

9.1 Intel® AMT Password

The Intel AMT password is automatically synchronized with the SW management password. Using any other method to change the Intel AMT password will break the synchronization. To change the SW management (password and the Intel AMT password), refer to Section 0.

IMPORTANT: Changing the Intel (R) ME Password (Intel AMT password) in the ME Configuration screen (BIOS) will break the synchronization with the SW management password. If an unsyscroniized Intel AMT password is lost, cannot be recovered. A subsequent Intel AMT password reset would require returning the Intel® Hybrid Cloud server to the place of purchase.

10. Intel ® Hybrid Cloud server BMC Configuration

This section applies only to Intel® Hybrid Cloud servers with Baseboard Management Controller (BMC), and does not apply to servers with Intel® Active Management Technology (Intel® AMT).

BMC is a specialized processor service that monitors the physical state of Intel® Hybrid Cloud server and provides remote management capabilities similar to Intel® AMT technology. You can access BMC through an independent IP port connection.

NOTE: If you are using an external firewall, refer to Section 4.1 for port forwarding details.

10.1 Change the BMC IP Address

1. Open the Intel® Hybrid Cloud server manager and connect to a server (as described in Section 6.2).

2. Use the following path in the Intel® Hybrid Cloud server manager to access the hardware information for BMC:

   "**Configuration**" menu button > "**Network Settings**" tab

3. Select the "**HW mgmt**" radio button.
4. Select the appropriate network type (i.e. DHCP or Static).

5. Change the default HW mgmt IP (BMC IP) to a suitable value.
   NOTE: The BMC IP address must be different from the remote IP address of the Intel® Hybrid Cloud server.

6. Close the current connection, and reconnect to the server to access the BMC Hardware features.

10.2 BMC Password

The BMC password is automatically synchronized with the SW management password. Using any other method to change the BMC password will break the synchronization. To change the SW management (password and the BMC password), refer to Section 0.

IMPORTANT: Changing the Intel (R) ME Password (BMC password) in the ME Configuration screen (BIOS) will break the synchronization with the SW management password. If an unsyscroniized BMC password is lost, cannot be recovered. A subsequent BMC password reset would require returning the Intel® Hybrid Cloud server to the place of purchase.

11. Intel® Hybrid Cloud command line tool (IXE)

Intel® Hybrid Cloud server can also be managed using the "`ixe`" command line tool. The tool is a one-operation-at-a-time kind of tool that can be scripted using any of the scripting languages the user may want to use. Both Linux* & Windows* variants of the tool are supported.

11.1 IXE command Line Format

The syntax for each operation supported by `ixe` is provided below.

Command Line Format:

```
# ixe -h | --host <IP Address/Hostname of the target machine>
-u | --user <target machine username> -p | --pass <target machine
password> -o | --operation <command name> [ <arg1><arg2>….]
```

Intel® AMT command format:

```
# ixe -h | --host < Intel® AMT IP Address/HostName> -u | --
user < Intel® AMT username> <-p | --pass> < Intel® AMT password> -
o | --operation < Intel® AMT command>
```

[AMT Commands: force-system-poweroff, force-system-reset, force-system-poweron, hw-system-information, hw-processor-information, hw-memory-information, hw-disk-information, and hw-event-log, change-hw-management-password]

[] → optional variable

<> → compulsory variable

- or -- → is fixed and must

Command Time out: 3 minutes

Help : **> ixe help** or > **ixe help <command>**

11.2 List of IXE Commands

The following tables provide the IXE commands that are supported on the Intel® Hybrid Cloud platform. Error codes are displayed separately at the end of this section.
NOTE: The results are provided as examples only. The results you see may differ.

Command: `activate-native-management`

Required Parameter	Null
Description	Enables xen center for the server to access
Supported User	{'admin'}
Usage	ixe –h *<server>* –u *admin* –p *<Password>* –o *activate-native-management*
Result	Command successful

Command: `active-aeon-md5sum`

Required Parameter	Null
Description	Updates active aeon
Supported User	{'admin'}
Usage	ixe –h *<server>* –u *admin* –p *<Password>* –o *active-aeon-md5sum <md5sum>*
Result	Command successful

Command: `allow-remote-login`

Required Parameter	<remote | local>
Description	Enable the remote login (SSH) option
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *allow-remote-login <remote/local>*
Result	Command successful

Command: `add-appliance-hard-disk-drive`

Required Parameters	<Appliance name> <Hard disk size in GB>
Description	Attach new harddisk to appliance.
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o add-appliance-hard-disk-drive* <Appliance name> <Hard disk size in GB>
Result	Command successful

Command: `appliance-attach-cdrom`

Required Parameters	<Appliance name> <CDROM name>
Description	Attach cd-rom to appliance.
Supported user	{'admin', 'user'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-attach-cdrom* <Appliance name> <CDROM name>
Result	Command successful

Command: `appliance-attach-usb`

Required Parameters	<Appliance name> <usb>
Description	Attach usb to appliance.
Supported user	{'admin', 'user' }
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-attach-usb* <Appliance name> <usb>
Result	Command successful

Command: `appliance-delete-hard-drive`

Required Parameters	<Appliance name> <Harddisk device position>
Description	Destroy harddisk connected to the appliance.
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-delete-hard-drive* <Appliance name> <Harddisk device position>
Result	Command successful

Command: `appliance-detach-cdrom`

Required Parameters	<Appliance name> <CDROM name>
Description	Detach cd-rom to appliance.
Supported user	{'admin', 'user'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-detach-cdrom* <Appliance name> <CDROM name>
Result	Command successful

Command: `appliance-detach-usb`

Required Parameters	<Appliance name> <usb>
Description	Detach usb to appliance.
Supported user	{'admin', 'user' }
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-detach-usb* <Appliance name> <usb>
Result	Command successful

Command: `appliance-resize-hard-drive`

Required Parameters	<Appliance name> <hard-drive-position> <new hdd size>
Description	Increases HDD capacity which is already attached to appliance.
Supported user	{'admin', 'user' }
Usage	*ixe -h <server ip> -u <username> -p <password> -o appliance-resize-hard-drive* <Appliance name> <hard-drive-position> <new hdd size>
Result	Command successful

Command: `appliance-uninstall`

Required Parameters	<appliance name>
Description	*uninstalls the requested appliance from system*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* appliance-uninstall <appliance name>
Result	*Command successful*

Command: `apply-restore-configuration`

Required Parameters	<system> | [<user> <restore file>]
Description	restore the system to old configurations.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o apply-restore-configuration <system> | [<user> <restore file>]
Result	Command successful. (Restores the system to original configurations.)

Command: `apply-stack-patch`

Required Parameters	Null
Description	Applies patch to IHC server.
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o apply-stack-patch*
Result	Command successful

Command: `apply-vm-metadata`

Required Parameters	<>
Description	apply the appliance metadata to the server host
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o apply-vm-metadata
Result	Command successful. (Restores the appliance metadata)

Command: `attach-appliances-to-network`

Required Parameter	<Appliance name>
Description	attaches the requested appliances to the network
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *attach-appliance-network <appliance name>*
Result	Command successful

Command: `block-remote-login`

Required Parameter	<remote | local>
Description	Disable the remote login (SSH) option for the requested interface.
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *block-remote-login <remote/local>*
Result	Command successful

Command: `change-appliance-memory`

Required Parameters	<Appliance name> <Memory in MB>
Description	Create Increase or Descrease the apliance Memory.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o change-appliance-memory <Appliance name> <Memory in MB>
Result	Command successful

Command: `change-default-password`

Required Parameters	<NewPassword>
Description	Resets the system password to new password this is a mandatory step before connecting to stack.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o change-default-password <NewPassword>
Result	Command successful

Command: `change-password`

Required Parameter	<Appliance Name>
Description	Change the password for the requested user
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *change-password <new password>*
Result	Command successful

Command: `configure-box-expiry-grace-period`

Required Parameter	<expiry days> <grace period days>
Description	Sets box expiry period days and grace period days
Supported User	{'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *configure-box-expiry-grace-period <expiry period days number> <grace period days number>*
Result	Command successful

Command: `configure-email-alerts`

Required Parameters	<disable | enable <msp | user email> <loglevels>>
Description	*Update the email parameters to which the alerts will be sent.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o configure-email-alerts* <disable | enable <msp | user email> <loglevels>>
Result	Command successful

Command: `configure-network-parameters`

Required Parameter	<local | remote> <static or dhcp> <IP Address > <Net mask> [gateway] [DNS server] (IP Address and Netmask is required for static and gateway is compulsory for remote for static)
Description	returns the network parameters for the requested interface
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip> -u <user name>*-p <password> –o *configure-network-parameters <remote/local>* <local | remote> <static or dhcp> <IP Address > <Net mask> [gateway] [DNS server]
Result	Command successful

Command : `configure-server-email-alerts`

Required Parameters	<smtp server IP address> <smtp port> <box username> <box password>
Description	*Update Update the server email parameters from which the alerts will be sent.*
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o configure-server-email-parameters* <smtp server IP address> <smtp port> <box username> <box password>
Result	Command successful

Command: `connect-appliance-console`

Required Parameter	Null
Description	*Connect to the Appliance console*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* connect-appliance-console
Result	*Command Successful (launches the appliance console)*

Command: `create-appliance-network-interface`

Required Parameters	<Appliance name> <remote | local>
Description	Create a new network interface for the appliance .
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o create-appliance-network-interface <Appliance name> <remote | local>
Result	Command successful

Command: `deactivate-native-management`

Required Parameter	Null
Description	disables xen center for the server to access
Supported User	{'admin'}
Usage	ixe –h *<server>* –u *admin* –p *<Password>* –o *deactivate-native-management*
Result	Command successful

Command: `delete-appliance-network-interface`

Required Parameters	<Appliance name> <mac address of the network interface>
Description	Destory a network interface for the appliance
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o delete-appliance-network-interface <Appliance name> <mac address of the network interface>
Result	Command successful

Command: `delete-event-log`

Required Parameter	<Error level | 0 (delete all logs in all level)>
Description	Deletes all logs from requested level.
Supported User	{'user'}
Usage	ixe –h *<server ip>* -u <user name>–p *<password>* –o *delete-event-log <Error level>*
Result	Event log cleared

Command: `detach-appliances-from-network`

Required Parameter	<Appliance name>
Description	Detaches the requested appliances from the network
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *detach-appliance-network <appliance name>*
Result	Command successful

Command: `disable-patching`

Required Parameter	Null
Description	Disables patch path
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *disable-patching*
Result	Command successful

Command: `disconnect-appliance-console`

Required Parameter	<appliance name>
Description	Closes console for the specified appliance
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *disconnect-appliance-console*
Result	Command successful

Command: `enable-patching`

Required Parameter	Null
Description	Enables patch path
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *enable-patching*
Result	Command successful

Command: `get-alert-messages`

Required Parameters	< >
Description	This command provides the messages related to box and appliances.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-alert-messages
Result	Returns the Stack messages for the User and MSP

Command: `get-appliance-backup-status`

Required Parameters	Null
Description	*returns the progress of the appliance backup*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get*-appliance-backup-status
Result	*NA/NA-Success/NA-failure/percentage*

Command: `get-appliance-boot-order`

Required Parameter	null
Description	Appliances name and the UUID are returned in the order they are set to boot
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-boot-order*
Result	Appliance1 : 075d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: `get-appliance-brand-info`

Required Parameter	<Appliance name>
Description	Returns the appliances brand info set by the admin
Supported User	{'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-brand-info <appliance name>*
Result	Command successful

Command: `get-appliance-license-configuration`

Required Parameter	<Appliance name>
Description	Returns the appliances configuration deatils
Supported User	{'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-license-configuration <appliance name>*
Result	Configuration details

Command: `get-appliance-management-url`

Required Parameter	<Appliance name>
Description	Returns the appliance management url to connect
Supported User	{'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-management-url <appliance name>*
Result	Management url

Command: `get-appliance-parameters`

Required Parameter	<Appliance name>
Description	returns all the appliances specific parameters
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-parameters <appliance name>*
Result	disktotal : 8.59 GB Numcpu : 1 Nos Memorytotal : 1.00 GB Uptime : 1 Day(s) 21:29:58

Command: `get-appliance-power-state`

Required Parameter	<Appliance Name>
Description	Returns the power state of the requested appliance
Supported User	{'user, 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *get-appliance-power-state Backup*
Result	name : Appliance1 uuid : 75d37ba0-40cb-d4cc-8adc-42de1d519487 powerstate : Halted

Command: `get-appliance-restore-status`

Required Parameters	Null
Description	*returns the progress of the appliance backup*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get*-appliance-restore-status
Result	*NA/NA-Success/NA-failure/percentage*

Command: `get-appliance-usage`

Required Parameter	<Appliance name>
Description	returns all the appliances specific usage [note :- ts - > time stamp Usage is in percentage]
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-appliance-usage <appliance name>*
Result	disktotal : 8.59 GB Numcpu : 1 Nos Memorytotal : 1.00 GB Uptime : 1 Day(s) 21:29:58

Command: `get-cdrom-list`

Required Parameter	Null
Description	Lists all cdroms attached to server
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-cdrom-list*
Result	name_lable : SCSI 2:0:0:0 vdi_uuid : 9db06e24-0299-44a2-8a61-6e16395190d4 virtual_size : 1073741312

Command: `get-close-logs`

Required Parameter	<log level>
Description	Lists all closed logs
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-close-logs 1*
Result	1 : 233 : Mon Mar 09 06:16:48 +0530 2009 : Access granted 1 : 232 : Mon Mar 09 06:16:40 +0530 2009 : Session Successfully Disconnected

Command: `get-command-permissions`

Required Parameter	Null
Description	*returns the api and the permission status set by admin*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get-command –permisssions*
Result	*returns the api and the permission status set by admin*

Command: `get-console-status`

Required Parameter	Null
Description	Returns the Console(USB) status
Supported User	{'admin', 'user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *get-console-status*
Result	Command successful

Command: `get-email-alert-parameters`

Required Parameters	Null
Description	*Displays the email alert parameters configured for the requested user.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get-email-alert-parameters*
Result	Email aler configuration for the user requested

Command: `get-event-log`

Required Parameter	<Error level> (0 - > to get logs of all level) Level 1 - > Information Level 2 -> Warnings Level 3 - > Alerts Level 4 -> Error
Description	returns all logs for the requested level
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *get-event-log 1*
Result	Detailed Logs for example 1,233, Mon Mar 09 06:16:48 +0530 2009, Access granted 1,232, Mon Mar 09 06:16:40 +0530 2009, Session Successfully Disconnected

Command: `get-installed-appliances`

Required Parameter	Null
Description	Returns the names and UUIDs of the appliances installed on the system.
Supported User	{'user, 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *get-installed-appliances*
Result	Appliance1 : 75d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: `get-internet-ip-address`

Required Parameters	<>
Description	displays the internet accessable ip address which can be used to connect to the server.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-internet-ip-address
Result	Internet accessible IP Address

Command: `get-log-size`

Required Parameters	<log level>
Description	Returns log count for the level
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-log-size 1
Result	20

Command: `get-network-detached-appliances`

Required Parameter	Null
Description	returns all the appliances that are detached from the network
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-network-detached-appliances*
Result	Appliance1 : 75d37ba0-40cb-d4cc-8adc-42de1d519487 Appliance2 : 127ba0-40cb-d4cc-7dc-42de1d519423

Command: `get-network-parameters`

Required Parameter	<local | remote>
Description	returns the network parameters for the requested interface
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-network-parameters local*
Result	netmask : 255.255.255.0 ip : 192.168.1.1 boot-protocol : static

Command: `get-network-policy`

Required Parameter	<remote | local>
Description	List the Network policy of the requested Interface (remote | local)
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-network-policy <remote/local*
Result	remote-management : enabled ssh : enabled xen-management : enabled

Command: `get-number-of-appliances`

Required Parameter	Null
Description	Returns the total number appliance installed on the system
Supported User	{'user, 'admin'}
Usage	ixe –h *<server>* –u *admin* –p *admin* –o *get-number-of-appliances*
Result	2

Command: `get-open-logs`

Required Parameter	<Log level>
Description	Lists all open logs
Supported User	{'user, 'admin'}
Usage	ixe –h *<server>* –u *<username>* –p *<password>* –o *get-open-logs 1*
Result	1 : 233 : Mon Mar 09 06:16:48 +0530 2009 : Access granted 1 : 232 : Mon Mar 09 06:16:40 +0530 2009 : Session Successfully Disconnected

Command: `get-power-state-for-all-appliances`

Required Parameter	Null
Description	*returns the power state of all the appliance installed in the System*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* get-power-state-for-all-appliances
Result	*returns the power state of all the appliance installed in the System*

Command: `get-restore-files`

Required Parameter	Null
Description	*returns backed up image files from USB connected to server*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* get-restore-files
Result	*Lists img files*

Command: `get-service-list`

Required Parameter	<appliance-name>
Description	*Lists all services available on particular appliance*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* get-sevice-list <appliance name>
Result	Name: SamSs Power_state: running app_id: sam1 type: service

Command: `get-system-asset-tag`

Required Parameters	Null
Description	*Display the System uniquely identified tag.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* get-system-asset-tag
Result	*System unique asset tag*

Command: `get-system-brand-info`

Required Parameter	Null
Description	Returns the Intel® Hybrid Cloud server Brand Info set by the admin
Supported User	{'admin','user'}
Example	ixe –h *<server ip>*-u <user name>-p <password> –o *get-system-brand-info*
Result	product : Intel® Hybrid Cloud client : Client name logo : test.png

Command: `get-system-event-log`

Required Parameters	Null
Description	*Displays xensource system event logs.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> –o get-system-event-log*
Result	Xensource *System event logs (only warning and error logs)*

Command: `get-system-log-size`

Required Parameters	Null
Description	*Returns system log count.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> –o get-system-log-size*
Result	200

Command: `get-system-parameters`

Required Parameter	Null
Description	Returns the system parameters
Supported User	{'user', 'admin'}
Usage	ixe –h <*server ip*>-u <user name>-p <password> –o *get-system-parameters*
Result	disktotal : 151 GB Name : system name cpumodel : Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz memorytotal : 3.90 GB version : 1.0 uptime : 1 Day(s) 12:09:47 systemmodel : DQ45CB

Command: `get-system-serial-id`

Required Parameters	< >
Description	This command retrieves the unique serial number of the box.
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o get-system-serial-id
Result	Returns the system unique serial id

Command: `get-system-time`

Required Parameter	Null
Description	returns system time and time zone
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get-system-time*
Result	returns the system time and time zone

Command: `get-system-timezones`

Required Parameter	Null
Description	returns list of time zone..
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get-system-timezones*
Result	returns the list of time zone

Command: `get-system-tpm-key`

Required Parameter	Null
Description	returns tpm key for the server
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o get-system-tpm-key*
Result	returns 64 bytes tpm key

Command: `get-system-usage`

Required Parameter	Null
Description	returns the system usage like wan, lan , cpu etc
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *get-system-usage*
Result	lan : 0.0 memory : 37.38 wan : 10.0 cpu : 12.8 ts : 03/09/2009 09:38:07 IST Disk : 92.93

Command: `get-usb-list`

Required Parameter	Null
Description	Lists all cdroms attached to server
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *get-usb-list*
Result	name_lable : USB 2:0:0:0 vdi_uuid : 9db06e24-0299-44a2-8a61-6e16395190d4 virtual_size : 1073741312

Command: `initiate-usage-reporting`

Required Parameter	Null
Description	Performs usage reporting of box to server and parses response from server
Supported User	{'admin','user'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o initiate-usage-reporting
Result	*Command successful*

Command: `install-system-license`

Required Parameters	<System license>
Description	*Applies the system license for the xenserver*
Supported user	{admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* install-system-license <System license>
Result	*Command successful*

Command: `is-appliance-license-valid`

Required Parameter	<Appliance Name>
Description	Returns the status of the license installed on the requested appliance
Supported User	{ 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *is-appliance-license-valid <appliance name>*
Result	valid/invalid

Command: `resume-appliance`

Required Parameter	<Appliance Name>
Description	Resume the requested appliance
Supported User	{'admin','user'}
Example	ixe –h *<server ip>*-u <user name>-p <password> –o *resume-appliance <appliance name>*
Result	Command successful

Command: `save-restore-configuration`

Required Parameters	<Path to Store the restore configuration file>
Description	Retrieves the current system configuration. This can be used by the
Supported user	{'user','admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o save-restore-configuration
Result	File Name of the system configuration

Command: `set-appliance-boot-order`

Required Parameter	<Appliance name in order required separated by space>
Description	set the appliance to boot during the system reboot Note: - If the Arguments are Empty the Command Clears the Boot order set previously.
Supported User	{ 'admin'}
Example	ixe –h *<server ip>*-u <user name> -p <password> –o *set-appliance-boot-order Backup Windows*
Result	Command successful

Command: `set-appliance-client-name`

Required Parameter	<Applaince Name><client name>
Description	Updates the requested Appliance Client name.
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password>–o *get-appliance-client-name* <Applaince Name><client name>
Result	Command successful

Command: `set-appliance-default-brand-info`

Required Parameters	<APP ID> <Vendor name> <vendor Logo>
Description	Updates the appliance brand information in the stack
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o `set-`appliance-default-brand-info <APP ID> <Vendor name> <vendor Logo>
Result	Command successful.

Command: `set-appliance-logo`

Required Parameter	<Appliance name><logo location>
Description	Uploads the requested Appliance Logo.
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *set-appliance-logo* <Appliance name><logo location>
Result	Command successful

Command: `set-appliance-vcpu-number`

Required Parameters	<Appliance name> <number of Vcpu>
Description	Increase appliance virtual CPU numbers.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o set-appliance-vcpu-number <Appliance name> <number of Vcpu>
Result	Command successful

Command: `set-appliance-vendor-name`

Required Parameter	<Appliance Name> <vendor name>
Description	Updates the requested Appliance Vendor name.
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password>–o *set-appliance-vendor-name* <Appliance Name> <vendor name>
Result	Command successful

Command: `set-console-disable`

Required Parameter	Null
Description	Disable the Console (USB) option
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *set-console-disable*
Result	Command successful

Command: `set-console-enable`

Required Parameter	Null
Description	Enable the Console (USB) option
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *set-console-enable*
Result	Command successful

Command: `set-logs-close`

Required Parameter	<log ID/s>
Description	Closes particular log IDs
Supported User	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *set-logs-close 200*
Result	Command successful

Command: `set-oem-factory-defaults`

Required Parameters	<>
Description	*Set the Server to OEM factory defaults(removes all VMS)*
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o set-oem-factory-defaults*
Result	*Command successful*

Command: `set-system-client-name`

Required Parameter	<Name>
Description	Updates the Intel® Hybrid Cloud server client name.
Supported User	{'admin'}
Example	ixe –h *<server ip>*-u <user name>-p <password> –o *set-system-client-name <new client name>*
Result	Command successful

Command: `set-system-defaults`

Required Parameter	Null
Description	Reset the system to factory defaults
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *set-system-defaults*
Result	Command successful

Command: `set-system-logo`

Required Parameter	<logo file location>
Description	Updates the Intel® Hybrid Cloud server logo.
Supported User	{'admin'}
Usage	ixe –h *<server ip>-u <user name>*-p <password> –o *set-system-logo <File location>*
Result	Command successful

Command: `set-system-product-name`

Required Parameter	<Product Name>
Description	Updates the Intel® Hybrid Cloud system vendor name.
Supported User	{'admin'}
Usage	ixe –h *<server ip>*-u <user name>-p <password> –o *set-system-product-name <product name>*
Result	Command successful

Command: `software-reset`

Required Parameter	null
Description	Restarts the Intel® Hybrid Cloud software stack.
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *software-reset*
Result	Command successful

Command: `start-appliance`

Required Parameter	<Appliance Name>
Description	Starts the requested appliance in the system.
Supported User	{'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *start-appliance Backup*
Result	Command successful

Command: `start-appliance-backup`

Required Parameters	<Appliance Name>
Description	*initiates the backup for the requested appliance.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* start-appliance-backup <Appliance Name>
Result	*Command successful*

Command: `start-appliance-restore`

Required Parameters	<path ><img file Name>
Description	*initiates the restore for the requested appliance.*
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* start-appliance-restore <path> <img file Name>
Result	*Command successful*

Command: `start-service`

Required Parameters	<Appliance Name> <Service/Application Name>
Description	*Starts the requested service/application.*
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* start-service <Appliance Name> <Service/Application Name>
Result	*Command successful*

Command: `stop-service`

Required Parameters	<Appliance Name> <Service/Application Name>
Description	*Stops the requested service/application.*
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o* stop-service <Appliance Name> <Service/Application Name>
Result	*Command successful*

Command: `stop-appliance`

Required Parameter	<Appliance Name>
Description	Stop the requested appliance in the system
Supported User	{'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* –p *<password>* –o *stop-appliance <appliance name>*
Result	Command successful

Command: `suspend-appliance`

Required Parameter	<Appliance Name>
Description	Suspends the requested appliance
Supported User	{'admin'}
Example	ixe –h *<server ip>*-u <user name>-p <password> –o *suspend-appliance <appliance name>*
Result	Command successful

Command: `sync-with-portal`

Required Parameter	null
Description	It syncs client with portal.
Supported User	{'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *sync-with-portal*
Result	Command successful

Command: `system-poweroff`

Required Parameter	null
Description	power off the system
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *system-poweroff*
Result	Command successful

Command: `system-reset`

Required Parameter	null
Description	Restarts the System.
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *system-reset*
Result	Command successful

Command: `update-appliance-name`

Required Parameters	<Appliance name> <New Appliance Name>
Description	Set new appliance name.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-appliance-name <Appliance name> <New Appliance Name>
Result	Command successful

Command: `update-eula`

Required Parameter	<license file>
Description	Updates the eula on the Intel Hybrid cloud System.
Supported user	{'admin' }
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *update-eula* <license file>
Result	Command successful

Command: `update-ntp-servers`

Required Parameters	<ntp server 1>[server2]… {max 3 serves}
Description	apply new ntp settings
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-ntp-server <ntp server IP>
Result	Command successful.

Command: `update-system-name-label`

Required Parameter	<system name>
Description	Update the system label with the requested name
Supported User	{'user', 'admin'}
Usage	ixe –h *<server ip>* –u *<user name>* -p <password>–o *update-system-name-label <new name>*
Result	Command successful

Command: `update-system-timezone`

Required Parameter	<time zone>
Description	Update the system time zone
Supported user	{'user','admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o update-system-timezone* <time zone>
Result	*Command Successful*

Command: `update-appliance-unattend-template`

Required Parameters	<unattended template>
Description	Uploads template for unattended installation.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-appliance-unattend-template <unattended template>
Result	Command successful.

Command: `update-catalog-server-url`

Required Parameters	<URL>
Description	Updates TC catalog server url
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-catalog-server-url <url>
Result	Command successful.

Command: `update-custom-template`

Required Parameters	<unattended template>
Description	Uploads template for unattended installation.
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-custom-template <unattended template>
Result	Command successful.

Command: `update-reg-server-url`

Required Parameters	<url>
Description	Updates registration server URL
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-reg-server-url <url>
Result	Command successful.

Command: `update-reg-ssl-cert`

Required Parameters	<certificate pem file>
Description	Uploads certificate to box
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o update-reg-ssl-cert <pem file>
Result	Command successful.

Command: `upgrade-host-server`

Required Parameters	<Xen update patch file>
Description	*upgrade the server Software*
Supported user	{'admin'}
Usage	*ixe -h <server ip> -u <username> -p <password> -o ,upgrade-host-server XenServer-5.5.0-Update2.xsupdate*
Result	*Command successful*

Command : `upgrade-management-software`

Required Parameter	<applications. zip>
Description	Upgrade the system software stack
Supported user	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *upgrade- management–software* <applications. zip>
Result	Command successful

Command: `upgrade-system-software`

Required Parameter	<System Stack File>
Description	Upgrade the system software stack
Supported user	{'admin','user'}
Usage	ixe –h *<server ip>* -u <user name> -p <password> –o *update-system-software* <System Stack File>
Result	Command successful

Command: `upload-system-scripts`

Required Parameters	<script location>
Description	Uploads script to script tabs to help user in diagnostics
Supported user	{'admin'}
Usage	ixe -h <server ip> -u <username> -p <password> -o upload-system-scripts <script>
Result	Command successful.

11.3 IXE AMT Commands

Command: `change-hardware-management-password`

Required Parameter	<new password>
Description	AMT password change
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *change-hardware-management-password* <new password>
Result	Command successful

IMPORTANT: The Intel AMT password is automatically synchronized with the SW management password. To change the SW management (password and the Intel AMT password), refer to Section 0. Changing the Intel AMT password by any other method will break the synchronization. If an unsyscroniized Intel AMT password is lost, it cannot be recovered. A subsequent Intel AMT password reset would require returning the Intel® Hybrid Cloud server to the place of purchase.

Command: `configure-hw-network-parameters`

Required Parameter	<dhcp|static>[if static <ip> <netmask> <gateway> [dns]]
Description	Configure hardware management network details
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *configure-hw-network-parameters* <dhcp|static>[if static <ip> <netmask> <gateway> [dns]]
Result	Command successful

Command: `force-system-poweroff`

Required Parameter	Null
Description	AMT system power off (force fully shutdowns the system)
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p *<password>* –o *force-system-poweroff*
Result	Command successful

Command: `force-system-poweron`

Required Parameter	Null
Description	AMT system power off (force fully shutdowns the system)
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *force-system-poweron*
Result	Command successful

Command: `force-system-reset`

Required Parameter	Null
Description	AMT system reboot (force fully reboot the system)
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p *<password>* –o *force-system-reset*
Result	Command successful

Command: `get-hw-network-parameters`

Required Parameter	Null
Description	AMT network details
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o get-hw-network-parameters
Result	AMT Network details {IP,Netmask,gateway etc}

Command: `get-hw-system-power-state`

Required Parameter	Null
Description	System power state.
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o get-hw-system-power-state
Result	System state

Command: `hardware-disk-information`

Required Parameter	Null
Description	Returns Hardware Disk Information
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *hardware-disk-information*
Result	returns hardware disk information

Command: `hardware-event-log`

Required Parameter	Null
Description	Returns Hardware event logs
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *hardware-event-log*
Result	returns hardware event logs

Command: `hardware-memory-information`

Required Parameter	Null
Description	Returns Hardware memory Information
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *hardware-memory-information*
Result	returns hardware memory information

Command: `hardware-processor-information`

Required Parameter	Null
Description	Returns Hardware Processor Information
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *hardware-processor-information*
Result	returns hardware processor information

Command: `hardware-system-information`

Required Parameter	Null
Description	Returns system hardware Information
Supported user	{'admin'}
Usage	ixe –h *<server ip>* -u <user name> –p <password> –o *hardware-system-information*
Result	returns hardware system information

11.4 IXE Error Messages

In the event of a error, IXE commands will provide an error message. For yor convenience, some error descriptions are provided below.

Table 4. IXE Error Messages

Failure Messages	Description
Command failed	Command could not be executed successfully.
Invalid parameters	Wrong arguments are supplied to the command.
Invalid session	Session to the Intel® Hybrid Cloud server is lost.
Invalid server response	Invalid response received.
Authentication failed	User name or password provided is incorrect.
No appliance Installed	No appliance available in Intel® Hybrid Cloud server.
No response from server	Command has reached timeout